

AOS-W Instant

6.5.1.0-4.3.1.0

Alcatel·Lucent 
Enterprise

User Guide

Copyright Information

Alcatel-Lucent and the Alcatel-Lucent Enterprise logo are trademarks of Alcatel-Lucent. To view other trademarks used by affiliated companies of ALE Holding, visit:

enterprise.alcatel-lucent.com/trademarks

All other trademarks are the property of their respective owners. The information presented is subject to change without notice. Neither ALE Holding nor any of its affiliates assumes any responsibility for inaccuracies contained herein. (July 2016)

Open Source Code

This product includes code licensed under the GNU General Public License, the GNU Lesser General Public License, and/or certain other open source licenses.

About this Guide	9
Intended Audience	9
Related Documents	9
Conventions	9
Contacting Support	10
About AOS-W Instant	12
AOS-W Instant Overview	12
What is New in this Release	15
Setting up an OAW-IAP	17
Setting up AOS-W Instant Network	17
Provisioning an OAW-IAP	18
Logging in to the AOS-W Instant UI	20
Accessing the AOS-W Instant CLI	21
Automatic Retrieval of Configuration	25
Managed Mode Operations	25
Prerequisites	25
Configuring Managed Mode Parameters	26
Verifying the Configuration	27
AOS-W Instant User Interface	29
Login Screen	29
Main Window	30
Initial Configuration Tasks	58
Configuring System Parameters	58
Changing Password	64
Customizing OAW-IAP Settings	65
Modifying the OAW-IAP Host Name	65
Configuring Zone Settings on an OAW-IAP	65
Specifying a Method for Obtaining IP Address	66
Configuring External Antenna	67
Configuring Radio Profiles for an OAW-IAP	68

Configuring Uplink VLAN for an OAW-IAP	70
Changing the OAW-IAP Installation Mode	70
Changing USB Port Status	71
Master Election and Virtual Controller	72
Adding an OAW-IAP to the Network	73
Removing an OAW-IAP from the Network	74
VLAN Configuration	75
VLAN Pooling	75
Uplink VLAN Monitoring and Detection on Upstream Devices	75
IPv6 Support	76
IPv6 Notation	76
Enabling IPv6 Support for OAW-IAP Configuration	76
Firewall Support for IPv6	78
Debugging Commands	78
Wireless Network Profiles	79
Configuring Wireless Network Profiles	79
Configuring Fast Roaming for Wireless Clients	99
Configuring Modulation Rates on a WLAN SSID	102
Multi-User-MIMO	103
Management Frame Protection	104
Disabling Short Preamble for Wireless Client	104
Editing Status of a WLAN SSID Profile	104
Editing a WLAN SSID Profile	105
Deleting a WLAN SSID Profile	105
Wired Profiles	106
Configuring a Wired Profile	106
Assigning a Profile to Ethernet Ports	111
Editing a Wired Profile	111
Deleting a Wired Profile	112
Link Aggregation Control Protocol	112
Understanding Hierarchical Deployment	113
Captive Portal for Guest Access	115
Understanding Captive Portal	115
Configuring a WLAN SSID for Guest Access	116

Configuring Wired Profile for Guest Access	122
Configuring Internal Captive Portal for Guest Network	124
Configuring External Captive Portal for a Guest Network	127
Configuring Facebook Login	133
Configuring Guest Logon Role and Access Rules for Guest Users	134
Configuring Captive Portal Roles for an SSID	136
Configuring Walled Garden Access	139
Authentication and User Management	141
Managing OAW-IAP Users	141
Supported Authentication Methods	146
Supported EAP Authentication Frameworks	148
Configuring Authentication Servers	149
Understanding Encryption Types	163
Configuring Authentication Survivability	164
Configuring 802.1X Authentication for a Network Profile	166
Enabling 802.1X Supplicant Support	168
Configuring MAC Authentication for a Network Profile	169
Configuring MAC Authentication with 802.1X Authentication	171
Configuring MAC Authentication with Captive Portal Authentication	172
Configuring WISPr Authentication	173
Blacklisting Clients	174
Uploading Certificates	177
Roles and Policies	180
Firewall Policies	180
Content Filtering	193
Configuring User Roles	197
Configuring Derivation Rules	199
Using Advanced Expressions in Role and VLAN Derivation Rules	206
DHCP Configuration	209
Configuring DHCP Scopes	209
Configuring the Default DHCP Scope for Client IP Assignment	216
Configuring Time-Based Services	219
Time Range Profiles	219
Configuring a Time Range Profile	219

Applying a Time Range Profile to a WLAN SSID	220
Verifying the Configuration	221
Dynamic DNS Registration	223
Enabling Dynamic DNS	223
Configuring Dynamic DNS Updates for Clients	224
Verifying the Configuration	225
VPN Configuration	226
Understanding VPN Features	226
Configuring a Tunnel from an OAW-IAP to a Mobility Controller	227
Configuring Routing Profiles	238
IAP-VPN Deployment	240
Understanding IAP-VPN Architecture	240
Configuring OAW-IAP and Switch for IAP-VPN Operations	243
Adaptive Radio Management	251
ARM Overview	251
Configuring ARM Features on an OAW-IAP	252
Configuring Radio Settings	258
Deep Packet Inspection and Application Visibility	263
Deep Packet Inspection	263
Enabling Application Visibility	263
Application Visibility	264
Enabling URL Visibility	269
Configuring ACL Rules for Application and Application Categories	269
Configuring Web Policy Enforcement Service	272
Voice and Video	275
Wi-Fi Multimedia Traffic Management	275
Media Classification for Voice and Video Calls	278
Enabling Enhanced Voice Call Tracking	279
Services	281
Configuring AirGroup	281
Configuring an OAW-IAP for RTLS Support	290
Configuring an OAW-IAP for Analytics and Location Engine Support	291
Managing BLE Beacons	292
Clarity Live	293

Configuring OpenDNS Credentials	295
Integrating an OAW-IAP with Palo Alto Networks Firewall	295
Integrating an OAW-IAP with an XML API Interface	297
CALEA Integration and Lawful Intercept Compliance	300
Cluster Security	306
Overview	306
Enabling Cluster Security	307
Cluster Security Debugging Logs	307
Verifying the Configuration	308
OAW-IAP Management and Monitoring	309
Managing an OAW-IAP from OmniVista	309
Uplink Configuration	319
Uplink Interfaces	319
Uplink Preferences and Switching	324
Intrusion Detection	329
Detecting and Classifying Rogue OAW-IAPs	329
OS Fingerprinting	329
Configuring Wireless Intrusion Protection and Detection Levels	330
Configuring IDS	335
Mesh OAW-IAP Configuration	336
Mesh Network Overview	336
Setting up AOS-W Instant Mesh Network	337
Configuring Wired Bridging on Ethernet 0 for Mesh Point	337
Mobility and Client Management	339
Layer-3 Mobility Overview	339
Configuring L3-Mobility	340
Spectrum Monitor	342
Understanding Spectrum Data	342
Configuring Spectrum Monitors and Hybrid OAW-IAPs	348
OAW-IAP Maintenance	350
Upgrading an OAW-IAP	350
Backing up and Restoring OAW-IAP Configuration Data	353
Converting an OAW-IAP to a Remote AP and Campus AP	354
Resetting a Remote AP or Campus AP to an OAW-IAP	360

Rebooting the OAW-IAP	360
Monitoring Devices and Logs	362
Configuring SNMP	362
Configuring a Syslog Server	366
Configuring TFTP Dump Server	367
Running Debug Commands	368
Uplink Bandwidth Monitoring	372
Hotspot Profiles	374
Understanding Hotspot Profiles	374
Configuring Hotspot Profiles	376
Sample Configuration	387
ClearPass Guest Setup	390
Configuring ClearPass Guest	390
Verifying ClearPass Guest Setup	393
Troubleshooting	393
IAP-VPN Deployment Scenarios	395
Scenario 1—IPsec: Single Datacenter Deployment with No Redundancy	396
Scenario 2—IPsec: Single Datacenter with Multiple Switches for Redundancy	400
Scenario 3—IPsec: Multiple Datacenter Deployment with Primary and Backup Switches for Redundancy	404
Scenario 4—GRE: Single Datacenter Deployment with No Redundancy	409
Glossary	412
Acronyms and Abbreviations	417
Glossary	432

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

Intended Audience

This guide is intended for administrators who configure and use OAW-IAPs.

Related Documents

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

- *AOS-W Instant Access Point Installation Guides*
- *AOS-W Instant Quick Start Guide*
- *AOS-W Instant CLI Reference Guide*
- *AOS-W Instant MIB Reference Guide*
- *AOS-W Instant Syslog Messages Reference Guide*
- *AOS-W Instant Release Notes*

Conventions

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

Table 1: *Typographical Conventions*

Style Type	Description
<i>Italics</i>	This style is used to emphasize important terms and to mark the titles of books.
System items	This fixed-width font depicts the following: <ul style="list-style-type: none">• Sample screen output• System prompts• Filenames, software devices, and specific commands when mentioned in the text.
Commands	In the command examples, this style depicts the keywords that must be typed exactly as shown.

Table 1: Typographical Conventions

Style Type	Description
<Arguments>	In the command examples, italicized text within angle brackets represents items that you should replace with information appropriate to your specific situation. For example: # send <text message> In this example, you would type “send” at the system prompt exactly as shown, followed by the text of the message you wish to send. Do not type the angle brackets.
[Optional]	Command examples enclosed in square brackets are optional. Do not type the square brackets.
{Item A Item B}	In the command examples, items within curly brackets and separated by a vertical bar represent the available choices. Enter only one choice. Do not type the curly brackets or bars.

The following informational icons are used throughout this guide:



NOTE

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



CAUTION

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



WARNING

Indicates a risk of personal injury or death.

Contacting Support

Table 2: Support Information

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

Contact Center Online	
EMEA	+800 00200100 (Toll Free) or +1-650-385-2193
Asia Pacific	+65 6240 8484
Worldwide	1-818-878-4507

This chapter provides the following information:

- [AOS-W Instant Overview on page 12](#)
- [What is New in this Release on page 15](#)

AOS-W Instant Overview

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

AOS-W Instant is a simple, easy to deploy turnkey WLAN solution consisting of one or more OAW-IAPs. An Ethernet port with routable connectivity to the Internet or a self-enclosed network is used for deploying an Instant Wireless Network. An Instant Access Point (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, AOS-W Instant is ideal for small customers or remote locations without requiring any on-site IT administrator.

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

Supported OAW-IAP Platforms

The following table provides a list of OAW-IAP platforms that support AOS-W Instant software:

Table 3: *Supported OAW-IAP Platforms*

OAW-IAP Platform	Minimum Required AOS-W Instant Software Version
OAW-IAP207	AOS-W Instant 6.5.1.0-4.3.1.0 or later
OAW-IAP304/305	AOS-W Instant 6.5.1.0-4.3.1.0 or later
OAW-IAP334/335	AOS-W Instant 6.5.0.0-4.3.0.0 or later
OAW-IAP314/315	AOS-W Instant 6.5.0.0-4.3.0.0 or later
OAW-IAP324/325	AOS-W Instant 6.4.4.3-4.2.2.0 or later
OAW-IAP205H OAW-IAP228 OAW-IAP277	AOS-W Instant 6.4.3.1-4.2.0.0 or later
OAW-IAP204/205 OAW-IAP214/215	AOS-W Instant 6.4.2.0-4.1.1.0 or later

Table 3: Supported OAW-IAP Platforms

OAW-IAP Platform	Minimum Required AOS-W Instant Software Version
OAW-IAP103 OAW-IAP274/275	AOS-W Instant 6.4.0.2-4.1.0.0 or later
OAW-IAP114/115 OAW-IAP224/225	AOS-W Instant 6.3.1.1-4.0.0.0 or later
OAW-RAP155/155P	AOS-W Instant 6.2.1.0-3.3.0.0 or later
OAW-RAP108/109	AOS-W Instant 6.2.0.0-3.2.0.0 or later



Each OAW-IAP model has a minimum required AOS-W Instant software version as shown in [Table 3](#). When a new OAW-IAP is added into an existing cluster, it can join the cluster only if the existing cluster is running at least the minimum required version of that OAW-IAP. If the existing cluster is running a version prior to the minimum required version of the new OAW-IAP, new OAW-IAP will not come up and may reboot with the reason **Image sync fail**. To recover from this condition, upgrade the existing cluster to at least the minimum required version of the new OAW-IAP first, and add the new OAW-IAP.



Alcatel-Lucent recommends that networks with more than 128 OAW-IAPs be designed as multiple, smaller VC networks with Layer-3 mobility enabled between these networks.

Alcatel-Lucent OAW-IAPs are available in the following variants:

- US (United States)
- JP (Japan)
- IS (Israel)
- RW

The following table provides the variants supported for each OAW-IAP platform:

Table 4: Supported OAW-IAP Variants

OAW-IAP Model (Reg Domain)	OAW-IAP###-US (US only)	OAW-IAP###-JP (Japan only)	OAW-IAP-###-IS (Israel only)	OAW-IAP-###-RW (Rest of the World except US/JP/IS)
OAW-IAP334/335	Yes	Yes	Yes	Yes
OAW-IAP314/315	Yes	Yes	Yes	Yes
OAW-IAP324/325	Yes	Yes	Yes	Yes

Table 4: Supported OAW-IAP Variants

OAW-IAP Model (Reg Domain)	OAW-IAP###-US (US only)	OAW-IAP###-JP (Japan only)	OAW-IAP-###-IS (Israel only)	OAW-IAP-###-RW (Rest of the World except US/JP/IS)
OAW-IAP277	Yes	Yes	No	Yes
OAW-IAP274/275	Yes	Yes	Yes	Yes
OAW-IAP228	Yes	Yes	No	Yes
OAW-IAP224/225	Yes	Yes	Yes	No
OAW-IAP214/215	Yes	Yes	Yes	Yes
OAW-IAP205H	Yes	Yes	Yes	Yes
OAW-IAP204/205	Yes	Yes	Yes	Yes
OAW-RAP155/155P	Yes	Yes	Yes	No
OAW-IAP114/115	Yes	Yes	Yes	No
OAW-RAP108/109	Yes	Yes	Yes	No
OAW-IAP103	Yes	Yes	Yes	Yes

For information on regulatory domains and the list of countries supported by the OAW-IAP-###-RW type, see the **Specifying Country Code** section in [Logging in to the AOS-W Instant UI on page 20](#)

AOS-W Instant UI

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

- Microsoft Internet Explorer 11 or earlier
- Apple Safari 6.0 or later
- Google Chrome 23.0.1271.95 or later
- Mozilla Firefox 17.0 or later

If the AOS-W Instant UI is launched through an unsupported browser, a warning message is displayed along with a list of recommended browsers. However, the users are allowed to log in using the **Continue login** link on the **Login** page.



To view the AOS-W Instant UI, ensure that JavaScript is enabled on the web browser.

The AOS-W Instant UI logs out automatically if the window is inactive for 15 minutes.

AOS-W Instant CLI

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

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

What is New in this Release

The following features are introduced in AOS-W Instant 6.5.1.0-4.3.1.0:

Table 5: New Features

Feature	Description
Cluster Security	Support for cluster security is introduced to secure control plane messages between OAW-IAPs. Additionally, DTLS is used with cluster security for extended security facilities. Cluster security also provides the option of logging and debugging by organizing the logs into modules which are later used for debugging.
Support for RFC5997	Starting from AOS-W Instant 6.5.1.0-4.3.1.0, you can configure the RFC5997 feature on the OAW-IAP to send a status request query to the RADIUS server each time there is an authentication or accounting request timeout. This helps determine if the server is actually down before marking the server as unavailable.
Clarity Live	AOS-W Instant now supports inline monitoring through Clarity Live to identify client connectivity issues and send the data to OmniVista for analysis. It helps in isolating the root cause of the connectivity issues experienced by receiving regular statistics and updates generated by the events.
Client Match for Access Points in a Zone	Starting from AOS-W Instant 6.5.1.0-4.3.1.0, the decision to move a client from a home OAW-IAP to a target OAW-IAP will be made at the SSID level instead of the radio level, by adding the SSID name to the client match radio database. Client Match will check if the same SSID (zone specific SSID on Home OAW-IAP) is available on the target OAW-IAP before it moves the client.
Changing the OAW-IAP Installation Mode	AOS-W Instant now allows users to change the installation type of the OAW-IAPs from indoor to outdoor or vice-versa.

Support for New IAP Devices

AOS-W Instant 6.5.1.0-4.3.1.0 release introduces support for the following new OAW-IAP devices. These new devices do not interoperate with Instant versions lower than AOS-W Instant 6.5.0.0-4.3.0.0. If these OAW-IAPs are placed into a cluster running older Instant versions prior to AOS-W Instant 6.5.1.0-4.3.1.0, the devices will reboot with the **Image Sync Fail** reason. To resolve this issue, upgrade the existing cluster to minimum AOS-W Instant 6.5.1.0-4.3.1.0 release, and then add the new OAW-IAP devices.

Table 6: *New Hardware Platforms*

Feature	Description
OAW-IAP304/305	The OAW-IAP300 Series (OAW-IAP304/305) wireless access points are equipped with one 10/100/1000Base-T auto-sensing MDI/MDX Ethernet port. This port supports wired-network connectivity, in addition to Power over Ethernet (PoE) from IEEE 802.3af and 802.3at compliant power sources. They also have two LEDs that indicate the system and radio status of the device and are equipped with three external antenna connectors.
OAW-IAP207	The OAW-IAP207 Series access points are equipped with one 10/100/1000Base-T (RJ-45) auto-sensing, MDI/MDX Ethernet port (ENET0) for wired network connectivity. This port supports IEEE 802.3af Power over Ethernet (PoE), as a standard defined Powered Device (PD) from a Power Sourcing Equipment (PSE) such as a PoE midspan injector or network infrastructure that supports PoE. The 207 Series access points have two LEDs that indicate the system and radio status of the device.

This chapter describes the following procedures:

- [Setting up AOS-W Instant Network on page 17](#)
- [Provisioning an OAW-IAP on page 18](#)
- [Logging in to the AOS-W Instant UI on page 20](#)
- [Accessing the AOS-W Instant CLI on page 21](#)

Setting up AOS-W Instant Network

Before installing an OAW-IAP:

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

Perform the following procedures to set up the AOS-W Instant network:

1. [Connecting an OAW-IAP on page 17](#)
2. [Assigning an IP address to the OAW-IAP on page 17](#)

Connecting an OAW-IAP

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

- PoE switch—Connect the Ethernet 0 (Enet0) port of the OAW-IAP to the appropriate port on the PoE switch.
- PoE midspan—Connect the Enet0 port of the 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.



OAW-RAP155P supports PSE for 802.3at-powered device (class 0-4) on one port (E1 or E2), or 802.3af-powered DC IN (Power Socket) on two ports (E1 and E2).

Assigning an IP address to the OAW-IAP

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

To obtain an IP address for an OAW-IAP:

1. Ensure that the DHCP service is enabled on the network.
2. Connect the Enet0 port of OAW-IAP to a switch or router using an Ethernet cable.
3. Connect the OAW-IAP to a power source. The OAW-IAP receives an IP address provided by the switch or router.



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

Assigning a Static IP

To assign a static IP to an OAW-IAP:

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

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

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

```
apboot> printenv
```

Provisioning an OAW-IAP

This section provides the following information:

- [Zero Touch Provisioning of OAW-IAPs on page 18](#)
- [Provisioning OAW-IAPs through OmniVista](#)

Zero Touch Provisioning of OAW-IAPs

Zero Touch Provisioning eliminates the traditional method of deploying and maintaining devices and allows you to provision new devices in your network automatically, without manual intervention. Following are the zero-touch provisioning methods for AOS-W Instant.

In order for zero-touch provisioning to be successful, the timezone of the OAW-IAP must be in synchronization with the NTP server.



To facilitate zero-touch provisioning using the OmniVista Management Platform (AMP), or Activate, you must configure the firewall and wired infrastructure to either allow the NTP traffic to pool.ntp.org, or provide alternative NTP servers under DHCP options. For more information on configuring an NTP server, see [NTP Server](#).

In a scenario where the NTP server is unreachable, the connection between the OAW-IAP and Activate will fall back to the unsecured status. The NTP client process running in the back end will continuously attempt to reconnect to the NTP server until a secure connection is established. The NTP client process receives a response from the NTP server on successfully establishing a connection and notifies the CLI process which runs a series of checks to ensure the NTP server is reachable.

Connecting to a Provisioning Wi-Fi Network

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

To connect to a provisioning Wi-Fi network:

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



The AOS-W Instant SSIDs are broadcast in 2.4 GHz only.

OAW-IAP Cluster

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



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

Disabling the Provisioning Wi-Fi Network

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

To disable the provisioning network:

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

Table 7: *Terminal Communication Settings*

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

3. Turn on the OAW-IAP. An autoboot countdown prompt that allows you to interrupt the normal startup process and access apboot is displayed.
4. Click **Enter** key before the timer expires. The OAW-IAP goes into the apboot mode through console.
5. In the apboot mode, execute the following commands to disable the provisioning network:

```
apboot> factory_reset
apboot> setenv disable_prov_ssid 1
```

```
apboot> saveenv
apboot> reset
```

Provisioning OAW-IAPs through OmniVista

For information on provisioning OAW-IAPs through OmniVista, refer to the *OmniVista Deployment Guide*.

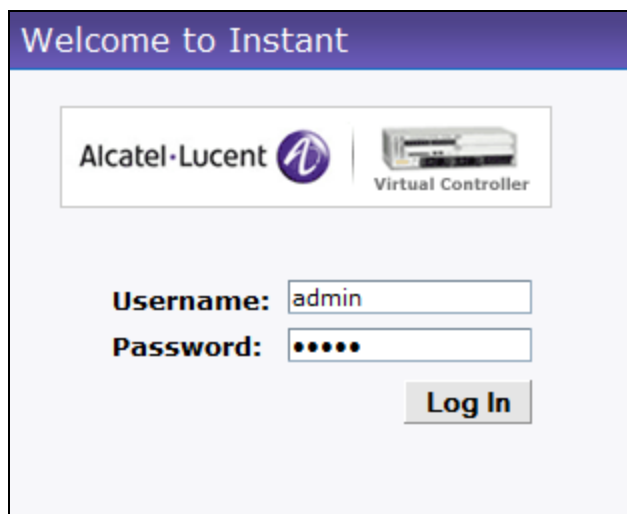
Logging in to the AOS-W Instant UI

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

- Username—admin
- Password—admin

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

Figure 1 *Login Screen*



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

Regulatory Domains

The IEEE 802.11 b/g/n Wi-Fi networks operate in the 2.4 GHz spectrum and IEEE 802.11 a/n operates in the 5 GHz spectrum. The spectrum is divided into channels. The 2.4 GHz spectrum is divided into 14 overlapping, staggered 20 MHz wireless carrier channels. These channels are spaced 5 MHz apart. The 5 GHz spectrum is divided into more channels. The channels that can be used in a particular country vary 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 AOS-W Instant operates. This configuration sets the regulatory domain for the radio frequencies that the OAW-IAPs use. Within the regulated transmission spectrum, a high-throughput 802.11 ac, 802.11 a, 802.11 b/g, or 802.11 n radio setting can be configured. The available 20 MHz, 40 MHz, or 80 MHz channels are dependent on the specified country code.

You cannot change the country code for the OAW-IAPs in the restricted regulatory domains such as US, Japan, and Israel for most of the OAW-IAP models. For OAW-IAP-RW variants, you can select from the list of supported regulatory domains. If the supported country code is not in the list, contact your Alcatel-Lucent Support team to know if the required country code is supported and obtain the software that supports the required country code.



Improper country code assignments can disrupt wireless transmissions. Most countries impose penalties and sanctions on operators of wireless networks with devices set to improper country codes.

To view the country code information, run the **show country-codes** command.

Specifying Country Code



This procedure is applicable only to the OAW-IAP-RW variants. Skip this step if you are installing OAW-IAP in the United States, Japan, or Israel.

The **Country Code** window is displayed for the OAW-IAP-RW variants when you log in to the OAW-IAP UI for the first time. The **Please Specify the Country Code** drop-down list displays only the supported country codes. If the OAW-IAP cluster consists of multiple OAW-IAP platforms, the country codes supported by the master OAW-IAP is displayed for all other OAW-IAPs in the cluster. Select a country code from the list and click **OK**. The OAW-IAP operates in the selected country code domain.

Figure 2 *Specifying a Country Code*



You can also view the list of supported country codes for the OAW-IAP-RW variants using the **show country-codes** command.

Accessing the AOS-W Instant CLI

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

For information on enabling SSH and Telnet access to the OAW-IAP CLI, see [Terminal access on page 62](#).

Connecting to a CLI Session

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

```
User: admin
```

If the login is successful, the privileged command mode is enabled and a command prompt is displayed. For example:

```
(Instant AP) #
```

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

```
(Instant AP) # configure terminal
```

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

```
(Instant AP) (config) #
```

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

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



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

Applying Configuration Changes

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

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

```
(Instant AP) # commit apply
```

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

```
(Instant AP) # commit apply no-save
```

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

```
(Instant AP) # show uncommitted-config
```

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

```
(Instant AP) # commit revert
```

Example:

To apply and view the configuration changes:

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

```
(Instant AP) # show uncommitted-config
rf dot11a-radio-profile
beacon-interval 200
no legacy-mode
dot11h
interference-immunity 3
csa-count 2
```

```
spectrum-monitor
```

```
(Instant AP)# commit apply
```

Using Sequence-Sensitive Commands

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

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

Table 8: *Sequence-Sensitive Commands*

Sequence-Sensitive Command	Corresponding no command
<code>opendns <username <password></code>	<code>no opendns</code>
<code>rule <dest> <mask> <match> <protocol> <start-port> <end-port> {permit deny src-nat dst-nat {<IP- address> <port> <port>}} [<option1...option9>]</code>	<code>no rule <dest> <mask> <match> <protocol> <start-port> <end-port> {permit deny src-nat dst-nat}</code>
<code>mgmt-auth-server <auth-profile-name></code>	<code>no mgmt-auth-server <auth-profile- name></code>
<code>set-role <attribute>{{equals not-equals starts- with ends-with contains} <operator> <role> value-of}</code>	<code>no set-role <attribute>{{equals not-equals starts-with ends-with contains} <operator> value-of}</code> <code>no set-role</code>
<code>set-vlan <attribute>{{equals not-equals starts- with ends-with contains} <operator> <VLAN-ID> value-of}</code>	<code>no set-vlan <attribute>{{equals not-equals starts-with ends-with contains} <operator> value-of}</code> <code>no set-vlan</code>
<code>auth-server <name></code>	<code>no auth-server <name></code>

Banner and Loginsession Configuration using CLI

Starting from AOS-W Instant 6.5.0.0-4.3.0.0, the Banner and Loginsession Configuration feature is introduced in the OAW-IAP, wherein the text banner can be displayed at the login prompt when users are on a management (Telnet or SSH) session of the CLI, and the management session can remain active even when there is no user activity involved.

The **banner** command defines a text banner to be displayed at the login prompt of a CLI. AOS-W Instant supports up to 16 lines text, and each line accepts a maximum of 255 characters including spaces.

To configure a banner:

```
(Instant AP) (config)# banner motd <motd_text>
```

Example of a text banner configuration:

```
(Instant AP) (config)# banner motd "#####welcome to login instant#####"  
(Instant AP) (config)# banner motd "####please start to input admin and password#####"  
(Instant AP) (config)# banner motd "###Don't leak the password###"  
(Instant AP) (config)# end  
(Instant AP)# commit apply
```

To display the banner:

```
(Instant AP) # show banner
```

The **loginsession** command configures the management session (Telnet or SSH) to remain active without any user activity.

To define a timeout interval:

```
(Instant AP) (config) #loginsession timeout <val>
```

<val> can be any number of minutes from 5 to 60, or any number of seconds from 1 to 3600. You can also specify a timeout value of 0 to disable CLI session timeouts. The users must re-login to the OAW-IAP after the session times out. The session does not time out when the value is set to 0.

This chapter provides the following information:

- [Managed Mode Operations on page 25](#)
- [Prerequisites on page 25](#)
- [Configuring Managed Mode Parameters on page 26](#)
- [Verifying the Configuration on page 27](#)

Managed Mode Operations

OAW-IAPs support managed mode operations to retrieve the configuration file from a server through the File Transfer Protocol (FTP) or FTP over Secure Sockets Layer (FTPS), and automatically update the OAW-IAP configuration.

The server details for retrieving configuration files are stored in the basic configuration of the OAW-IAPs. The basic configuration of an OAW-IAP includes settings specific to an OAW-IAP, for example, host name, static IP, and radio configuration settings. When an OAW-IAP boots up, it performs a GET operation to retrieve the configuration (.cfg) file from the associated server using the specified download method.

After the initial configuration is applied to the OAW-IAPs, the configuration can be changed at any point. You can configure a polling mechanism to fetch the latest configuration by using an FTP or FTPS client periodically. If the remote configuration is different from the one running on the OAW-IAP and if a difference in the configuration file is detected by the OAW-IAP, the new configuration is applied. At any given time, OAW-IAPs can fetch only one configuration file, which may include the configuration details specific to an OAW-IAP. For configuring polling mechanism and downloading configuration files, the users are required to provide credentials (username and password). However, if automatic mode is enabled, the user credentials required to fetch the configuration file are automatically generated. To enable automatic configuration of the OAW-IAPs, configure the managed mode command parameters.

Prerequisites

Perform the following checks before configuring the managed mode command parameters:

- Ensure that the OAW-IAP is running AOS-W Instant 6.2.1.0-3.4 or later versions.
- When the OAW-IAPs are in the managed mode, ensure that the OAW-IAPs are not managed by OmniVista.

Configuring Managed Mode Parameters

To enable the automatic configuration, perform the steps described in the following table:

Table 9: *Managed Mode Commands*

Steps	Command
1. Start a CLI session to configure the managed-mode profile for automatic configuration.	<pre>(Instant AP) (config) # managed-mode-profile</pre>
2. Enable automatic configuration Or Specify the user credentials.	<pre>(Instant AP) (managed-mode-profile) # automatic</pre> <p>Or</p> <pre>(Instant AP) (managed-mode-profile) # username <username> (Instant AP) (managed-mode-profile) # password <password></pre> <p>NOTE: If the automatic mode is enabled, the user credentials are automatically generated based on OAW-IAP MAC address.</p>
3. Specify the configuration file.	<pre>(Instant AP) (managed-mode-profile) # config-filename <file_name></pre> <p>Filename—Indicates filename in the alphanumeric format. Ensure that configuration file name does not exceed 40 characters.</p>
4. Specify the configuration file download method.	<pre>(Instant AP) (managed-mode-profile) # download-method <ftp ftps></pre> <p>You can use either FTP or FTPS for downloading configuration files.</p>
5. Specify the name of the server or the IP address of the server from which the configuration file must be downloaded.	<pre>(Instant AP) (managed-mode-profile) # server <server_name></pre>

Table 9: Managed Mode Commands

Steps	Command
6. Configure the day and time at which the OAW-IAPs can poll the configuration files from the server.	<pre>(Instant AP) (managed-mode-profile)# sync-time day <dd> hour <hh> min <mm> window <window></pre> <p>Based on the expected frequency of configuration changes and maintenance window, you can set the configuration synchronization timeline.</p> <ul style="list-style-type: none"> • <code>day <dd></code>—Indicates day, for example to configure Sunday as the day, specify 01. To configure the synchronization period as everyday, specify 00. • <code>hour <hh></code>—Indicates hour within the range of 0-23. • <code>min <mm></code>—Indicates minutes within the range of 0-59. • <code>window <hh></code>—Defines a window for synchronization of the configuration file. The default value is 3 hours.
7. Configure the time interval in minutes between two retries, after which OAW-IAPs can retry downloading the configuration file.	<pre>(Instant AP) (managed-mode-profile)# retry-poll-period <seconds></pre> <p>NOTE: Specify the retry interval in seconds within the range of 5-60 seconds. The default retry interval is 5 seconds.</p>
8. Apply the configuration changes.	<pre>(Instant AP) (managed-mode-profile)# end (Instant AP)# commit apply</pre>

If you want to apply the configuration immediately and do not want to wait until next configuration retrieval attempt, execute the following command:

```
(Instant AP)# managed-mode-sync-server
```

Example

To configure managed mode profile:

```
(Instant AP) (config)# managed-mode-profile
(Instant AP) (managed-mode-profile)# username <username>
(Instant AP) (managed-mode-profile)# password <password>
(Instant AP) (managed-mode-profile)# config-filename instant.cfg
(Instant AP) (managed-mode-profile)# download-method ftps
(Instant AP) (managed-mode-profile)# sync-time day 00 hour 03 min 30 window 02
(Instant AP) (managed-mode-profile)# retry-poll-period 10
(Instant AP) (managed-mode-profile)# end
(Instant AP)# commit apply
```

Verifying the Configuration

To verify if the automatic configuration functions, perform the following checks:

1. Verify the status of configuration by running the following commands at the command prompt:

```
(Instant AP)# show managed-mode config
(Instant AP)# show managed-mode status
```

2. Verify the status of download by running the following command at the command prompt:

```
(Instant AP)# show managed-mode logs
```

If the configuration settings retrieved in the configuration file are incomplete, OAW-IAPs reboot with the earlier configuration.

This chapter describes the following AOS-W Instant UI elements:

- [Login Screen on page 29](#)
- [Main Window on page 30](#)

Login Screen

The AOS-W Instant login page allows you to perform the following tasks:

- View AOS-W Instant Network Connectivity summary
- View the AOS-W Instant UI in a specific language
- Log in to the AOS-W Instant UI

Viewing Connectivity Summary

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

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

Figure 3 Connectivity Summary

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

Language

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

You can also select the required language option from the **Languages** drop-down list located on the AOS-W Instant main window.

Logging into the AOS-W Instant UI

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

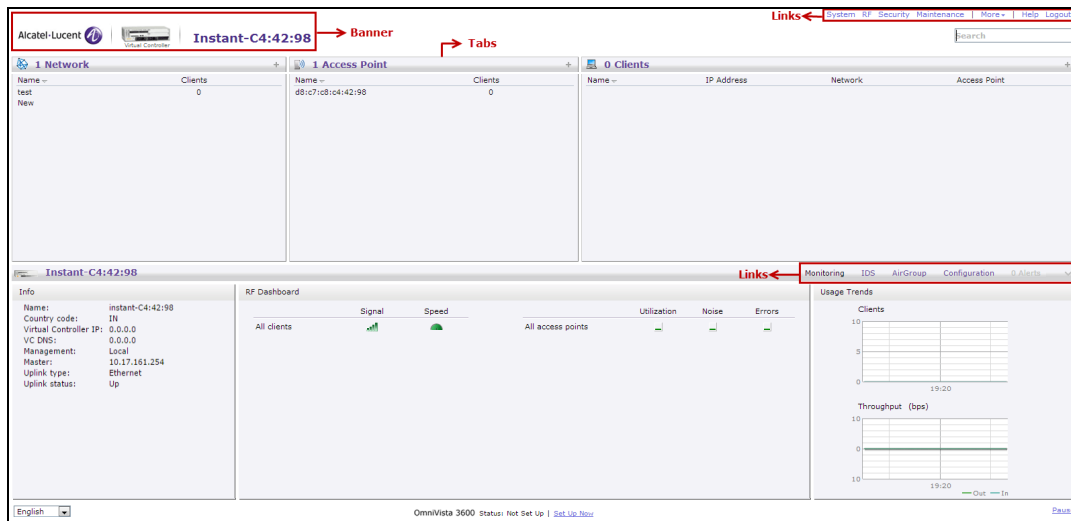
- Username—admin
- Password—admin

The AOS-W Instant UI main window is displayed.

Main Window

On logging in to Instant, the Instant UI Main Window is displayed. The following figure shows the AOS-W Instant main window:

Figure 4 AOS-W Instant Main Window



The main window consists of the following elements:

- [Banner](#)
- [Search Text Box](#)
- [Tabs](#)
- [Links](#)
- [Views](#)

Banner

The banner is a horizontal rectangle that appears on the AOS-W Instant main window. It displays the company name, logo, and the VC's name.

Search Text Box

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

Tabs

The AOS-W Instant main window consists of the following tabs:

- [Network Tab](#)—Provides information about the network profiles configured in the Instant network.
- [Access Points Tab](#)—Provides information about the OAW-IAPs configured in the Instant network.
- [Clients Tab](#)—Provides information about the clients in the Instant network.

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

Network Tab

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

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

To add a wireless network profile, click the **New** link on the **Network** tab. To edit, click the **edit** link that is displayed on clicking the network name in the **Network** tab. To delete a network, click the **x** link.

For more information on the procedure to add or modify a wireless network, see [Wireless Network Profiles on page 79](#).

Access Points Tab

If the Auto-Join Mode feature is enabled, a list of enabled and active OAW-IAPs in the AOS-W Instant network is displayed on the **Access Points** tab. The OAW-IAP names are displayed as links. If the Auto Join Mode feature is disabled, the **New** link is displayed. Click 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 of the **Access Points** tab displays the following information about each OAW-IAP:

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

An **edit** link is displayed on clicking the OAW-IAP name. For details on editing OAW-IAP settings, see [Customizing OAW-IAP Settings on page 65](#).

Clients Tab

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

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

Links

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

- [New Version Available](#)
- [System](#)
- [RF](#)
- [Security](#)
- [Maintenance](#)
- [More](#)
- [Help](#)
- [Logout](#)
- [Monitoring](#)
- [Client Match](#)
- [AppRF](#)
- [Spectrum](#)
- [Alerts](#)
- [IDS](#)
- [AirGroup](#)
- [Configuration](#)
- [OmniVista Setup](#)
- [Pause/Resume](#)

Each of these links is explained in the subsequent sections.

New Version Available

This link is displayed on the AOS-W Instant main window only if a new image version is available on the image server and OmniVista is not configured. For more information on the **New version available** link and its functions, see [Upgrading an OAW-IAP on page 350](#).

System

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



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

- **General**—Allows you to configure, view, or edit the Name, IP address, NTP Server, and other OAW-IAP settings for the VC.
- **Admin**—Allows you to configure administrator credentials for access to the VC Management UI. You can also configure OmniVista in this tab. For more information on management interface and OmniVista configuration, see [Managing OAW-IAP Users on page 141](#) and [Managing an OAW-IAP from OmniVista on page 309](#), respectively.
- **Uplink**—Allows you to view or configure uplink settings. See [Uplink Configuration on page 319](#) for more information.
- **L3 Mobility**—Allows you to view or configure the Layer-3 mobility settings. See [Configuring L3-Mobility on page 340](#) for more information.
- **Enterprise Domains**—Allows you to view or configure the DNS domain names that are valid in the enterprise network. See [Configuring Enterprise Domains on page 194](#) for more information.
- **Monitoring**—Allows you to view or configure the following details:
 - **Syslog**—Allows you to view or configure Syslog server details for sending syslog messages to the external servers. See [Configuring a Syslog Server on page 366](#) for more information.
 - **TFTP Dump**—Allows you to view or configure a Trivial File Transfer Protocol (TFTP) dump server for core dump files. See [Configuring TFTP Dump Server on page 367](#) for more information.
 - **SNMP**—Allows you to view or configure Simple Network Management Protocol (SNMP) agent settings. See [Configuring SNMP on page 362](#) for more information.
- **WISPr**—Allows you to view or configure the Wireless ISP-roaming (WISPr) settings. See [Configuring WISPr Authentication on page 173](#) for more information.
- **Proxy**—Allows you to configure HTTP proxy on an OAW-IAP. See [Configuring HTTP Proxy on an OAW-IAP on page 350](#) for more information.
- **Time Based Services**—Allows you to configure a time profile which can be assigned to the SSID configured on the OAW-IAP. See [Configuring Time-Based Services on page 219](#)

RF

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

- **ARM**—Allows you to view or configure channel and power settings for all the OAW-IAPs in the network. For information on ARM configuration, see [ARM Overview on page 251](#).
- **Radio**—Allows you to view or configure radio settings for 2.4 GHz and the 5 GHz radio profiles. For information on Radio, see [Configuring Radio Settings on page 258](#).

Security

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

- **Authentication Servers**—Use this tab to configure an external RADIUS server for a wireless network. For more information, see [Configuring an External Server for Authentication on page 154](#).
- **Users for Internal Server**—Use this tab to populate the system's internal authentication server with users. This list is used by networks for which per-user authorization is specified using the internal authentication server of the VC. For more information on users, see [Managing OAW-IAP Users on page 141](#).

- **Roles** —Use this tab to view the roles defined for all the Networks. The Access Rules part allows you to configure permissions for each role. For more information, see [Configuring User Roles on page 197](#) and [Configuring ACL Rules for Network Services on page 180](#).
- **Blacklisting**—Use this tab to blacklist clients. For more information, see [Blacklisting Clients on page 174](#).
- **Firewall Settings**—Use this tab to enable or disable Application Layer Gateway (ALG) supporting address and port translation for various protocols and to configure protection against wired attacks. For more information, see [Configuring ALG Protocols on page 186](#) and [Configuring Firewall Settings for Protection from ARP Attacks on page 187](#)
- **Inbound Firewall**—Use this tab to enhance the inbound firewall by allowing the configuration of inbound firewall rules, management subnets, and restricted corporate access through an uplink switch. For more information, see [Managing Inbound Traffic on page 189](#).
- **Walled Garden**—Use this tab to allow or prevent access to a selected list of websites. For more information, see [Configuring Walled Garden Access on page 139](#).
- **External Captive Portal**—Use this tab to configure external captive portal profiles. For more information, see [Configuring External Captive Portal for a Guest Network on page 127](#).
- **Custom Blocked Page URL**—Use this tab to create a list of URLs that can be blocked using an ACL rule. For more information, see [Creating Custom Error Page for Web Access Blocked by AppRF Policies on page 196](#).

Maintenance

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

- **About**—Displays the name of the product, build time, OAW-IAP model name, the AOS-W Instant version, website address of Alcatel-Lucent, and copyright information.
- **Configuration**—Displays the following details:
 - **Current Configuration**—Displays the current configuration details.
 - **Clear Configuration**—Allows you to clear the current configuration details of the network.
 - **Backup Configuration**—Allows you to back up local configuration details. The backed up configuration data is saved in the file named **instant.cfg**.
 - **Restore Configuration**—Allows you to restore the backed up configuration. After restoring the configuration, the OAW-IAP must be rebooted for the changes to take effect.
- **Certificates**—Displays information about the certificates installed on the OAW-IAP. You can also upload new certificates to the OAW-IAP database. For more information, see [Uploading Certificates on page 177](#).
- **Firmware**—Displays the current firmware version and provides various options to upgrade to a new firmware version. For more information, see [Upgrading an OAW-IAP on page 350](#).
- **Reboot**—Displays the OAW-IAPs in the network and provides an option to reboot the required OAW-IAP or all OAW-IAPs. For more information, see [Upgrading an OAW-IAP on page 350](#).
- **Convert**—Provides an option to convert an OAW-IAP to a OmniAccess WLAN Switch managed Remote AP or Campus AP, or to the default VC mode. For more information, see [Converting an OAW-IAP to a Remote AP and Campus AP on page 354](#).

More

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

- [VPN](#)
- [IDS](#)
- [Wired](#)
- [Services](#)

- DHCP Server
- Support

VPN

The **VPN** window allows you to define communication settings with an Alcatel-Lucent switch or a third party VPN concentrator. See [VPN Configuration on page 226](#) for more information. The following figure shows an example of the IPsec configuration options available in the **VPN** window:

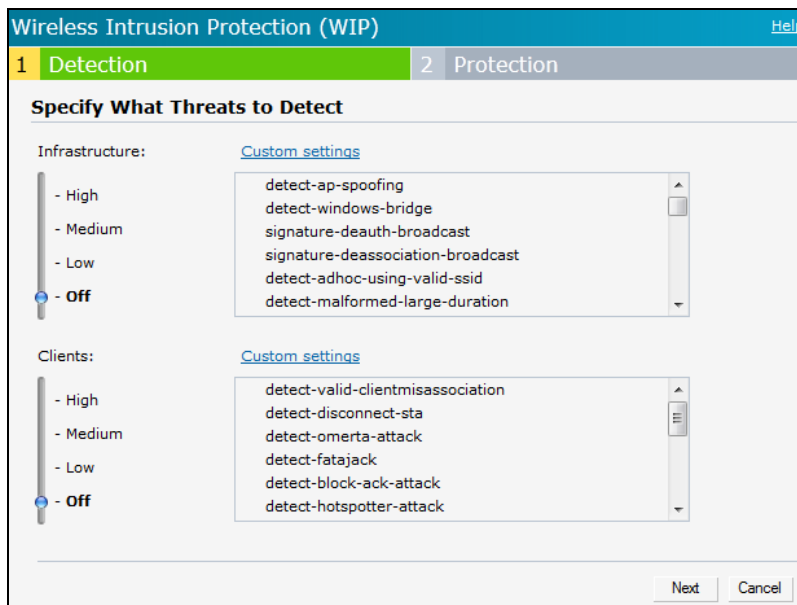
Figure 5 VPN Window for IPsec Configuration



IDS

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

Figure 6 IDS Window: Intrusion Detection



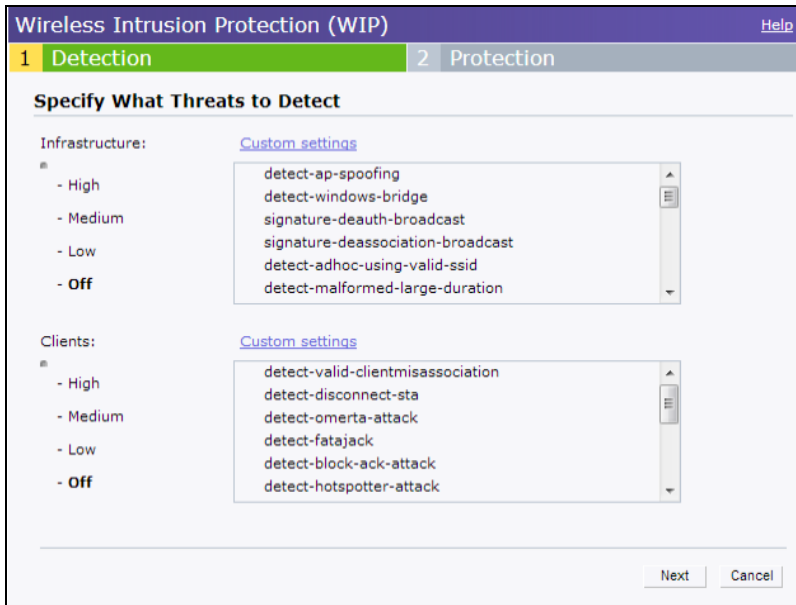
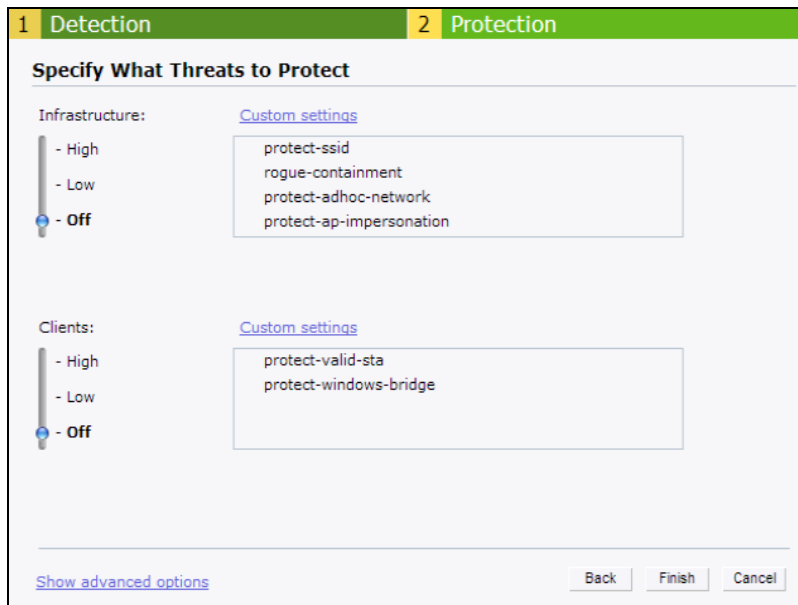


Figure 7 IDS Window: Intrusion Protection

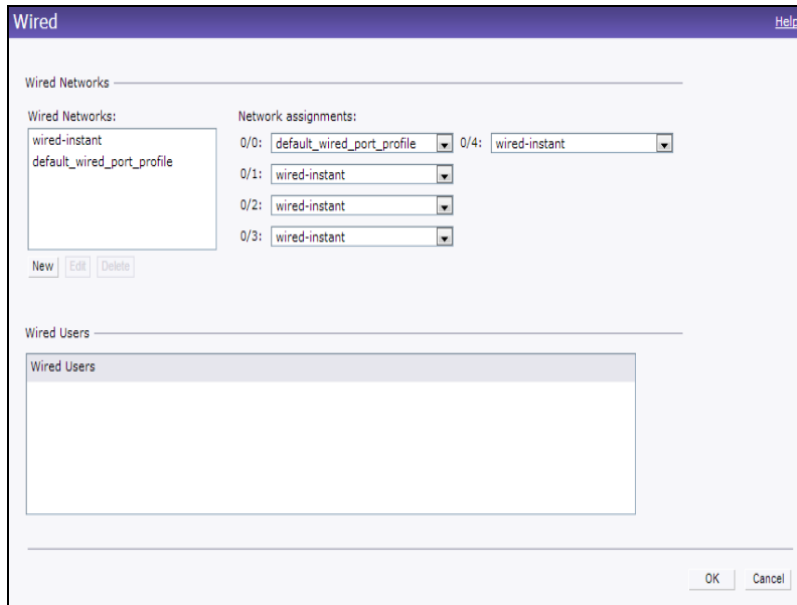


For more information on wireless intrusion detection and protection, see [Detecting and Classifying Rogue OAW-IAPs on page 329](#).

Wired

The **Wired** window allows you to configure a wired network profile. See [Wired Profiles on page 106](#) for more information. The following figure shows the **Wired** window:

Figure 8 *Wired Window*



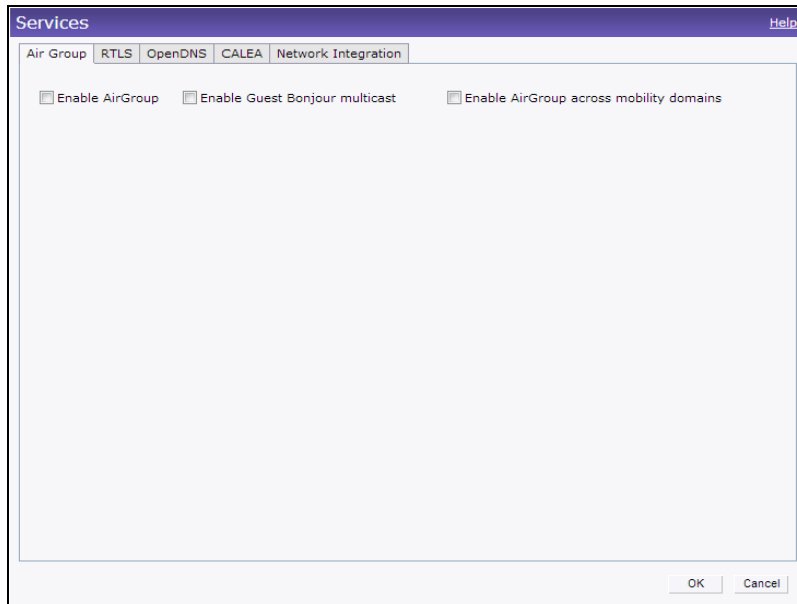
Services

The **Services** window allows you to configure services such as AirGroup, Real Time Location System (RTLS), and OpenDNS. The Services window consists of the following tabs:

- **AirGroup**—Allows you to configure the AirGroup and AirGroup services. For more information, see [Configuring AirGroup on page 281](#).
- **RTLS**—Allows you to integrate AMP or third-party RTLS such as Aeroscout Real Time Location Server with AOS-W Instant. For more information, see [Configuring an OAW-IAP for RTLS Support on page 290](#).
The RTLS tab also allows you to integrate OAW-IAP with the Analytics and Location Engine (ALE). For more information about configuring an OAW-IAP for ALE integration, see [Configuring an OAW-IAP for Analytics and Location Engine Support on page 291](#).
- **OpenDNS**—Allows you to configure support for OpenDNS business solutions, which require an OpenDNS (www.opendns.com) account. The OpenDNS credentials are used by AOS-W Instant and OmniVista to filter content at the enterprise level. For more information, see [Configuring OpenDNS Credentials on page 295](#).
- **CALEA**—Allows you configure support for Communications Assistance for Law Enforcement Act (CALEA) server integration, thereby ensuring compliance with Lawful Intercept and CALEA specifications. For more information, see [CALEA Integration and Lawful Intercept Compliance on page 300](#).
- **Network Integration**—Allows you to configure an OAW-IAP for integration with Palo Alto Networks (PAN) Firewall and XML API server. For more information on OAW-IAP integration with PAN, see [Integrating an OAW-IAP with Palo Alto Networks Firewall on page 295](#) and [Integrating an OAW-IAP with an XML API Interface on page 297](#).

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

Figure 9 *Services Window: Default View*



DHCP Server

The **DHCP Servers** window allows you to configure various DHCP modes. The following figure shows the options available in the **DHCP Servers** window:

Figure 10 *DHCP Servers Window*

For more information, see [DHCP Configuration on page 209](#).

Support

The **Support** link consists of the following details:

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

For more information on support commands, see [Running Debug Commands on page 368](#).

Help

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


To activate the context-sensitive help:

1. Click the **Help** link available above the Search bar on the AOS-W Instant main window.
2. Click any text or term displayed in green italics to view its description or definition.
3. To disable the help mode, click **Done**.

Logout

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

Monitoring

The **Monitoring** link displays the Monitoring pane for the AOS-W Instant network. Use the down arrow  located to the right side of these links to compress or expand the Monitoring pane.

The Monitoring pane consists of the following sections:

- [Info](#)
- [RF Dashboard](#)
- [RF Trends](#)
- [Usage Trends](#)
- [Mobility Trail](#)

Info

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

Table 10: Contents of the Info Section in the AOS-W Instant Main Window

Name	Description
<p>Info section in the Virtual Controller view</p>	<p>The Info section in the Virtual Controller view displays the following information:</p> <ul style="list-style-type: none"> ● Name—Displays the VC name. ● Country Code—Displays the Country in which the VC is operating. ● Virtual Controller IP address—Displays the IP address of the VC. ● VC DNS—Displays the DNS IP address configured for the VC. ● Management—Indicates if the OAW-IAP is managed locally or through OmniVista. ● Master—Displays the IP address of the OAW-IAP acting as VC. ● OpenDNS Status—Displays the OpenDNS status. If the OpenDNS status indicates Not Connected, ensure that the network connection is up and appropriate credentials are configured for OpenDNS. ● MAS integration—Displays the status of the Mobility Access Switch (MAS) integration feature. ● Uplink type—Displays the type of uplink configured on the OAW-IAP, for example, Ethernet or 3G. ● Uplink status—Indicates the uplink status. ● Blacklisted clients—Displays the number of blacklisted clients. ● Internal RADIUS Users—Displays the number of internal RADIUS users. ● Internal Guest Users—Displays the number of internal guest users. ● Internal User Open Slots—Displays the available slots for user configuration as supported by the OAW-IAP model.
<p>Info section in the Network view</p>	<p>The Info section in the Network view displays the following information:</p> <ul style="list-style-type: none"> ● Name—Displays the name of the network. ● Status—Displays the status of the network. ● Type—Displays the type of network, for example, Employee, Guest, or Voice. ● VLAN—Displays VLAN details. ● IP Assignment—Indicates if the OAW-IAP clients are assigned IP address from the network that the VC is connected to, or from an internal autogenerated IP scope from the VC. ● Access—Indicates the level of access control configured for the network. ● WMM DSCP—Displays Wi-Fi Multimedia (WMM) DSCP mapping details. ● Security level—Indicates the type of user authentication and data encryption configured for the network. <p>The info section for WLAN SSIDs also indicates status of captive portal and CALEA ACLs and provides a link to upload certificates for the internal server. For more information, see Uploading Certificates on page 177.</p>
<p>Info section in the Access Point view</p>	<p>The Info section in the Access Point view displays the following information:</p> <ul style="list-style-type: none"> ● Name—Displays the name of the selected OAW-IAP. ● IP Address—Displays the IP address of the OAW-IAP.

Table 10: Contents of the Info Section in the AOS-W Instant Main Window

Name	Description
	<ul style="list-style-type: none"> ● Mode—Displays the mode in which the OAW-IAP is configured to operate. ● Spectrum—Displays the status of the spectrum monitor. ● Clients—Number of clients associated with the OAW-IAP. ● Type—Displays the model number of the OAW-IAP. ● Zone—Displays OAW-IAP zone details. ● CPU Utilization—Displays the CPU utilization in percentage. ● Memory Free—Displays the memory availability of the OAW-IAP in MB. ● Serial number—Displays the serial number of the OAW-IAP. ● MAC—Displays the MAC address. ● From Port—Displays the port from where the slave OAW-IAP is learned in hierarchy mode.
<p>Info section in the Client view</p>	<p>The Info section in the Client view displays the following information:</p> <ul style="list-style-type: none"> ● Name—Displays the name of the client. ● IP Address—Displays the IP address of the client. ● MAC Address—Displays MAC address of the client. ● OS—Displays the operating system that is running on the client. ● ESSID—Indicates the network to which the client is connected. ● Access Point—Indicates the OAW-IAP to which the client is connected. ● Channel—Indicates the channel that is currently used by the client. ● Type—Displays the channel type on which the client is broadcasting. ● Role—Displays the role assigned to the client.

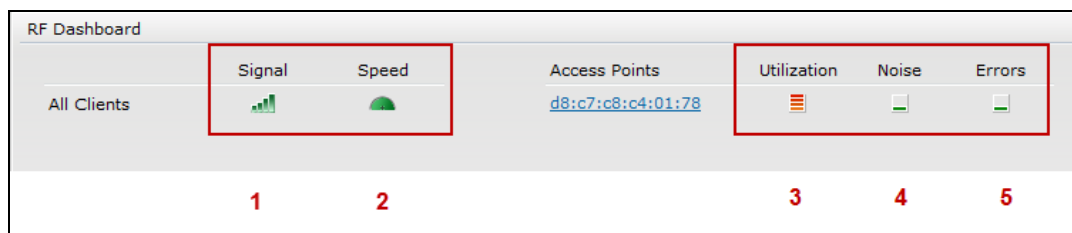
RF Dashboard

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

The OAW-IAP names are displayed as links. When an OAW-IAP is clicked, the OAW-IAP configuration information is displayed in the Info section and the RF Dashboard section is displayed on the AOS-W Instant main window.

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

Figure 11 RF Dashboard in the Monitoring Pane



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

Table 11: RF Dashboard Icons

Icon number	Name	Description
1	Signal	<p>Displays the signal strength of the client. Signal strength is measured in decibels. Depending on the signal strength of the client, the color of the lines on the Signal icon changes in the following order:</p> <ul style="list-style-type: none">• Green—Signal strength is more than 20 dB.• Orange—Signal strength is between 15 dB and 20 dB.• Red—Signal strength is less than 15 dB. <p>To view the signal graph for a client, click the signal icon next to the client in the Signal column.</p>
2	Speed	<p>Displays the data transfer speed of the client. Depending on the data transfer speed of the client, the color of the Speed icon changes in the following order:</p> <ul style="list-style-type: none">• Green—Data transfer speed is more than 50% of the maximum speed supported by the client.• Orange—Data transfer speed is between 25% and 50% of the maximum speed supported by the client.• Red—Data transfer speed is less than 25% of the maximum speed supported by the client. <p>To view the data transfer speed graph of a client, click the speed icon corresponding to the client name in the Speed column.</p>
3	Utilization	<p>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 in the following order:</p> <ul style="list-style-type: none">• Green—Utilization is less than 50%.• Orange—Utilization is between 50% and 75%.• Red—Utilization is more than 75%. <p>To view the utilization graph of an OAW-IAP, click the Utilization icon next to the OAW-IAP in the Utilization column.</p>

Table 11: RF Dashboard Icons

Icon number	Name	Description
4	Noise	<p>Displays the noise floor details for the OAW-IAPs. Noise is measured in decibels/meter. Depending on the noise floor, the color of the lines on the Noise icon changes in the following order:</p> <ul style="list-style-type: none"> Green—Noise floor is more than -87 dBm. Orange—Noise floor is between -80 dBm and -87 dBm. Red—Noise floor is less than -80 dBm. <p>To view the noise floor graph of an OAW-IAP, click the Noise icon next to the OAW-IAP in the Noise column.</p>
5	Errors	<p>Displays the errors for the OAW-IAPs. Depending on the errors, color of the lines on the Errors icon changes in the following order:</p> <ul style="list-style-type: none"> Green—Errors are less than 5000 frames per second. Orange—Errors are between 5000 and 10,000 frames per second. Red—Errors are more than 10000 frames per second. <p>To view the errors graph of an OAW-IAP, click the Errors icon next to the OAW-IAP in the Errors column.</p>

RF Trends

The **RF Trends** section displays the following graphs for the selected OAW-IAP and the client. To view the details on the graphs, click the graphs and hover the mouse on a data point:

Figure 12 RF Trends for Access Point

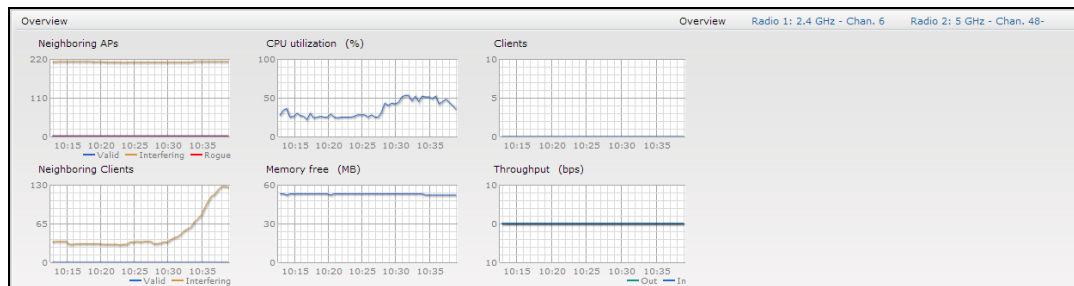
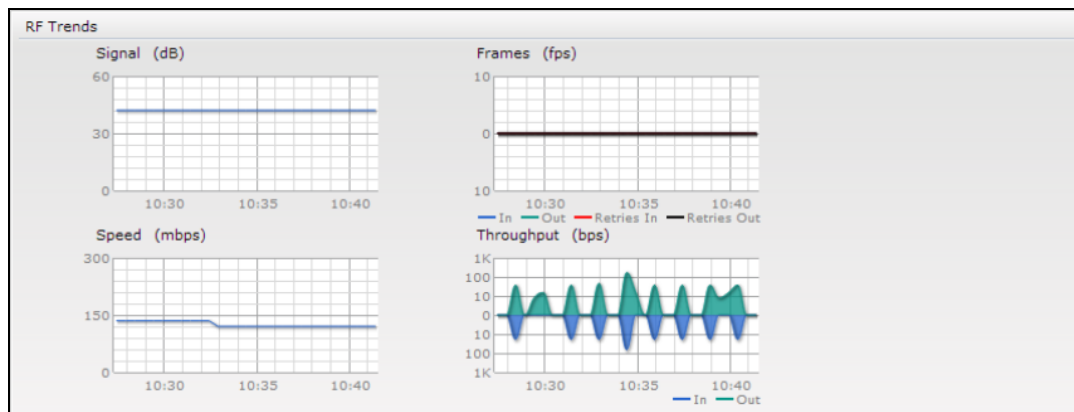


Figure 13 RF Trends for Clients



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

Table 12: 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. The enlarged view provides Last, Minimum, Maximum, and Average signal statistics of the client for the last 15 minutes.</p> <p>To see the exact signal strength at a particular time, move 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"> 1. Log in to the AOS-W Instant UI. The Virtual Controller view is displayed. This is the default view. 2. On the Clients tab, click the IP address of the client for which you want to monitor the signal strength. 3. Study the Signal graph in the RF Trends pane. For example, the graph shows that signal strength for the client is 54.0 dB at 12:23 hours.
Frames	<p>The Frames graph shows the In and Out frame rate per second of the client for the last 15 minutes. It also shows data for the Retry In and Retry Out frames.</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 are displayed above the median line in black . • Retry In—Retries for the incoming frames are displayed below the median line in red. <p>To see an enlarged view, click the graph. The enlarged view provides Last, Minimum, Maximum, and Average statistics for the In, Out, Retries In, and Retries Out frames.</p> <p>To see the exact frames at a particular time, move 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"> 1. Log in to the AOS-W Instant UI. The Virtual Controller view is displayed. This is the default view. 2. On the Clients tab, click the IP address of the client for which you want to monitor the frames. 3. Study the Frames graph in the RF Trends pane. For example, the graph shows 4.0 frames per second for the client at 12:27 hours.
Speed	<p>The Speed graph shows the data transfer speed for the client. Data transfer is measured in Mbps.</p> <p>To see an enlarged view, click the graph. The enlarged view shows Last, Minimum, Maximum, and Average statistics of the client for the last 15 minutes.</p>	<p>To monitor the speed for the client for the last 15 minutes:</p> <ol style="list-style-type: none"> 1. Log in to the AOS-W Instant UI. The Virtual Controller view is displayed. This is the default view. 2. On the Clients tab, click the IP address of the client for which you want to monitor the speed. 3. Study the Speed graph in the RF Trends pane. For

Table 12: Client View—RF Trends Graphs and Monitoring Procedures

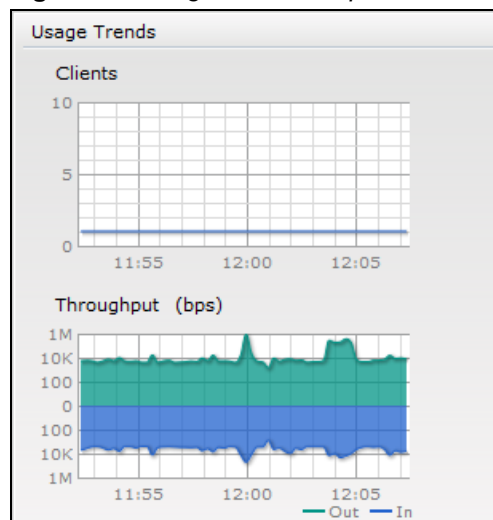
Graph Name	Description	Monitoring Procedure
	To see the exact speed at a particular time, move the cursor over the graph line.	example, the graph shows that the data transfer speed at 12:26 hours is 240 Mbps.
Throughput	<p>The Throughput Graph shows the throughput of the selected client for the last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

Usage Trends

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

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

Figure 14 Usage Trends Graphs in the Default View



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

Table 13: 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 VC for the last 15 minutes. To see the exact number of clients in the AOS-W Instant network at a particular time, move 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"> Log in to the AOS-W Instant UI. The Virtual Controller view is displayed. This is the default view. On the Network tab, click the network for which you want to check the client association. Study the Clients graph in the Usage Trends pane. For example, the graph shows that one client is associated with the selected network at 12:00 hours.
Throughput	<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 the outgoing traffic is displayed in green. Outgoing traffic is shown above the median line. Incoming traffic—Throughput for the 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, move 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 AOS-W Instant UI. The Virtual Controller view is displayed. This is the default view. On the Network tab, click the network for which you want to check the client association. Study the Throughput graph in the Usage Trends pane. For example, the graph shows 22.0 Kbps incoming traffic throughput for the selected network at 12:03 hours.

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

Table 14: Access Point View—Usage Trends and Monitoring Procedures

Graph Name	OAW-IAP Description	Monitoring Procedure
Neighboring OAW-IAPs	<p>The Neighboring OAW-IAPs graph shows the number of OAW-IAPs detected by the selected OAW-IAP:</p> <ul style="list-style-type: none"> Valid OAW-IAPs: An OAW-IAP that is part of the enterprise providing WLAN service. Interfering OAW-IAPs: An OAW-IAP that is seen in the RF environment but is not connected to the network. Rogue OAW-IAPs: An unauthorized OAW-IAP that is plugged into the wired side of the network. <p>To see the number of different types of neighboring OAW-IAPs for the last 15 minutes, move the cursor over the respective graph lines.</p>	<p>To check the neighboring OAW-IAPs detected by the OAW-IAP for the last 15 minutes:</p> <ol style="list-style-type: none"> Log in to the AOS-W Instant UI. The Virtual Controller view is displayed. This is the default view. On the Access Points tab, click the OAW-IAP for which you want to monitor the client association. Study the Neighboring OAW-IAPs graph in the Overview section. For example, the graph shows that 148 interfering OAW-IAPs are detected by the OAW-IAP at 12:04 hours.
CPU Utilization	<p>The CPU Utilization graph displays the utilization of CPU for the selected OAW-IAP.</p> <p>To see the CPU utilization of the OAW-IAP, move the cursor over the graph line.</p>	<p>To check the CPU utilization of the OAW-IAP for the last 15 minutes:</p> <ol style="list-style-type: none"> Log in to the AOS-W Instant UI. The Virtual Controller view is displayed. This is the default view. On the Access Points tab, click the OAW-IAP for which you want to monitor the client association. Study the CPU Utilization graph in the Overview pane. For example, the graph shows that the CPU utilization of the OAW-IAP is 30% at 12:09 hours.
Neighboring Clients	<p>The Neighboring Clients graph shows the number of clients not connected to the selected OAW-IAP, but heard by it.</p> <ul style="list-style-type: none"> Any client that successfully authenticates with a valid OAW-IAP and passes encrypted traffic is classified as a valid client. Interfering: A client associated to any OAW-IAP and is not valid is classified as an interfering client. <p>To see the number of different types of neighboring clients for the last 15 minutes, move the cursor over the respective graph lines.</p>	<p>To check the neighboring clients detected by the OAW-IAP for the last 15 minutes,</p> <ol style="list-style-type: none"> Log in to the AOS-W Instant UI. The Virtual Controller view is displayed. This is the default view. On the Access Points tab, click the OAW-IAP for which you want to monitor the client association. Study the Neighboring Clients graph in the Overview pane. For example, the graph shows that 20 interfering clients were detected by the OAW-IAP at 12:15 hours.
Memory free (MB)	<p>The Memory free graph displays the memory availability of the OAW-IAP in MB.</p>	<p>To check the free memory of the OAW-IAP for the last 15 minutes:</p>

Table 14: Access Point View—Usage Trends and Monitoring Procedures

Graph Name	OAW-IAP Description	Monitoring Procedure
	<p>To see the free memory of the OAW-IAP, move the cursor over the graph line.</p>	<ol style="list-style-type: none"> 1. Log in to the AOS-W Instant UI. The Virtual Controller view is displayed. This is the default view. 2. On the Access Points tab, click the OAW-IAP for which you want to monitor the client association. 3. Study the Memory free graph in the Overview pane. For example, the graph shows that the free memory of the OAW-IAP is 64 MB at 12:13 hours.
<p>Clients</p>	<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. 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> <p>To see the exact number of clients associated with the selected OAW-IAP at a particular time, move 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"> 1. Log in to the AOS-W Instant UI. The Virtual Controller view is displayed. This is the default view. 2. On the Access Points tab, click the OAW-IAP for which you want to monitor the client association. 3. Study the Clients graph. For example, the graph shows that six clients are associated with the OAW-IAP at 12:11 hours.
<p>Throughput</p>	<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 the outgoing traffic is displayed in green. It is shown above the median line. ● Incoming traffic—Throughput for the incoming 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 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, move 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"> 1. Log in to the AOS-W Instant UI. The Virtual Controller view is displayed. This is the default view. 2. On the Access Points tab, click the OAW-IAP for which you want to monitor the throughput. 3. Study the Throughput graph. For example, the graph shows 44.03 Kbps incoming traffic throughput at 12:08 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. The AOS-W Instant UI shows the client and OAW-IAP association over the last 15 minutes.
- **Access Point**—The 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.

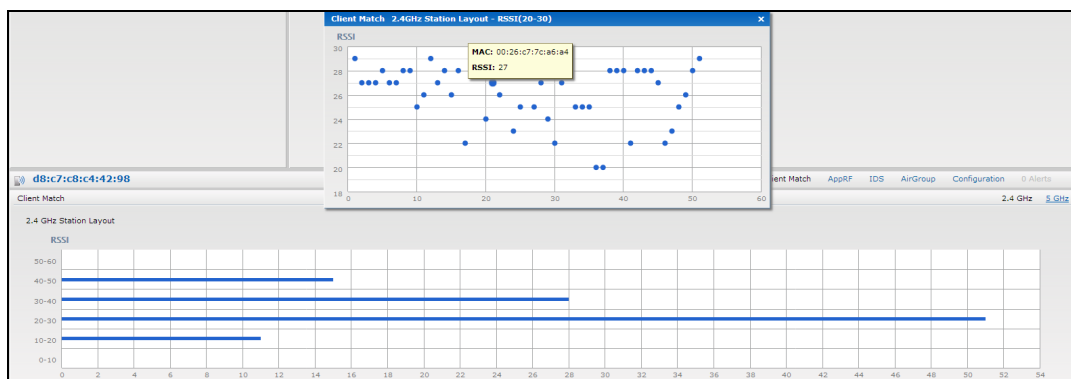
Client Match

If Client Match is enabled, the **Client Match** link provides a graphical representation of radio map view of an OAW-IAP and the client distribution on an OAW-IAP radio.

On clicking an access point in the **Access Points** tab and the **Client Match** link, a stations map view is displayed and a graph is drawn with real-time data points for the OAW-IAP radio. If the OAW-IAP supports dual-band, you can toggle between 2.4 GHz and 5 GHz links in the Client Match graph area to view the data. When you hover the mouse on the graph, details such as RSSI, Client Match status, and the client distribution on channels are displayed.

The following figure shows the client distribution details for an OAW-IAP radio.

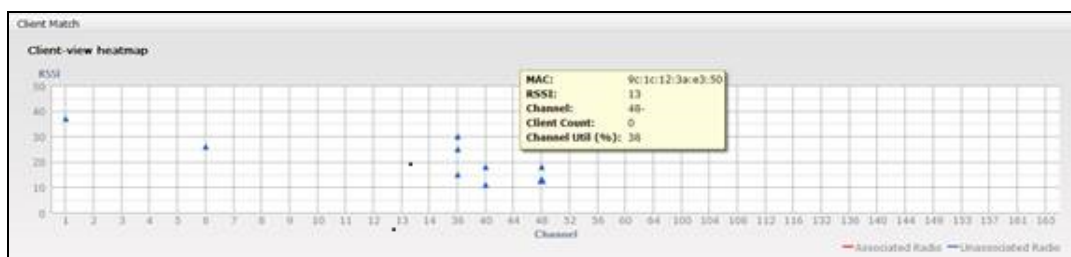
Figure 15 Client Distribution on OAW-IAP Radio



On clicking a client in the **Clients** tab and the **Client Match** link, a graph is drawn with real-time data points for an OAW-IAP radio map. When you hover the mouse on the graph, details such as RSSI, channel utilization details, and client count on each channel are displayed.

The following figure shows the client view heatmap for an OAW-IAP radio:

Figure 16 Channel Availability Map for Clients



AppRF

The **AppRF** link displays the application traffic summary for OAW-IAPs and client devices. The **AppRF** link in the activity panel is displayed only if **AppRF visibility** is enabled in the **System** window. For more information on application visibility and AppRF charts, see [Application Visibility on page 264](#).

Spectrum

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

The spectrum link displays the following:

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

For more information on spectrum monitoring, see [Spectrum Monitor on page 342](#).

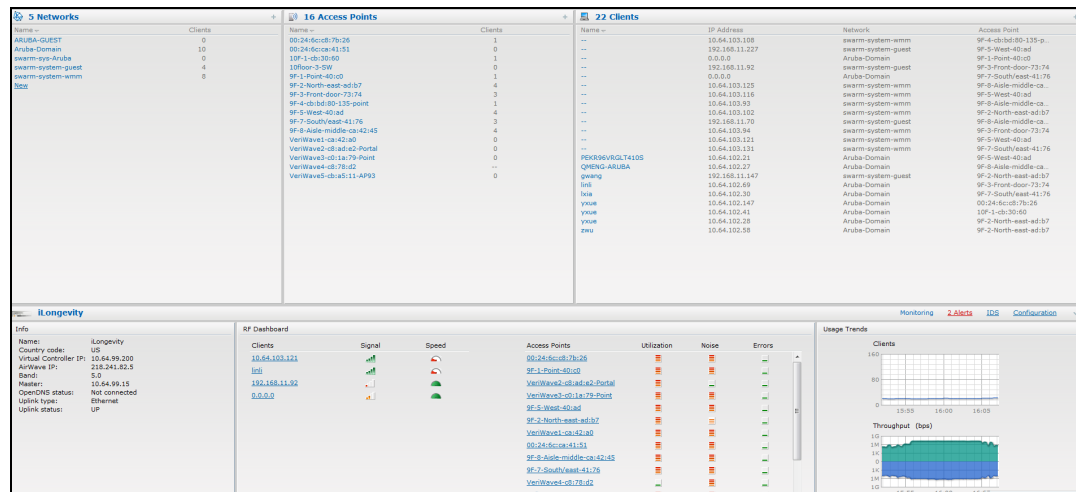
Alerts

Alerts are generated when a user encounters problems while accessing or connecting to a network. The alerts that are generated can be categorized as follows:

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

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

Figure 17 Alerts Link



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

- Client Alerts
- Active Faults
- Fault History

Table 15: Types of Alerts

Type of Alert	Description	Information Displayed
Client Alerts	The alert type, Client Alerts , occur when clients are connected to the AOS-W Instant network.	The alert type, Client Alert displays the following information: <ul style="list-style-type: none"> • Timestamp—Displays the time at which the client alert was recorded. • MAC address—Displays the MAC address of the client that 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.
Active Faults	The Active Faults alerts occur in the event of a system fault.	The Active Faults alerts consists of the following information: <ul style="list-style-type: none"> • Time—Displays the system time when an event occurs. • Number—Indicates the number of sequence. • Description—Displays the event details.
Fault History	The Fault History alerts display the historic system faults.	The Fault History alert displays the following information: <ul style="list-style-type: none"> • Time—Displays the system time when an event occurs. • Number—Indicates the number of sequence. • Cleared by—Displays the module which cleared this fault. • Description—Displays the event details.

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

Figure 18 Client Alerts

The screenshot displays the AOS-W Instant User Interface with three panels: Networks, Access Points, and Clients. Below these panels, the 'Client Alerts' section is visible, showing a table of alerts.

Name	Clients	Name	Clients	Name	IP Address
ARUBA-GUEST	0	00:24:6c:cd:7b:26	2	--	192.168.11.70
Aruba-Domain	8	00:24:6c:cd:41:51	0	--	192.168.11.227
swarm-system-aruba	0	10f:5:cd:30:50	0	--	10.64.103.110
swarm-system-guest	3	10floor-3-SW	0	--	10.64.103.102
swarm-system-wmm	9	9F-1-Point-40:ad	0	--	10.64.103.112
None		9F-2-North-east-ad:b7	5	--	10.64.103.96
		9F-3-Front-door-73:74	3	--	10.64.103.108
		9F-4-ob-bd80-135-point	1	--	0.0.0.0
		9F-5-West-40:ad	3	--	10.64.103.93
		9F-7-South/east-41:76	1	--	169.254.59.45
		9F-8-Suite-middle-ca42:45	5	--	10.64.103.121
		VerWave1-ca:45:80	0	--	10.64.103.125
		VerWave3-cb:ad:e2-Portal	0	PEKR05V/RGLT4105	10.64.32.102
		VerWave3-cd:1a:79-Point	0	QIENG-ARUBA	10.64.102.27
		VerWave4-cb:75:62	--	bob	10.64.102.30
		VerWave5-cb:a5:11-AP93	0	xxxx	192.168.11.147
				yxur	10.64.102.147
				yxur	10.64.102.41
				yxur	10.64.102.28
				zvu	10.64.102.58

Timestamp	MAC Address	Description	Access Point	Details
15:48:27	40:8f:bed:f3:ce	DHCP request timed out	9F-5-West-40:ad	more

Figure 19 Active Faults

Name	Clients	Name	Clients	Name	IP Address
ARUBA-GUEST	0	00:24:6c:cb:7b:26	2	---	192.168.11.227
Aruba-Domain	0	00:24:6c:ca:41:51	0	---	10.64.103.125
swarm-sys-Aruba	0	10F-1-cb:30:60	0	---	10.64.103.116
swarm-system-guest	3	10Floor-3-SW	0	---	10.64.103.102
swarm-system-wmm	0	9F-1-Floor-40-c0	0	---	10.64.103.94
Netx	0	9F-2-North-east-sd:b7	5	---	10.64.103.108
		9F-3-Front-door-73:74	3	---	169.254.99.45
		9F-4-cb:bd:80-135-point	1	---	0.0.0.0
		9F-5-West-40:ad	3	---	10.64.103.93
		9F-7-South/West-41:76	1	---	10.64.103.121
		9F-8-Aisle-middle-ca:42:45	4	---	192.168.11.70
		VeriWave1-ca:42:40	0	PEKRR6VRGLT410S	10.64.103.21
		VeriWave2-c8:ad:e2-Portal	0	QWENG-ARUBA	10.64.102.27
		VeriWave3-c0:1a:79-Point	0	linb	10.64.102.30
		VeriWave4-cb:78:d2	0	gwwng	192.168.11.147
		VeriWave5-cb:a5:11-AP93	0	linb	10.64.102.59
				linb	10.64.102.36
				yxue	10.64.102.147
				yxue	10.64.102.41
				yxue	10.64.102.28
				yxue	10.64.102.41
				zwx	10.64.102.58

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

Figure 20 Fault History

Name	Clients	Name	Clients	Name	IP Address
ARUBA-GUEST	0	00:24:6c:cb:7b:26	2	---	192.168.11.70
Aruba-Domain	0	00:24:6c:ca:41:51	0	---	192.168.11.227
swarm-sys-Aruba	0	10F-1-cb:30:60	0	---	10.64.103.125
swarm-system-guest	3	10Floor-3-SW	0	---	10.64.103.116
swarm-system-wmm	0	9F-1-Floor-40-c0	0	---	10.64.103.102
Netx	0	9F-2-North-east-sd:b7	5	---	10.64.103.94
		9F-3-Front-door-73:74	3	---	10.64.103.108
		9F-4-cb:bd:80-135-point	1	---	0.0.0.0
		9F-5-West-40:ad	3	---	10.64.103.93
		9F-7-South/West-41:76	1	---	169.254.99.45
		9F-8-Aisle-middle-ca:42:45	4	---	10.64.103.121
		VeriWave1-ca:42:40	0	PEKRR6VRGLT410S	10.64.103.21
		VeriWave2-c8:ad:e2-Portal	0	QWENG-ARUBA	10.64.102.27
		VeriWave3-c0:1a:79-Point	0	gwwng	192.168.11.147
		VeriWave4-cb:78:d2	0	linb	10.64.102.59
		VeriWave5-cb:a5:11-AP93	0	linb	10.64.102.36
				yxue	10.64.102.147
				yxue	10.64.102.41
				yxue	10.64.102.28
				zwx	10.64.102.58

Time	Number	Cleared By	Description
13:47:48	2	System	Access point 00:24:6c:ca:40:c0 is down
14:30:54	2	System	Access point 0b:c7:c8:cb:bd:90 is down
08:29:19	3	System	Access point 00:24:6c:c0:1a:79 is down
08:26:33	2	System	Access point 00:24:6c:c0:1a:79 is down

The following table displays a list of alerts that are generated in the OAW-IAP network:

Table 16: Alerts List

Description 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 AP's configuration.	Ascertain the correct authentication or encryption settings and try to associate again.

Table 16: Alerts List

Description Code	Description	Details	Corrective Actions
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 its 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.
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. If the OAW-IAP is using the internal RADIUS server, it is recommend to check the related configuration as well as the installed certificate and passphrase.	If the OAW-IAP is using the internal RADIUS server, Alcatel-Lucent recommends checking the related configuration as well as the installed certificate and passphrase. If the OAW-IAP is using an external RADIUS server, check if there are any issues with the RADIUS server and try connecting again.
100309	RADIUS server authentication failure	The OAW-IAP cannot authenticate this client using 802.1X, because the RADIUS server rejected the authentication credentials (for example, password) provided by the client.	Ascertain the correct authentication credentials and log in again.

Table 16: Alerts List

Description Code	Description	Details	Corrective Actions
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. Recommend checking the encryption setting on the client and on the OAW-IAP.	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. Recommend checking the status of the DHCP server in the network.	Check the status of the DHCP server in the network.
101012	Wrong Client VLAN	VLAN mismatch between the OAW-IAP and the upstream device. Upstream device can be upstream switch or RADIUS server.	

IDS

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

- **Foreign Access Points Detected**—Lists the OAW-IAPs that are not controlled by the VC. The following information is displayed for each foreign OAW-IAP:
 - **MAC address**—Displays the MAC address of the foreign OAW-IAP.
 - **Network**—Displays the name of the network to which the foreign OAW-IAP is connected.
 - **Classification**—Displays the classification of the foreign OAW-IAP, for example, Interfering OAW-IAP or Rogue OAW-IAP.
 - **Channel**—Displays the channel in which the foreign OAW-IAP is operating.
 - **Type**—Displays the Wi-Fi type of the foreign OAW-IAP.
 - **Last seen**—Displays the time when the foreign OAW-IAP was last detected in the network.
 - **Where**—Provides information about the OAW-IAP that detected the foreign OAW-IAP. Click the push pin icon to view the information.
- **Foreign Clients Detected**— Lists the clients that are not controlled by the VC. 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 Push Pin icon to view the information.

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

Figure 21 *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:82:145:72	docomo	Interfering	1	G	11:31:07	📌	00:26:c6:b7:7a:76	ethersphere-voip	Interfering	1	GN 20MZ	11:31:07	📌
00:0b:86:b6:29:31	NTT-SPOT	Interfering	1	G	11:31:07	📌	1c:b0:94:a1:9e:b6	ethersphere-wpa2	Interfering	1	GN 20MZ	11:31:07	📌
00:24:6c:80:a4:b2	docomo	Interfering	1	G	11:31:07	📌	58:94:6b:57:50:38	ethersphere-wpa2	Interfering	1	GN 20MZ	11:31:07	📌
00:24:6c:0f:9d:42	docomo	Interfering	1	G	11:31:07	📌	24:77:03:7a:67:5c	UI_Dashboard	Interfering	1	G	11:31:07	📌
00:24:6c:b0:bce:e2	docomo	Interfering	1	G	11:31:07	📌	00:14:65:30:7a:d8	ethersphere-wpa2	Interfering	1	GN 20MZ	11:30:51	📌
00:24:6c:ae:9a:d0	aruba-ap	Interfering	1	GN 20MZ	11:31:07	📌	04:46:68:8c:0d:ea	ethersphere-wpa2	Interfering	1	GN 20MZ	11:30:35	📌
00:0b:86:b6:34:b2	docomo	Interfering	1	G	11:31:07	📌	24:77:03:7a:66:ec	ip6-alpha	Interfering	1	GN 20MZ	11:30:35	📌
00:0b:86:b6:29:32	docomo	Interfering	1	G	11:31:07	📌	00:37:6d:e2:df:b2	ethersphere-voip	Interfering	1	GN 20MZ	11:30:20	📌
00:24:6c:33:0c:11	NTT-SPOT	Interfering	1	G	11:31:07	📌	00:03:2a:02:5b:b7	skvoicel1	Interfering	1	G	11:30:20	📌
ec:f3:7f:18:6d:08	hotspot_each	Interfering	157	AN 40MZ	11:31:07	📌	20:02:af:9e:6b:b5	ethersphere-wpa2	Interfering	1	GN 20MZ	11:29:34	📌
00:24:6c:33:0c:12	docomo	Interfering	1	G	11:31:07	📌	00:17:ca:ae:7a:a6	ethersphere-voip	Interfering	1	B	11:29:05	📌
ec:f3:7f:18:6d:00	nvp1	Interfering	1	GN 20MZ	11:31:07	📌	84:29:99:11:35:0d	mdns-coaming	Interfering	11	GN 20MZ	11:29:05	📌
d8:c7:c8:27:23:65	sandip-test	Interfering	11	GN 20MZ	11:31:07	📌	5c:0a:5b:13:a5:cd	ethersphere-voip	Interfering	11	GN 20MZ	11:28:50	📌
00:24:6c:0b:30:40	7SPOT	Interfering	1	GN 20MZ	11:31:07	📌	20:64:32:51:fc:3f	ip6-alpha	Interfering	1	GN 20MZ	11:27:49	📌
00:24:6c:06:82:60	7SPOT	Interfering	1	GN 20MZ	11:31:07	📌	20:64:32:81:c2:37	ethersphere-wpa2	Interfering	1	BN 20MZ	11:23:34	📌
00:24:6c:80:4b:f1	ARUBA-VISITOR	Interfering	1	GN 20MZ	11:31:07	📌	58:94:6b:31:c1:00	mdns-coaming	Interfering	11	B	11:21:49	📌
00:0b:86:70:4b:61	san-mdns-psk	Interfering	1	GN 20MZ	11:31:07	📌	00:16:6f:31:88:8a	UI_Dashboard	Interfering	6	G	11:18:18	📌
d8:c7:c8:27:23:3c:2	Milford_Staff	Interfering	1	GN 20MZ	11:31:07	📌	00:26:c6:be:68:b8	ethersphere-voip	Interfering	8	GN 20MZ	11:18:18	📌

For more information on the intrusion detection feature, see [Intrusion Detection on page 329](#).

AirGroup

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

- **MAC**—Displays the MAC address of the AirGroup servers.
- **IP**—Displays the IP address of the AirGroup servers.
- **Host Name**—Displays the machine name or host name of the AirGroup servers.
- **Service**— Displays the type of services such as AirPlay or AirPrint.
- **VLAN**—Displays VLAN details of the AirGroup servers.
- **Wired/Wireless**—Displays if the AirGroup server is connected through a wired or wireless interface.
- **Role**—Displays the user role if the server is connected through 802.1X authentication. If the server is connected through Phase-Shift Keying (PSK) or open authentication, this parameter is blank.
- **Group**—Displays the group.
- **CPPM**—By clicking this, you get details of the registered rules in ClearPass Policy Manager (CPPM) for this server.
- **MDNS Cache**—By clicking this, you receive MDNS record details of a particular server.

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

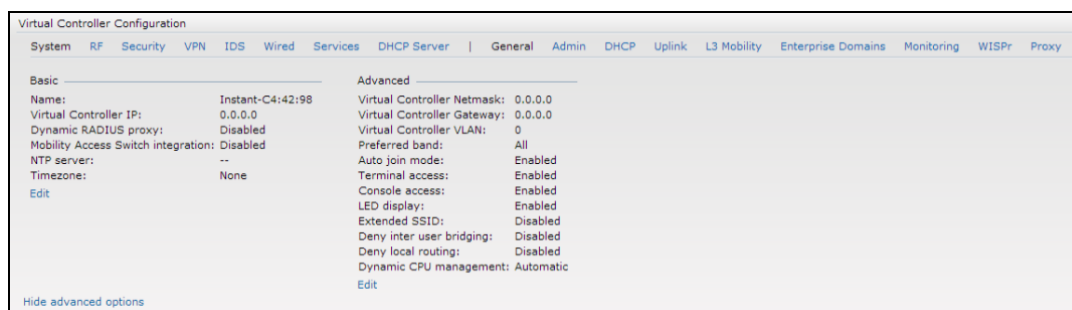
Figure 22 *AirGroup Link*

MAC	IP	Host Name	Service	VLAN	Wired/Wireless	Role	Username	AP Name	CPPI
00:20:7b:05:3e:89	172.16.22.245	wmccz	airplay	22	Wireless			08:c7:c8:0b:43:82	📌
00:20:7b:05:18:04	172.16.22.249	Family-Room-Apple-TVairplay		22	Wireless			08:c7:c8:0b:43:82	📌
d4:ee:07:98:ed:0a	172.16.31.202	EPIC@BREDNA	airprint	18	Wireless			24:6a:c6:0b:07:37	📌

Configuration

The **Configuration** link provides an overall view of your VC, OAW-IAPs, and WLAN SSID configuration. The following figure shows the VC configuration details displayed on clicking the **Configuration** link.

Figure 23 Configuration Link



OmniVista 3600 Setup

OmniVista is a solution for managing rapidly changing wireless networks. When enabled, OmniVista allows you to manage the AOS-W Instant network. For more information on OmniVista, see [Managing an OAW-IAP from OmniVista on page 309](#). The OmniVista status is displayed below the Virtual Controller section of the AOS-W Instant main window. If the OmniVista status is **Not Set Up**, click the **Set Up Now** link to configure OmniVista. The **System > Admin** window is displayed.

Pause/Resume

The **Pause/Resume** link is located on the AOS-W Instant main window.

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

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

Views

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

- **Virtual Controller** view—The VC view is the default view. This view allows you to monitor the AOS-W Instant network.
- The following AOS-W Instant UI elements are available in this view:
 - **Tabs**—Networks, Access Points, and Clients. For detailed information on the tabs, see [Tabs on page 30](#).
 - **Links**—Monitoring, Client Alerts, and IDS. The Spectrum link is visible if you have configured the OAW-IAP as a spectrum monitor. These links allow you to monitor the AOS-W Instant network. For more information on these links, see [Monitoring on page 39](#), [IDS on page 54](#), [Alerts on page 50](#), and [Spectrum Monitor on page 342](#).
- **Network** view—The Network view provides information that is necessary to monitor a selected wireless network. All Wi-Fi networks in the AOS-W Instant network are listed in the **Network** tab. Click the name of the network that you want to monitor.
- AOS-W Instant Access Point view—The AOS-W Instant Access Point view provides information that is necessary to monitor a selected OAW-IAP. All OAW-IAPs in the AOS-W Instant network are listed in the **Access Points** tab. Click the name of the OAW-IAP that you want to monitor.
- **Client** view—The Client view provides information that is necessary to monitor a selected client. In the Client view, all the clients in the AOS-W Instant network are listed in the **Clients** tab. Click the IP address of the client that you want to monitor.

For more information on the graphs and the views, see [Monitoring on page 39](#).

This chapter consists of the following sections:

- [Configuring System Parameters on page 58](#)
- [Changing Password on page 64](#)

Configuring System Parameters

This section describes how to configure the system parameters of an OAW-IAP.

To configure system parameters:

1. Select **System**.

Table 17: *System Parameters*

Parameter	Description	CLI Configuration
Name	Name of the OAW-IAP.	(Instant AP) # name <name>
System location	Physical location of the OAW-IAP.	(Instant AP) # (config) # syslocation <location-name>
Virtual Controller IP	This parameter allows you to specify a single static IP address that can be used to manage a multi-OAW-IAP AOS-W Instant network. This IP address is automatically provisioned on a shadow interface on the OAW-IAP that takes the role of a VC. When an OAW-IAP becomes a VC, it sends three Address Resolution Protocol (ARP) messages with the static IP address and its MAC address to update the network ARP cache.	(Instant AP) (config) # virtual- controller-ip <IP- address>
Allow IPv6 Management	Select the check box to enable IPv6 configuration	
Virtual Controller IPv6	This parameter is used to configure the IPv6 address.	(Instant AP) (config) # virtual- controller-ipv6 <ipv6 address>
Uplink switch native VLAN	This parameter notifies the OAW-IAP about the native-VLAN of the upstream switch to which the OAW-IAP is connected. The parameter stops the OAW-IAP from sending out tagged frames to clients connected with the SSID that has the same VLAN as the native VLAN of the upstream switch, to which the OAW-IAP is connected. By default, the OAW-IAP considers the uplink switch native VLAN value as 1.	(Instant AP) (config) # enet-vlan <vlan- ID>

Table 17: System Parameters

Parameter	Description	CLI Configuration
Dynamic Proxy	<p>This parameter allows you to enable or disable the dynamic proxy for RADIUS and Terminal Access Controller Access Control System (TACACS) servers.</p> <ul style="list-style-type: none"> Dynamic RADIUS proxy—When dynamic RADIUS proxy is enabled, the VC network will use the IP address of the VC for communication with external RADIUS servers. Ensure that you set the VC IP address as a Network Access Server (NAS) client in the RADIUS server if Dynamic RADIUS proxy is enabled. Dynamic TACACS proxy—When enabled, the VC network will use the IP address of the VC for communication with external TACACS servers. The IP address is chosen based on one of the following rules: <ul style="list-style-type: none"> If a VPN tunnel exists between the OAW-IAP and the TACACS server, then the IP address of the tunnel interface will be used. If a VC IP address is configured, the the same will be used by the VC network to communicate with the external TACACS server. If a VC IP is not configured, then the IP address of the bridge interface is used. <p>NOTE: When dynamic-tacacs-proxy is enabled on the OAW-IAP, the TACACS server cannot identify the slave OAW-IAP that generates the TACACS traffic as the source IP address is changed.</p>	<p>To enable dynamic RADIUS proxy:</p> <pre>(Instant AP) (config) # dynamic-radius-proxy</pre> <p>To enable TACACS proxy:</p> <pre>(Instant AP) (config) # dynamic-tacacs-proxy</pre>
NTP Server	<p>This parameter allows you to configure NTP server. To facilitate communication between various elements in a network, time synchronization between the elements and across the network is critical. Time synchronization allows you to:</p> <ul style="list-style-type: none"> Trace and track security gaps, monitor network usage, and troubleshoot network issues. Validate certificates. Map an event on one network element to a corresponding event on another. Maintain accurate time for billing services and similar tasks. 	<p>To configure an NTP server:</p> <pre>(Instant AP) (config) # ntp-server <name></pre>

Table 17: System Parameters

Parameter	Description	CLI Configuration
	<p>NTP helps obtain the precise time from a server and regulate the local time in each network element. Connectivity to a valid NTP server is required to synchronize the OAW-IAP clock to set the correct time. If NTP server is not configured in the OAW-IAP network, an OAW-IAP reboot may lead to variation in time data.</p> <p>By default, the OAW-IAP tries to connect to pool.ntp.org to synchronize time. The NTP server can also be provisioned through the DHCP option 42. If the NTP server is configured, it takes precedence over the DHCP option 42 provisioned value. The NTP server provisioned through the DHCP option 42 is used if no server is configured. The default server pool.ntp.org is used if no NTP server is configured or provisioned through DHCP option 42.</p> <p>NOTE: To facilitate zero-touch provisioning using the AMP or Activate, you must configure the firewall and wired infrastructure to either allow the NTP traffic to pool.ntp.org, or provide alternative NTP servers under DHCP options.</p>	
Timezone	<p>Timezone in which the OAW-IAP must operate. You can also enable daylight saving time (DST) on OAW-IAPs if the time zone you selected supports the daylight saving time. When enabled, the DST ensures that the OAW-IAPs reflect the seasonal time changes in the region they serve.</p>	<p>To configure timezone:</p> <pre>(Instant AP) (config) # clock timezone <name> <hour-offset> <minute-offset></pre> <p>To configure daylight saving time:</p> <pre>(Instant AP) (config) # clock summer-time <timezone> recurring <start-week> <start-day> <start-month> <start-hour> <end-week> <end-day> <end-month> <end-hour></pre>
Preferred Band	<p>The preferred band for the OAW-IAP.</p> <p>NOTE: Reboot the OAW-IAP after modifying the radio profile for changes to take effect.</p>	<pre>(Instant AP) (config) # rf-band <band></pre>
AppRF Visibility	<p>Select one of the following options from the AppRF visibility drop-down list.</p> <ul style="list-style-type: none"> ● App—Displays only inbuilt Deep Packet Inspection (DPI) data. ● WebCC—Displays the DPI data hosted on the 	<pre>(Instant AP) (config) # dpi</pre>

Table 17: System Parameters

Parameter	Description	CLI Configuration
	<p>cloud.</p> <ul style="list-style-type: none"> • All—Displays both App and WebCC DPI data. • None—Does not display any AppRF content. 	
URL Visibility	Select Enabled or Disabled from the URL visibility drop-down list.	(Instant AP) (config) # url-visibility
Cluster security	<p>Select Enabled to ensure that the control plane messages between access points are secured. This option is disabled by default.</p> <p>NOTE: The Cluster security setting can be enabled only if the default NTP server or a static NTP server is reachable.</p>	(Instant AP) (config) # cluster-security
Virtual Controller network settings	<p>If the VC IP address is in the same subnet as the OAW-IAP, ensure that you select Custom from the Virtual Controller network settings drop-down list and configure the following details:</p> <ul style="list-style-type: none"> • Virtual Controller Netmask—Enter subnet mask details. • Virtual Controller Gateway—Enter a gateway address. • Virtual Controller DNS—If the DNS IP address is configured for a master OAW-IAP, the DNS IP settings are synchronized for all APs in an OAW-IAP cluster. <ul style="list-style-type: none"> • If the DNS IP address is configured for an OAW-IAP as part of the per OAW-IAP setting (Edit Access Point > General), it takes precedence over the VC DNS IP address defined in the System > General window. • If the OAW-IAPs are not explicitly assigned a DNS IP address, the DNS IP address defined in System > General takes precedence. • If the DNS IP address is not defined for OAW-IAPs or VC, the DNS address dynamically assigned from the DHCP server is used. • Virtual Controller VLAN—Ensure that the VLAN defined for the VC is not the same as the native VLAN of the OAW-IAP. <p>VC VLAN, gateway, and subnet mask details.</p>	<pre>(Instant AP) (config) # virtual- controller-dnsip <addr> (Instant AP) (config) # virtual- controller-vlan <vcvlan> <vcmask> <vcgw></pre>

Table 17: System Parameters

Parameter	Description	CLI Configuration
Auto join mode	<p>The Auto-Join feature allows OAW-IAPs to automatically discover the VC and join the network. The Auto-Join feature is enabled by default. If the Auto-Join feature is disabled, a link is displayed in the Access Points tab indicating that there are new OAW-IAPs discovered in the network. Click this link if you want to add these OAW-IAPs to the network.</p> <p>When Auto-Join feature is disabled, the inactive OAW-IAPs are displayed in red.</p>	<p>To disable auto-join mode:</p> <pre>(Instant AP) (config) # no allow-new-aps</pre> <p>To enable auto-join mode:</p> <pre>(Instant AP) (config) # allow-new-aps</pre>
Terminal access	<p>When terminal access is enabled, you can access the OAW-IAP CLI through SSH.</p> <p>The terminal access is enabled by default</p>	<pre>(Instant AP) (config) # terminal-access</pre>
Console access	<p>When enabled, you can access the OAW-IAP through the console port.</p>	<pre>(Instant AP) (config) # console</pre>
Telnet server	<p>To start a Telnet session with the OAW-IAP CLI, enable access to the Telnet server.</p>	<pre>(Instant AP) (config) # telnet-server</pre>
LED display	<p>LED display status of the OAW-IAP. To enable or disable LED display for all OAW-IAPs in a cluster, select Enabled or Disabled, respectively.</p> <p>NOTE: The LEDs are always enabled during the OAW-IAP reboot.</p>	<pre>(Instant AP) (config) # led-off</pre>
Extended SSID	<p>Extended SSID is enabled by default in the factory default settings of OAW-IAPs. This disables mesh in the factory default settings.</p> <ul style="list-style-type: none"> The OAW-RAP108/109 access points support up to 6 SSIDs with Extended SSID disabled and up to 8 SSIDs with Extended SSID enabled. All other OAW-IAPs support up to 14 SSIDs when Extended SSID is disabled and up to 16 SSIDs with Extended SSID enabled. 	<pre>(Instant AP) (config) # extended-ssid</pre>
Deny inter user bridging	<p>If you have security and traffic management policies defined in upstream devices, you can disable bridging traffic between two clients connected to the same OAW-IAP on the same VLAN. When inter user bridging is denied, the clients can connect to the Internet but cannot communicate with each other, and the bridging traffic between the clients is sent to the upstream device to make the forwarding decision.</p> <p>By default, the Deny inter user bridging parameter is disabled.</p>	<pre>(Instant AP) (config) # deny-inter-user-bridging</pre> <p>To disable inter-user bridging for the WLAN SSID clients:</p> <pre>(Instant AP) (config) # wlan ssid-profile <ssid-profile></pre>

Table 17: System Parameters

Parameter	Description	CLI Configuration
		<pre>(Instant AP) (SSID Profile <ssid- profile>) # deny- inter-user-bridging</pre>
Deny local routing	<p>If you have security and traffic management policies defined in upstream devices, you can disable routing traffic between two clients connected to the same OAW-IAP on different VLANs. When local routing is disabled, the clients can connect to the Internet but cannot communicate with each other, and the routing traffic between the clients is sent to the upstream device to make the forwarding decision.</p> <p>By default, the Deny local routing parameter is disabled.</p>	<pre>(Instant AP) (config) # deny-local-routing</pre>
Dynamic CPU Utilization	<p>OAW-IAPs perform various functions such as wired and wireless client connectivity and traffic flows, wireless security, network management, and location tracking. If an OAW-IAP is overloaded, it prioritizes the platform resources across different functions. Typically, the OAW-IAPs manage resources automatically in real time. However, under special circumstances, if dynamic resource management needs to be enforced or disabled altogether, the dynamic CPU management feature settings can be modified.</p> <p>To configure dynamic CPU management, select any of the following options from DYNAMIC CPU UTILIZATION.</p> <ul style="list-style-type: none"> ● Automatic—When selected, the CPU management is enabled or disabled automatically during runtime. This decision is based on real-time load calculations taking into account all different functions that the CPU needs to perform. This is the default and recommended option. ● Always Disabled in all APs—When selected, this setting disables CPU management on all OAW-IAPs, typically for small networks. This setting protects user experience. ● Always Enabled in all APs—When selected, the client and network management functions are protected. This setting helps in large networks with high client density. 	<pre>(Instant AP) (config) # dynamic-cpu-mgmt</pre>

Changing Password

You can update your password details by using the AOS-W Instant UI or the CLI.

In the AOS-W Instant UI

To change the admin user password:

1. Navigate to **System > Admin**.
2. Under **Local**, provide a new password that you would like the admin users to use.
3. Click **OK**.

In the CLI

To change the admin user password:

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

Hashing of Management User Password

Starting from AOS-W Instant 6.5.0.0-4.3.0.0, all the management user passwords can be stored and displayed as hash instead of plain text. Hashed passwords are more secure as they cannot be converted back to plain text format.

Upgrading to the AOS-W Instant 6.5.0.0-4.3.0.0 version will not automatically enable hashing of management user passwords, as this setting is optional. Users can choose if management passwords need to be stored and displayed as hash, or if the passwords need to remain in encrypted format.

This setting is enabled by default on factory reset OAW-IAPs running AOS-W Instant 6.5.0.0-4.3.0.0 onwards, and is applicable to all OAW-IAPs in the cluster.

Hashing of the management user password can be configured by using either the AOS-W Instant UI or the CLI.

In the AOS-W Instant UI

To set the management password in hash format:

1. Navigate to **System > Admin**.
2. Click the **show advanced options** link.
3. Select the **Hash Management Password** check box. This will enable the hashing of the management user password.

The check box will appear grayed out after this setting is enabled, as this setting cannot be reversed.

In the CLI

The following example enables the hashing of a management user password:

```
(Instant AP) (config)# hash-mgmt-password
(Instant AP) (config)# end
(Instant AP)# commit apply
```

The following example adds a management user with read-only privilege:

```
(Instant AP) (config)# hash-mgmt-user john password cleartext password01 usertype read-only
(Instant AP) (config)# end
(Instant AP)# commit apply
```

The following examples removes a management user with read-only privilege:

```
(Instant AP) (config)# no hash-mgmt-user read-only
(Instant AP) (config)# end
(Instant AP)# commit apply
```


This chapter describes the procedures for configuring settings that are specific to an OAW-IAP in the cluster.

- [Modifying the OAW-IAP Host Name on page 65](#)
- [Configuring Zone Settings on an OAW-IAP on page 65](#)
- [Specifying a Method for Obtaining IP Address on page 66](#)
- [Configuring External Antenna on page 67](#)
- [Configuring Radio Profiles for an OAW-IAP on page 68](#)
- [Configuring Uplink VLAN for an OAW-IAP on page 70](#)
- [Changing the OAW-IAP Installation Mode on page 70](#)
- [Changing USB Port Status on page 71](#)
- [Master Election and Virtual Controller on page 72](#)
- [Adding an OAW-IAP to the Network on page 73](#)
- [Removing an OAW-IAP from the Network on page 74](#)

Modifying the OAW-IAP Host Name

You can change the host name of an OAW-IAP through the AOS-W Instant UI or the CLI.

In the AOS-W Instant UI

To change the host name:

1. On the **Access Points** tab, click the OAW-IAP you want to rename.
2. Click the **edit** link.
3. Edit the OAW-IAP name in **Name**. You can specify a name of up to 32 ASCII characters.
4. Click **OK**.

In the CLI

To change the name:

```
(Instant AP)# hostname <name>
```

Configuring Zone Settings on an OAW-IAP

All OAW-IAPs in a cluster use the same SSID configuration including master and slave OAW-IAPs. However, if you want to assign an SSID to a specific OAW-IAP, you can configure zone settings for an OAW-IAP.

The following constraints apply to the OAW-IAP zone configuration:

- An OAW-IAP can belong to only one zone and only one zone can be configured on an SSID.
- If an SSID belongs to a zone, all OAW-IAPs in this zone can broadcast this SSID. If no OAW-IAP belongs to the zone configured on the SSID, the SSID is not broadcast.
- If an SSID does not belong to any zone, all OAW-IAPs can broadcast this SSID.

You can add an OAW-IAP zone by using the UI or the CLI.



For the SSID to be assigned to an OAW-IAP, the same zone details must be configured on the SSID. For more information on SSID configuration, see [Configuring WLAN Settings for an SSID Profile on page 80](#).

In the AOS-W Instant UI

1. On the **Access Points** tab, click the OAW-IAP for which you want to set the zone. The **edit** link is displayed.
2. Click the **edit** link. The edit window for modifying OAW-IAP details is displayed.
3. Specify the OAW-IAP zone in **Zone**.
4. Click **OK**.

In the CLI

To change the name:

```
(Instant AP) # zone <name>
```

Specifying a Method for Obtaining IP Address

You can either specify a static IP address or allow the OAW-IAP to obtain an IP address from the DHCP server. By default, the OAW-IAPs obtain IP address from the DHCP server. You can specify a static IP address for the OAW-IAP by using the AOS-W Instant UI or the CLI.

In the AOS-W Instant UI

To configure a static IP address:

1. On the **Access Points** tab, click the OAW-IAP to modify.
2. Click the **edit** link.
3. Select **Specify statically** option to specify a static IP address. The following text boxes are displayed:
 - a. Enter a new IP address for the OAW-IAP in the **IP address** text box.
 - b. Enter the subnet mask of the network in the **Netmask** text box.
 - c. Enter the IP address of the default gateway in the **Default gateway** text box.
 - d. Enter the IP address of the DNS server in the **DNS server** text box.
 - e. Enter the domain name in the **Domain name** text box.
4. Click **OK** and reboot the OAW-IAP.

In the CLI

To configure a static IP address:

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



When IAP-VPN is not configured or IPsec tunnel to the controller is down, DNS query from the client that is associated to the master OAW-IAP is taken by DNS proxy function on the master OAW-IAP. So, if the DNS server address for the the master OAW-IAP is set (by `dnsip` or from DHCP server), the DNS query will be sent to the DNS server by the master OAW-IAP. But if the DNS server address is not set, the DNS query will not be sent by the master OAW-IAP. However, the DNS query from the client that is associated to the slave OAW-IAP is not affected to this behavior.

Configuring External Antenna

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

EIRP and Antenna Gain

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

$$\text{EIRP} = \text{Tx RF Power (dBm)} + \text{GA (dB)} - \text{FL (dB)}$$

The following table describes this formula:

Table 18: Formula Variable Definitions

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

Example

For example, the maximum gain that can be configured on an OAW-IAP with AP-ANT-1F dual-band and omnidirectional antenna is as follows:

Table 19: Maximum Antenna Gains

Frequency Band	Gain (dBi)
2.4–2.5 GHz	2.0 dBi
4.9–5.875 GHz	5.0 dBi

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

Configuring Antenna Gain

You can configure antenna gain for OAW-IAPs with external connectors by using the AOS-W Instant UI or the CLI.

In the AOS-W Instant UI

To configure the antenna gain value:

1. Navigate to the **Access Points** tab, select the OAW-IAP to configure, and then click **edit**.
2. In the **Edit Access Point** window, select **External Antenna** to configure the antenna gain value. This option is available only for access points that support external antennas,

3. Enter the antenna gain values in dBm for the 2.4 GHz and 5 GHz bands.
4. Click **OK**.

In the CLI

To configure external antenna for 5 GHz frequency:

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

To configure external antenna for 2.4 GHz frequency:

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

Configuring Radio Profiles for an OAW-IAP

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

ARM is enabled on AOS-W Instant by default. It automatically assigns appropriate channel and power settings for the OAW-IAPs. For more information on ARM, see [Adaptive Radio Management on page 251](#).

Configuring ARM-Assigned Radio Profiles for an OAW-IAP

To enable ARM-assigned radio profiles:

1. On the **Access Points** tab, click the OAW-IAP to modify.
2. Click the **edit** link.
3. Click the **Radio** tab. The **Radio** tab details are displayed.
4. Select the **Access** mode.
5. Select the **Adaptive radio management assigned** option under the bands that are applicable to the OAW-IAP configuration.
6. Click **OK**.

Configuring Radio Profiles Manually for OAW-IAP



When radio settings are assigned manually by the administrator, the ARM is disabled.

To manually configure radio settings:

1. On the **Access Points** tab, click the OAW-IAP for which you want to enable ARM.
2. Click the **edit** link.
3. Click the **Radio** tab.
4. Ensure that an appropriate mode is selected.

By default, the channel and power for an OAW-IAP are optimized dynamically using ARM. You can override ARM on the 2.4 GHz and 5 GHz bands and set the channel and power manually if desired. The following table describes various configuration modes for an OAW-IAP:

Table 20: OAW-IAP Radio Modes

Mode	Description
Access	<p>In Access mode, the OAW-IAP serves clients, while also monitoring for rogue OAW-IAPs in the background.</p> <p>If the Access mode is selected, perform the following actions:</p> <ol style="list-style-type: none"> 1. Select Administrator assigned in 2.4 GHz and 5 GHz band sections. 2. Select appropriate channel number from the Channel drop-down list for both 2.4 GHz and 5 GHz band sections. 3. Enter appropriate transmit power value in the Transmit power text box in 2.4 GHz and 5 GHz band sections.
Monitor	<p>In Monitor mode, the OAW-IAP acts as a dedicated monitor, scanning all channels for rogue OAW-IAPs and clients. You can set one radio on the Monitor mode and the other radio on the access mode, so that the clients can use one radio when the other one is in the Air Monitor mode.</p>
Spectrum Monitor	<p>In Spectrum Monitor mode, the OAW-IAP functions as a dedicated full-spectrum RF monitor, scanning all channels to detect interference, whether from the neighboring OAW-IAPs or from non-WiFi devices such as microwaves and cordless phones.</p>



In the Spectrum Monitor mode, the OAW-IAPs do not provide access services to clients.

4. Click **OK**.

In the CLI

To configure a radio profile:

```
(Instant AP) # wifi0-mode {<access> | <monitor> | <spectrum-monitor>}
(Instant AP) # wifi1-mode {<access> | <monitor> | <spectrum-monitor>}
```

If the access mode is configured, you can configure the channel and transmission power by running the following commands:

```
(Instant AP) # a-channel <channel> <tx-power>
(Instant AP) # g-channel <channel> <tx-power>
```

Configuring Maximum Clients on SSID Radio Profiles

You can also set the maximum number of clients individually for SSID profiles operating on the 2.4 GHz and 5 GHz radios. This configuration is not persistent and is lost once the OAW-IAP is rebooted.

To configure maximum clients for an SSID radio profile in the privileged exec mode:

```
(Instant AP) # a-max-clients <ssid_profile> <max-clients>
(Instant AP) # g-max-clients <ssid_profile> <max-clients>
```

To view the maximum clients allowed for an SSID profile:

```
(Instant AP) # show a-max-clients <ssid_profile>
(Instant AP) # show g-max-clients <ssid_profile>
```



You can also set the maximum clients when configuring SSID profiles using the **Max Clients Threshold** parameter in the AOS-W Instant UI and **max-clients-threshold** parameter in the AOS-W Instant CLI. For more information, see [Configuring WLAN Settings for an SSID Profile on page 80](#).

If the maximum clients setting is configured multiple times, using either the configuration mode or Privileged EXEC mode, the latest configuration takes precedence.

Configuring Uplink VLAN for an OAW-IAP

AOS-W Instant supports a management VLAN for the uplink traffic on an OAW-IAP. You can configure an uplink VLAN when an OAW-IAP needs to be managed from a non-native VLAN. After an OAW-IAP is provisioned with the uplink management VLAN, all management traffic sent from the OAW-IAP is tagged with the management VLAN.



Ensure that the native VLAN of the OAW-IAP and uplink are not the same.

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

In the AOS-W Instant UI

To configure uplink management VLAN:

1. On the **Access Points** tab, click the OAW-IAP to modify.
2. Click the **edit** link.
3. Click the **Uplink** tab.
4. Specify the VLAN in the **Uplink Management VLAN** text box.
5. Click **OK**.
6. Reboot the OAW-IAP.

In the CLI

To configure an uplink VLAN:

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

To view the uplink VLAN status:

```
(Instant AP)# show uplink-vlan
Uplink Vlan Current :0
Uplink Vlan Provisioned :1
```

Changing the OAW-IAP Installation Mode

By default, all OAW-IAP models initially ship with an indoor or outdoor installation mode. This means that OAW-IAPs with an indoor installation mode are normally placed in enclosed, protected environments and those with an outdoor installation mode are used in outdoor environments and exposed to harsh elements.

In most countries, there are different channels and power that are allowed for indoor and outdoor operation. You may want to change an OAW-IAP's installation mode from indoor to outdoor or vice versa.

In the AOS-W Instant UI

To configure the installation mode for an OAW-IAP, follow these steps:

1. Navigate to the **Access Points** tab, select the OAW-IAP to configure, and then click **edit**.

2. In the **Edit Access Point** window, select **Installation Type** to configure the installation type for the OAW-IAP you have selected.



Note that, by default, the **Default** mode is selected. This means that the OAW-IAP installation type is based on the OAW-IAP model.

3. You can either select the **Indoor** option to change the installation to Indoor mode or select the **Outdoor** option to change the installation to Outdoor mode.

the to Outdoor mode.

4. Click **OK**. A pop-up appears on the screen indicating the OAW-IAP needs to be rebooted for the changes to take effect.
5. Click **OK**.

In the CLI

To configure the Installation Type:

```
(Instant AP) # ap-installation <type[default|indoor|outdoor]>
```

To view the installation type of the OAW-IAPs:

```
(Instant AP) # show ap allowed-channels
```

Changing USB Port Status

The USB port can be enabled or disabled based on your uplink preferences. If you do not want to use the cellular uplink or 3G/4G modem in your current network setup, you can set the USB port status to disabled. By default, the USB port status is enabled.

You can change the USB port status by using the AOS-W Instant UI or the CLI.

In the AOS-W Instant UI

To change the USB port status:

1. From the **Access Points** tab, click the OAW-IAP to modify.
2. Click the **edit** link.
3. Click the **Uplink** tab.
4. Set the port status by selecting any of the following options:
 - **Disabled**—To disable the port status.
 - **Enabled**—To re-enable the port status.
5. Click **OK**.
6. Reboot the OAW-IAP.

In the CLI

To disable the USB port:

```
(Instant AP) # usb-port-disable
```

To re-enable the USB port:

```
(Instant AP) # no usb-port-disable
```

To view the USB port status:

```
(Instant AP) # show ap-env  
Antenna Type:External  
usb-port-disable:1
```

Master Election and Virtual Controller

AOS-W Instant does not require an external to regulate and manage the Wi-Fi network. Instead, one OAW-IAP in every network assumes the role of VC. It coordinates, stores, and distributes the settings required for providing a centralized functionality to regulate and manage the Wi-Fi network. The VC is the single point of configuration and firmware management. When configured, the VC sets up and manages the Virtual Private Network (VPN) tunnel in the data center.

The VC also functions like any other OAW-IAP 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 AOS-W Instant network to dynamically elect an OAW-IAP to take on a VC role and allow graceful failover to a new VC when the existing VC is not available. 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.

Preference to an OAW-IAP with 3G/4G Card

The Master Election Protocol prefers the OAW-IAP with a 3G/4G card when electing a VC for the AOS-W Instant network during the initial setup.

The VC is selected based on the following criteria:

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



OAW-IAP135 is preferred over OAW-IAP105 when a VC is elected.

Preference to an OAW-IAP with Non-Default IP

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

Viewing Master Election Details

To verify the status of an OAW-IAP and master election details, execute the following commands:

```
(Instant AP)# show election statistics  
(Instant AP)# show summary support
```

Manual Provisioning of Master OAW-IAP

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

Provisioning an OAW-IAP as a Master OAW-IAP

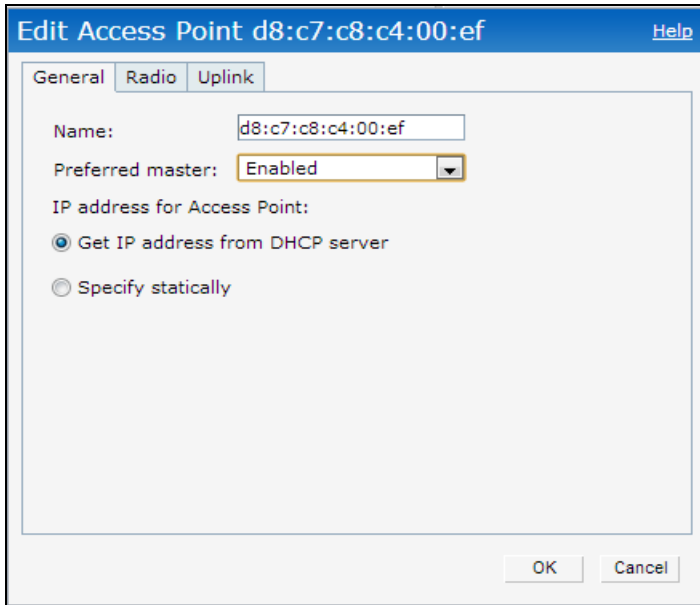
You can provision an OAW-IAP as a master OAW-IAP by using the AOS-W Instant UI or the CLI.

In the AOS-W Instant UI

To provision an OAW-IAP as a master OAW-IAP:

1. On the **Access Points** tab, click the OAW-IAP to modify.
2. Click the **edit** link.
3. Select **Enabled** from the **Preferred master** drop-down list. This option is disabled by default.

Figure 24 OAW-IAP Settings—Provisioning Master OAW-IAP



4. Click **OK**.

In the CLI

To provision an OAW-IAP as a master OAW-IAP:

```
(Instant AP) # iap-master
```

To verify if the OAW-IAP is provisioned as master OAW-IAP:

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

Adding an OAW-IAP to the Network

To add an OAW-IAP to the Instant network, assign an IP address. For more information, see [Assigning an IP address to the OAW-IAP on page 17](#).

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

If the auto-join mode is disabled, perform the following steps by using the AOS-W Instant UI.

In the AOS-W Instant UI:

To add an OAW-IAP to the network:

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

Removing an OAW-IAP from the Network

You can remove an OAW-IAP from the network by using the AOS-W Instant UI, only if the Auto-Join feature is disabled.

In the AOS-W Instant UI

To remove an OAW-IAP from the network:

1. On the **Access Points** tab, click the OAW-IAP to delete. The **x** icon is displayed beside the OAW-IAP.
2. Click **x** to confirm the deletion.



The deleted OAW-IAPs cannot join the Instant network anymore and are not displayed in the AOS-W Instant UI. However, the master OAW-IAP details cannot be deleted from the VC database.

This chapter explains the following topics:

- [VLAN Pooling](#)
- [Uplink VLAN Monitoring and Detection on Upstream Devices](#)

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

For more information on VLAN configuration for a WLAN SSID and wired port profile, see [Configuring VLAN Settings for a WLAN SSID Profile on page 85](#) and [Configuring VLAN for a Wired Profile on page 107](#), respectively.

VLAN Pooling

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

Uplink VLAN Monitoring and Detection on Upstream Devices

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

Figure 25 Uplink VLAN Detection

Instant-CC:42:39					
Client Alerts					
Timestamp	MAC address	Description	Alert ID	Severity	Action
2013/11/11 11:50:30	b4:b6:76:42:6d:05	Wrong Client VLAN	6c:f3:7f:c4:42:ce	more	
2013/11/11 11:50:30	b4:b6:76:42:6d:05	DHCP request timed out	6c:f3:7f:c4:42:ce	more	

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

This chapter includes the following topics:

- [IPv6 Notation on page 76](#)
- [Enabling IPv6 Support for OAW-IAP Configuration on page 76](#)
- [Firewall Support for IPv6 on page 78](#)
- [Debugging Commands on page 78](#)

IPv6 Notation

IPv6 is the latest version of Internet Protocol (IP) that is suitable for large-scale IP networks. IPv6 supports a 128-bit address to allow 2^{128} , or approximately 3.4×10^{38} addresses while IPv4 supports only 2^{32} addresses.

The IP address of the IPv6 host is always represented as eight groups of four hexadecimal digits separated by colons. For example `2001:0db8:0a0b:12f0:0000:0000:0000:0001`. However, the IPv6 notation can be abbreviated to compress one or more groups of zeroes or to compress leading or trailing zeroes.

The following examples show various representations of the address

```
2001:0db8:0a0b:12f0:0000:0000:0000:0001
```

- Valid format—`2001:db8:a0b:12f0::0:0:1`
- Invalid format—`2001:db8:a0b:12f0:::0:1`. The “:” sign appears only once in an address.
- With leading zeros omitted—`2001:db8:a0b:12f0:0:0:0:1`
- Switching from upper to lower case—`2001:DB8:A0B:12f0:0:0:0:1`

IPv6 uses a “/” notation which describes the number of bits in netmask as in IPv4.

```
2001:db8::1/128 - Single Host
```

```
2001:db8::/64 - Network
```



IPv6 configuration is supported only on OAW-IAP214/215, OAW-IAP224/225, OAW-IAP274/275, OAW-IAP314/315, OAW-IAP324/325, and OAW-IAP334/335 access points.

Enabling IPv6 Support for OAW-IAP Configuration

OAW-IAPs support IPv6 address mode for the following features:

- [Supported IP modes](#)
- [Configuring IPv6 Address for an OAW-IAP](#)
- [RADIUS over IPv6](#)
- [SNMP Over IPv6](#)
- [SNTP Over IPv6](#)

Supported IP modes

AOS-W Instant supports two modes of IP address configuration:

- V4-only—The OAW-IAP would allow IPv6 clients to pass-through just like the previous AOS-W Instant release.

- **V4-prefer**—Supports both IPv4 and IPv6 addresses. If the OAW-IAP gets both IPv4 and IPv6 responses for a DNS query, then the OAW-IAP would prefer the IPv4 DNS address instead of the IPv6 DNS address.

When the IP mode is set to v4-prefer mode, the OAW-IAP derives a link local IPv6 address and attempts to acquire a routable IPv6 address by monitoring Router Advertisements (RA) packets. OAW-IAP assigns itself to both Stateless address autoconfiguration (SLAAC) and DHCPv6 client address. OAW-IAPs also support IPv6 DNS server addresses and use these for DNS resolution.

In the CLI:

To enable IPv4 mode or dual stack mode:

```
(Instant AP) (config)# ip-mode {v4-only|v4-prefer}
(Instant AP) (config)# end
(Instant AP) (config)# commit apply
```

Configuring IPv6 Address for an OAW-IAP

You can enable the IPv6 mode on the OAW-IAP and also configure a VC IPv6 address using the AOS-W Instant UI or the CLI:

In the AOS-W Instant UI:

To enable IPv6 and configure VC IPv6 address:

1. Go to the **System** link, directly above the Search bar in the AOS-W Instant UI.
2. Under **General**, select the **Allow IPv6 Management** check box.
3. Enter the IP address in the **Virtual Controller IPv6** address text box.
4. Click **OK**.

In the CLI:

To configure an IPv6 address for an OAW-IAP:

```
(Instant AP) (config)# virtual-controller-ipv6 <ipv6 address>
(Instant AP) (config)# end
(Instant AP)# commit apply
```



The VC IPv6 address can be configured only after enabling the v4-prefer mode in the AOS-W Instant CLI.

RADIUS over IPv6

With the address mode set to v4-prefer, the OAW-IAP supports an IPv6 IP address for the RADIUS server. The authentication server configuration can also include the NAS IPv6 address (that defaults to the routable IPv6 address when not configured).

To configure an IPv6 address for the RADIUS server:

```
(Instant AP) (config)# wlan auth-server radiusIPv6
(Instant AP) (Auth Server "radiusIPv6")# ip <host>
(Instant AP) (Auth Server "radiusIPv6")# nas-ip <ip_ipv6>
(Instant AP) (Auth Server "radiusIPv6")# end
(Instant AP)# commit apply
```

SNMP Over IPv6

In this release, you can configure a community string to authenticate messages sent between the VC and the SNMP agent, where the IPv6 address will be used as the VC address. For more information on configuring SNMP parameters, see [Configuring SNMP on page 363](#).

To view the SNMP configuration:

```
(Instant AP)# show running-config|include snmp
snmp-server community e96a5ff136b5f481b6b55af75d7735c16ee1f61ba082d7ee
snmp-server host 2001:470:20::121 version 2c aruba-string inform
```

SNTP Over IPv6

To view the SNTP configuration:

```
(Instant AP)# show running-config|include ntp
ntp-server 2001:470:20::121
```

Firewall Support for IPv6

For a given client, a single ACL is used to firewall both IPv4 and IPv6 rules. A rule **any any match any any any permit** in the access rule configuration will expand to two different ACL entries:

- any any any P6
- any any any P4

Similarly, if any IPv6 specific rule is added. For example, if any DHCPv6 or FTPv6 rule is added, the ACE would be expanded as follows:

```
any 2002::/64 17 0-65535 546-547 6—destined to network 2002::/64 DHCPv6 is denied.
```

```
any 2001::10/128 6 0-65535 20-21 6—destined to host 2001::10 FTP is denied.
```

For all ACLs the OAW-IAP will have an implicit IPv4 and IPv6 **allow all** acl rule.

Debugging Commands

Use the following commands to troubleshoot issues pertaining to IPv6 configuration:

- `show ipv6 interface brief` and `show ipv6 interface details`— displays the configured IPv6 address, and any duplicate addresses.
- `show ipv6 route`—displays the IPv6 routing information.
- `show datapath ipv6 session`—displays IPv6 sessions.
- `show datapath ipv6 user`—displays IPv6 client details.
- `show clients` and `show clients debug`—displays the details about OAW-IAP clients.

This chapter provides the following information:

- [Configuring Wireless Network Profiles on page 79](#)
- [Configuring Fast Roaming for Wireless Clients on page 99](#)
- [Configuring Modulation Rates on a WLAN SSID on page 102](#)
- [Disabling Short Preamble for Wireless Client on page 104](#)
- [Multi-User-MIMO on page 103](#)
- [Management Frame Protection on page 104](#)
- [Editing Status of a WLAN SSID Profile on page 104](#)
- [Editing a WLAN SSID Profile on page 105](#)
- [Deleting a WLAN SSID Profile on page 105](#)

Configuring Wireless Network Profiles

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

AOS-W Instant wireless networks are categorized as:

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



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

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

1. [Configuring WLAN Settings](#)
2. [Configuring VLAN Settings](#)
3. [Configuring Security Settings](#)

4. Configuring Access Rules for a Network

Configuring WLAN Settings for an SSID Profile

You can configure WLAN settings using the AOS-W Instant UI or the CLI.

In the AOS-W Instant UI

To configure WLAN settings:

1. On the **Network** tab of the AOS-W Instant main window, click the **New** link. The **New WLAN** window is displayed. The following figure shows the contents of the **WLAN Settings** tab:

Figure 26 WLAN Settings Tab

2. Enter a name that uniquely identifies a wireless network in the **Name (SSID)** text box.



The SSID name must be unique and may contain any special character except for ' and ''.

3. Based on the type of network profile, select any of the following options under **Primary usage**:
 - **Employee**
 - **Voice**
 - **Guest**
4. Click the **Show advanced options** link. The advanced options for configuration are displayed. Specify the following parameters as required.

Table 21: WLAN Configuration Parameters

Parameter	Description
Broadcast filtering	<p>Select any of the following values:</p> <ul style="list-style-type: none"> • All—When set to All, the OAW-IAP drops all broadcast and multicast frames except DHCP and ARP, IGMP group queries, and IPv6 neighbor discovery protocols. • ARP—When set to ARP, the OAW-IAP drops all broadcast and multicast frames except DHCP and ARP, IGMP group queries, and IPv6 neighbor discovery protocols; additionally, it converts ARP requests to unicast and send frames directly to the associated client. The broadcast filtering option is set to ARP by default when an SSID profile is created. • Unicast-ARP-Only—When set to Unicast-ARP-Only, the OAW-IAP allows all broadcast and multicast frames as it is, however the ARP requests are converted to unicast frames and sends them to the associated clients. • Disabled—When set to Disabled, all broadcast and multicast traffic is forwarded to the wireless interfaces.
Multicast transmission optimization	<p>Select Enabled if you want the OAW-IAP to select the optimal rate for sending broadcast and multicast frames based on the lowest of unicast rates across all associated clients. When this option is enabled, multicast traffic can be sent at up to 24 Mbps. The default rate of sending frames for 2.4 GHz is 1 Mbps and that for 5 GHz is 6 Mbps. This option is disabled by default.</p>
Dynamic multicast optimization	<p>Select Enabled to allow the OAW-IAP to convert multicast streams into unicast streams over the wireless link. Enabling Dynamic Multicast Optimization (DMO) enhances the quality and reliability of streaming video, while preserving the bandwidth available to the non-video clients.</p> <p>NOTE: When you enable DMO on multicast SSID profiles, ensure that the DMO feature is enabled on all SSIDs configured in the same VLAN.</p>
DMO channel utilization threshold	<p>Specify a value to set a threshold for DMO channel utilization. With DMO, the OAW-IAP converts multicast streams into unicast streams as long as the channel utilization does not exceed this threshold. The default value is 90% and the maximum threshold value is 100%. When the threshold is reached or exceeds the maximum value, the OAW-IAP sends multicast traffic over the wireless link.</p>
Transmit Rates	<p>Specify the following parameters:</p> <ul style="list-style-type: none"> • 2.4 GHz—If the 2.4 GHz band is configured on the OAW-IAP, specify the minimum and maximum transmission rate. The default value for minimum transmission rate is 1 Mbps and maximum transmission rate is 54 Mbps. • 5 GHz—If the 5 GHz band is configured on the OAW-IAP, specify the minimum and maximum transmission rate. The default value for minimum transmission rate is 6 Mbps and maximum transmission rate is 54 Mbps.
Band	<p>Select a value to specify the band at which the network transmits radio signals. You can set the band to 2.4 GHz, 5 GHz, or All. The All option is selected by default.</p>

Table 21: WLAN Configuration Parameters

Parameter	Description
DTIM interval	The DTIM interval indicates the delivery traffic indication message (DTIM) period in beacons, which can be configured for every WLAN SSID profile. The DTIM interval determines how often the OAW-IAP should deliver the buffered broadcast and multicast frames to associated clients in the powersave mode. The default value is 1, which means the client checks for buffered data on the OAW-IAP at every beacon. You can also configure a higher DTIM value for power saving.
Min RSSI probe request	Sets a minimum received signal strength indication (RSSI) threshold for probe requests.
Min RSSI auth request	Sets a minimum RSSI threshold for authentication requests.
Very high throughput	Enables the VHT function on OAW-IAP devices that support VHT. For 802.11ac OAW-IAPs, the VHT function is enabled by default. However, you can disable the VHT function if you want the 802.11ac OAW-IAPs to function as 802.11n OAW-IAPs. If VHT is configured or disabled on an SSID, the changes will apply only to the SSID on which it is enabled or disabled.
Zone	Specify the zone for the SSID. When the zone is defined in SSID profile and if the same zone is defined on an OAW-IAP, the SSID is created on that OAW-IAP. For more information on configuring zone details, see Configuring Zone Settings on an OAW-IAP on page 65 .
Time Range	Click Edit , select a Time Range Profile from the list and specify if the profile must be enabled or disabled for the SSID, and then click OK .
Bandwidth Limits	Select the required options under Bandwidth Limits : <ul style="list-style-type: none"> • Airtime—Select this check box to specify an aggregate amount of airtime that all clients in this network can use for sending and receiving data. Specify the airtime percentage. • Each radio—Select this check box to specify an aggregate amount of throughput that each radio is allowed to provide for the connected clients. • Downstream and Upstream—Specify the downstream and upstream rates within a range of 1 to 65,535 Kbps for the SSID users. If the assignment is specific for each user, select the Per user check box.
Wi-Fi Multimedia (WMM) traffic management	Configure the following options for WMM traffic management. WMM supports voice, video, best effort, and background access categories. To allocate bandwidth for the following types of traffic, specify a percentage value under Share . To configure Differentiated Service Code Point (DSCP) mapping, specify a value under DSCP Mapping . <ul style="list-style-type: none"> • Background WMM—For background traffic such as file downloads or print jobs. • Best effort WMM—For best effort traffic such as traffic from legacy devices or traffic from applications or devices that do not support QoS. • Video WMM—For video traffic generated from video streaming. • Voice WMM—For voice traffic generated from the incoming and outgoing voice communication.

Table 21: WLAN Configuration Parameters

Parameter	Description
	<p>For more information on WMM traffic and DSCP mapping, see Wi-Fi Multimedia Traffic Management on page 275.</p> <p>For voice traffic and Spectralink Voice Prioritization, configure the following parameters:</p> <ul style="list-style-type: none"> • Traffic Specification (TSPEC)—To prioritize time-sensitive traffic such as voice traffic initiated by the client, select the Traffic Specification (TSPEC) check box. • TSPEC Bandwidth—To reserve bandwidth, set the TPSEC bandwidth to the desired value within the range of 200–600,000 Kbps. The default value is 2000 Kbps. • Spectralink Voice Protocol (SVP)—Select the check box to prioritize voice traffic for SVP handsets.
Content filtering	Select Enabled to route all DNS requests for the non-corporate domains to OpenDNS on this network.
Inactivity timeout	Specify an interval for session timeout in seconds, minutes, or hours. If a client session is inactive for the specified duration, the session expires and the user is required to log in again. You can specify a value within the range of 60–86,400 seconds (24 hours) for a client session. The default value is 1000 seconds.
Deauth Inactive Clients	Select Enabled to allow the OAW-IAP to send a deauthentication frame to the inactive client and clear client entry.
SSID	<p>Select the Hide check box if you do not want the SSID (network name) to be visible to users.</p> <p>Select the Disable check box if you want to disable the SSID. On selecting this, the SSID will be disabled, but will not be removed from the network. By default, all SSIDs are enabled.</p>
Out of service (OOS)	<p>Enable or disable the SSID based on the following OOS states of the OAW-IAP:</p> <ul style="list-style-type: none"> • VPN down • Uplink down • Internet down • Primary uplink down <p>The network will be out of service when selected event occurs and the SSID is enabled or disabled as per the configuration settings applied. For example, if you select the VPN down option from the drop-down list and set the status to enabled, the SSID is enabled when the VPN connection is down and is disabled when the VPN connection is restored.</p>
OOS time (global)	Configure a hold time interval in seconds within a range of 30–300 seconds, after which the out-of-service operation is triggered. For example, if the VPN is down and the configured hold time is 45 seconds, the effect of this out-of-service state impacts the SSID availability after 45 seconds.
Max clients threshold	<p>Specify the maximum number of clients that can be configured for each Basic Service Set Identifier (BSSID) on a WLAN. You can specify a value within the range of 0–255. The default value is 64.</p> <p>NOTE: This is a per-ap configuration setting, hence the maximum client threshold is set</p>

Table 21: WLAN Configuration Parameters

Parameter	Description
	individually for each OAW-IAP in the cluster.
SSID Encoding	To encode the SSID, select UTF-8. By default, the SSIDs are not encoded. NOTE: When a wireless SSID is encoded, by default, UTF-8 is added to the access rules that are active on the SSID. However this does not apply for the access rules that are configured separately for the SSID. UTF-8 is not supported for wired networks.
Deny inter user bridging	When enabled, the bridging traffic between two clients that are connected to the same SSID on the same VLAN is disabled. The clients can connect to the Internet, but cannot communicate with each other, and the bridging traffic between the clients is sent to the upstream device to make the forwarding decision.
ESSID	Enter the Extended Service Set Identifier (ESSID). If the value defined for ESSID value is not the same as the profile name, the SSIDs can be searched based on the ESSID value and not by its profile name.

- Click **Next** to configure VLAN settings. For more information, see [Configuring VLAN Settings for a WLAN SSID Profile on page 85](#).

In the CLI

To configure WLAN settings for an SSID profile:

```
(Instant AP) (config)# wlan ssid-profile <name>
(Instant AP) (SSID Profile <name>)# essid <ESSID-name>
(Instant AP) (SSID Profile <name>)# type {<Employee>|<Voice>|<Guest>}
(Instant AP) (SSID Profile <name>)# broadcast-filter {All|ARP|Unicast-ARP-Only|Disabled}
(Instant AP) (SSID Profile <name>)# dtim-period <number-of-beacons>
(Instant AP) (SSID Profile <name>)# multicast-rate-optimization
(Instant AP) (SSID Profile <name>)# dynamic-multicast-optimization
(Instant AP) (SSID Profile <name>)# dmo-channel-utilization-threshold
(Instant AP) (SSID Profile <name>)# a-max-tx-rate <rate>
(Instant AP) (SSID Profile <name>)# a-min-tx-rate <rate>
(Instant AP) (SSID Profile <name>)# g-max-tx-rate <rate>
(Instant AP) (SSID Profile <name>)# g-min-tx-rate <rate>
(Instant AP) (SSID Profile <name>)# zone <zone>
(Instant AP) (SSID Profile <name>)# bandwidth-limit <limit>
(Instant AP) (SSID Profile <name>)# per-user-bandwidth-limit <limit>
(Instant AP) (SSID Profile <name>)# air-time-limit <limit>
(Instant AP) (SSID Profile <name>)# wmm-background-dscp <dscp>
(Instant AP) (SSID Profile <name>)# wmm-background-share <share>
(Instant AP) (SSID Profile <name>)# wmm-best-effort-dscp <dscp>
(Instant AP) (SSID Profile <name>)# wmm-best-effort-share <share>
(Instant AP) (SSID Profile <name>)# wmm-video-dscp <dscp>
(Instant AP) (SSID Profile <name>)# wmm-video-share <share>
(Instant AP) (SSID Profile <name>)# wmm-voice-dscp <dscp>
(Instant AP) (SSID Profile <name>)# wmm-voice-share <share>
(Instant AP) (SSID Profile <name>)# rf-band {<2.4>|<5>|<all>}
(Instant AP) (SSID Profile <name>)# content-filtering
(Instant AP) (SSID Profile <name>)# mfp-capable
(Instant AP) (SSID Profile <name>)# mfp-required
(Instant AP) (SSID Profile <name>)# hide-ssid
(Instant AP) (SSID Profile <name>)# out-of-service <def> <name>
(Instant AP) (SSID Profile <name>)# time-range <profile name> {<Enable>|<Disable>}
(Instant AP) (SSID Profile <name>)# inactivity-timeout <interval>
(Instant AP) (SSID Profile <name>)# local-probe-req-thresh <threshold>
```

```
(Instant AP) (SSID Profile <name>)# max-clients-threshold <number-of-clients>
(Instant AP) (SSID Profile <name>)# end
(Instant AP)# commit apply
```

Temporal Diversity and Maximum Retries using CLI

Starting from AOS-W Instant 6.5.0.0-4.3.0.0, when clients are not responding to 802.11 packets with the **temporal-diversity** parameter disabled, which is the default setting, OAW-IAPs can attempt only hardware retries. But if this parameter is enabled when the clients are not responding to 802.11 packets, OAW-IAPs can perform two hardware retries. When the hardware retry attempts fail, OAW-IAPs can perform software retries.

The **max-retries** parameter indicates the maximum number of attempts the OAW-IAP performs when clients are not responding to 802.11 packets. By default, the OAW-IAP attempts a maximum of eight retries when clients are not responding to 802.11 packets.

The following example shows the configuration of **temporal-diversity** and **max-retries** in a WLAN SSID profile:

```
(Instant AP) (config) # wlan ssid-profile Name
(Instant AP) (SSID Profile "Name") # temporal-diversity
(Instant AP) (SSID Profile "Name") # max-retries 3
(Instant AP) (SSID Profile "Name") # end
(Instant AP) # commit apply
```

Configuring VLAN Settings for a WLAN SSID Profile

If you are creating a new SSID profile, complete the WLAN Settings procedure before configuring the VLAN. For more information, see [Configuring WLAN Settings for an SSID Profile on page 80](#).

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

In the AOS-W Instant UI

To configure VLAN settings for an SSID:

1. On the **VLAN** tab of the **New WLAN** window, perform the following steps. The following figure displays the contents of the **VLAN** tab.

Figure 27 VLAN Tab

The screenshot displays the 'New WLAN' configuration interface with the 'VLAN' tab selected. The interface includes a breadcrumb trail: '1 WLAN Settings', '2 VLAN', '3 Security', and '4 Access'. The main section is titled 'Client IP & VLAN Assignment'. Under 'Client IP assignment', there are two radio buttons: 'Virtual Controller assigned' and 'Network assigned', with 'Network assigned' selected. Under 'Client VLAN assignment', there are three radio buttons: 'Default', 'Static', and 'Dynamic', with 'Dynamic' selected. Below these options is a table titled 'VLAN Assignment Rules' with one entry: 'Default VLAN: 1'. At the bottom of the table are buttons for 'New', 'Edit', 'Delete', and two arrow buttons. At the bottom right of the page are 'Back', 'Next', and 'Cancel' buttons.

2. Select any for the following options for **Client IP assignment**:
 - **Virtual Controller assigned**—On selecting this option, the client obtains the IP address from the VC.
 - **Network assigned**—On selecting this option, the IP address is obtained from the network.
3. Based on the type of client IP assignment mode selected, you can configure the VLAN assignment for clients as described in the following table:

Table 22: IP and VLAN Assignment for WLAN SSID Clients

Client IP Assignment	Client VLAN Assignment
Virtual Controller assigned	<p>If Virtual Controller assigned is selected for client IP assignment, the VC creates a private subnet and VLAN on the OAW-IAP for the wireless clients. The network address translation for all client traffic that goes out of this interface is carried out at the source. This setup eliminates the need for complex VLAN and IP address management for a multisite wireless network.</p> <p>On selecting this option, the following client VLAN assignment options are displayed:</p> <ul style="list-style-type: none"> • Default—When selected, the default VLAN as determined by the VC is assigned for clients. • Custom—When selected, you can specify a custom VLAN assignment option. You can select an existing DHCP scope for client IP and VLAN assignment or you can create a new DHCP scope by selecting New. For more information on DHCP scopes, see Configuring DHCP Scopes on page 209.
Network assigned	<p>If Network assigned is selected, you can specify any of the following options for the Client VLAN assignment.</p> <ul style="list-style-type: none"> • Default—On selecting this option, the client obtains the IP address in the same subnet as the OAW-IAPs. By default, the client VLAN is assigned to the native VLAN on the wired network. • Static—On selecting this option, you need to specify any one of the following: a single VLAN, a comma separated list of VLANs, or a range of VLANs for all clients on this network. Select this option for configuring VLAN pooling. • Dynamic—On selecting this option, you can assign the VLANs dynamically from a Dynamic Host Configuration Protocol (DHCP) server. To create VLAN assignment rules, click New to assign the user to a VLAN. In the New VLAN Assignment Rule window, enter the following information: <ul style="list-style-type: none"> • Attribute—Select an attribute returned by the RADIUS server during authentication. • Operator—Select an operator for matching the string. • String—Enter the string to match . • VLAN—Enter the VLAN to be assigned.

4. Click **Next** to configure security settings for the Employee network. For more information, see [Configuring Security Settings for a WLAN SSID Profile on page 88](#).

In the CLI

To manually assign VLANs for WLAN SSID users:

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

To create a new VLAN assignment rule:

```
(Instant AP) (config)# wlan ssid-profile <name>
(Instant AP) (SSID Profile <name>)# set-vlan <attribute> {{contains|ends-with|equals|matches-regular-expression|not-equals|starts-with} <operand> <vlan>|value-of}
(Instant AP) (SSID Profile <name>)# end
(Instant AP)# commit apply
```

Enforcing DHCP

Starting from AOS-W Instant 6.4.3.4-4.2.1.0, you can configure a WLAN SSID profile to enforce DHCP on OAW-IAP clients.

When DHCP is enforced:

- A layer-2 user entry is created when a client associates with an OAW-IAP.
- The client DHCP state and IP address are tracked.
- When the client obtains an IP address from DHCP, the DHCP state changes to complete.
- If the DHCP state is complete, a layer-3 user entry is created.
- When a client roams between the OAW-IAPs, the DHCP state and the client IP address will be synchronized with the new OAW-IAP.

By default, enforcing DHCP feature is disabled.

To enforce DHCP:

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

Configuring Security Settings for a WLAN SSID Profile

This section describes the procedure for configuring security settings for an Employee or Voice network. For information on guest network configuration, see [Captive Portal for Guest Access](#).



If you are creating a new SSID profile, configure the WLAN and VLAN settings before defining security settings. For more information, see [Configuring WLAN Settings for an SSID Profile on page 80](#) and [Configuring VLAN Settings for a WLAN SSID Profile on page 85](#).

Configuring Security Settings for an Employee or Voice Network

You can configure security settings for an Employee or Voice network by using the AOS-W Instant UI or the CLI.

In the AOS-W Instant UI

To configure security settings for an Employee or Voice network:

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

The default security setting for a network profile is **Personal**.

The following figures show the configuration options for **Enterprise**, **Personal**, and **Open** security settings:

Figure 28 Security Tab: Enterprise

The screenshot shows the 'Security Tab: Enterprise' configuration page. At the top, there are four tabs: '1 WLAN Settings', '2 VLAN', '3 Security', and '4 Access'. The 'Security' tab is active. On the left, a vertical slider is positioned at 'Enterprise', with 'Personal' and 'Open' options below it. The main area contains the following settings:

- Key management: WPA-2 Enterprise
- Termination: Disabled
- Authentication server 1: InternalServer
- Reauth interval: 0 min.
- MAC authentication: Perform MAC authentication before 802.1X, MAC authentication fail-thru
- Internal server: [1 User](#)
- Internal server: Default certificate [Upload certificate](#)
- Blacklisting: Disabled
- Fast Roaming: Opportunistic Key Caching(OKC):
- 802.11r:
- 802.11k:
- 802.11v:

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

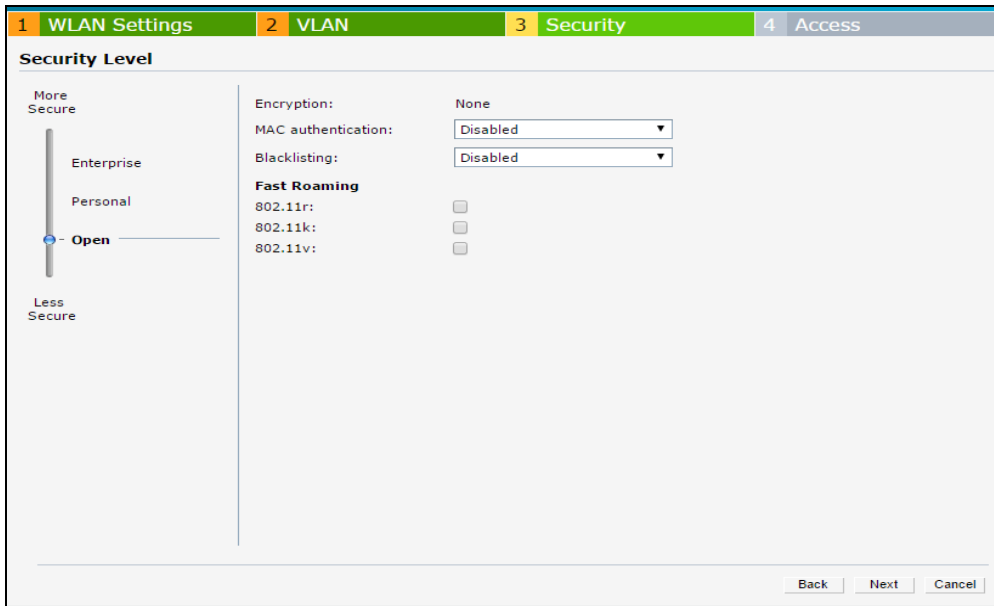
Figure 29 Security Tab: Personal

The screenshot shows the 'Security Tab: Personal' configuration page. At the top, there are four tabs: '1 WLAN Settings', '2 VLAN', '3 Security', and '4 Access'. The 'Security' tab is active. On the left, a vertical slider is positioned at 'Personal', with 'Enterprise' and 'Open' options above it. The main area contains the following settings:

- Key management: WPA-2 Personal
- Passphrase format: 8-63 chars
- Passphrase: [text input field]
- Retype: [text input field]
- MAC authentication: Disabled
- Blacklisting: Disabled
- Fast Roaming:
- 802.11r:
- 802.11k:
- 802.11v:

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

Figure 30 *Security Tab: Open*



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

Table 23: Configuration Parameters for WLAN Security Settings in an Employee or Voice Network

Parameter	Description	Security Level
Key Management	<p>Click the Enterprise security level, select any of the following options from the Key management drop-down list:</p> <ul style="list-style-type: none"> ● WPA-2 Enterprise ● WPA Enterprise ● Both (WPA-2 & WPA) ● Dynamic Wired Equivalent Privacy (WEP) with 802.1X—If you do not want to use a session key from the RADIUS server to derive pairwise unicast keys, set Session Key for LEAP to Enabled. This is required for old printers that use dynamic WEP through Lightweight Extensible Authentication Protocol (LEAP) authentication. The Session Key for LEAP feature is set to Disabled by default. <p>For the Personal security level, select any of the following encryption keys from the Key management drop-down list.</p> <ul style="list-style-type: none"> ● WPA-2 Personal ● WPA-Personal (Both TKIP and AES Encryption) ● WPA-Personal (TKIP Encryption only) ● WPA-Personal (AES Encryption only) ● Both (WPA-2 & WPA) ● Static WEP <p>If a WPA-2, WPA encryption, or Both (WPA-2&WPA) is selected, configure the passphrase:</p> <ol style="list-style-type: none"> 1. Select a passphrase format from the Passphrase format drop-down list. The options available are 8–63 alphanumeric characters and 64 hexadecimal characters. 2. Enter a passphrase in the Passphrase text box and reconfirm. NOTE: The Passphrase may contain any special character except for " . <p>For Static WEP, specify the following parameters:</p> <ol style="list-style-type: none"> 1. Select an appropriate value for WEP key size from the WEP key size drop-down list. You can specify 64-bit or 128-bit . 2. Select an appropriate value for Tx key from the Tx Key drop-down list. You can specify 1, 2, 3, or 4. 3. Enter an appropriate WEP key and reconfirm. 	<p>Applicable to Enterprise and Personal security levels only.</p> <p>For the Open security level, no encryption settings are required.</p>
Termination	<p>To terminate the Extensible Authentication Protocol (EAP) portion of 802.1X authentication on the OAW-IAP instead of the RADIUS server, set Termination to Enabled. Enabling Termination can reduce network traffic to the external RADIUS server by terminating the authorization protocol on the OAW-IAP. By default, for 802.1X authorization, the client conducts an EAP exchange with the RADIUS server, and the OAW-IAP acts as a relay for this exchange.</p>	<p>Enterprise security level</p>

Table 23: Configuration Parameters for WLAN Security Settings in an Employee or Voice Network

Parameter	Description	Security Level
	<p>When Termination is enabled, the OAW-IAP by itself acts as an authentication server and terminates the outer layers of the EAP protocol, only relaying the innermost layer to the external RADIUS server. It can also reduce the number of exchange packets between the OAW-IAP and the authentication server.</p> <p>NOTE: AOS-W Instant supports the configuration of primary and backup authentication servers in an EAP termination-enabled SSID.</p> <p>NOTE: If you are using LDAP for authentication, ensure that OAW-IAP termination is configured to support EAP.</p>	
Authentication server 1 and Authentication server 2	<p>Select any of the following options from the Authentication server 1 drop-down list:</p> <ul style="list-style-type: none"> • Select an authentication server from the list if an external server is already configured. To modify the server parameters, click Edit. • Select New to add a new server. For information on configuring external servers, see Configuring an External Server for Authentication on page 154. • To use an internal server, select Internal server and add the clients that are required to authenticate with the internal RADIUS server. Click the Users link to add the users. For information on adding a user, see Managing OAW-IAP Users on page 141. <p>If an external server is selected, you can also configure another authentication server.</p>	Enterprise, Personal, and Open security levels.
Load balancing	<p>Set this to Enabled if you are using two RADIUS authentication servers, so that the load across the two RADIUS servers is balanced. For more information on the dynamic load balancing mechanism, see Dynamic Load Balancing between Two Authentication Servers on page 154.</p>	Enterprise, Personal, and Open security levels.
Reauth interval	<p>Specify a value for Reauth interval. When set to a value greater than zero, OAW-IAPs periodically reauthenticate all associated and authenticated clients.</p> <p>The following list provides descriptions for three reauthentication interval configuration scenarios:</p> <ul style="list-style-type: none"> • When Reauth interval is configured on an SSID performing L2 authentication (MAC or 802.1X authentication)—When reauthentication fails, the clients are disconnected. If the SSID is performing only MAC authentication and has a pre-authentication role assigned to the client, the client will get a post-authentication role only after a successful reauthentication. If reauthentication fails, the client retains the pre-authentication role. • When Reauth interval is configured on an SSID performing both L2 and L3 authentication (MAC with captive portal authentication)—When reauthentication succeeds, the client retains the role that is already assigned. If reauthentication fails, a pre-authentication role is assigned 	Enterprise, Personal, and Open security levels.

Table 23: Configuration Parameters for WLAN Security Settings in an Employee or Voice Network

Parameter	Description	Security Level
	<p>to the client.</p> <ul style="list-style-type: none"> When Reauth interval is configured on an SSID performing only L3 authentication (captive portal authentication)—When reauthentication succeeds, a pre-authentication role is assigned to the client that is in a post-authentication role. Due to this, the clients are required to go through captive portal to regain access. 	
Blacklisting	<p>To enable blacklisting of the clients with a specific number of authentication failures, select Enabled from the Blacklisting drop-down list and specify a value for Max authentication failures. The users who fail to authenticate the number of times specified in Max authentication failures are dynamically blacklisted.</p>	Enterprise, Personal, and Open security levels.
Accounting	<p>Select any of the following options:</p> <ul style="list-style-type: none"> To enable accounting, select Use authentication servers from the Accounting drop-down list. On enabling the accounting function, OAW-IAPs post accounting information to the RADIUS server at the specified Accounting interval. To use a separate server for accounting, select Use separate servers. The accounting server is distinguished from the authentication server specified for the SSID profile. To disable the accounting function, select Disabled. 	Enterprise, Personal, and Open security levels.
Authentication survivability	<p>To enable authentication survivability, set Authentication survivability to Enabled. Specify a value in hours for Cache timeout (global) to set the duration after which the authenticated credentials in the cache must expire. When the cache expires, the clients are required to authenticate again. You can specify a value within a range of 1–99 hours and the default value is 24 hours.</p> <p>NOTE: The authentication survivability feature requires ClearPass Policy Manager 6.0.2 or later, and is available only when the New server option is selected. On setting this parameter to Enabled, AOS-W Instant authenticates the previously connected clients using EAP-PEAP authentication even when connectivity to ClearPass Policy Manager is temporarily lost. The Authentication survivability feature is not applicable when a RADIUS server is configured as an internal server.</p>	Enterprise security level
MAC authentication	<p>To enable MAC-address-based authentication for Personal and Open security levels, set MAC authentication to Enabled.</p> <p>For Enterprise security level, the following options are available:</p> <ul style="list-style-type: none"> Perform MAC authentication before 802.1X—Select this check box to use 802.1X authentication only when the MAC authentication is successful. MAC authentication fail-thru—On selecting this check box, the 802.1X authentication is attempted when the MAC authentication fails. 	Enterprise, Personal, and Open security levels.

Table 23: Configuration Parameters for WLAN Security Settings in an Employee or Voice Network

Parameter	Description	Security Level
	NOTE: If Enterprise Security level is chosen, the server used for mac authentication will be the same as the server, defined for 802.1x authentication. You will not be able to use the OAW-IAPs internal database for mac authentication and external RADIUS server for 802.1x authentication on the same SSID.	
Delimiter character	Specify a character (for example, colon or dash) as a delimiter for the MAC address string. When configured, the OAW-IAP will use the delimiter in the MAC authentication request. For example, if you specify colon as the delimiter, MAC addresses in the xx:xx:xx:xx:xx:xx format are used. If the delimiter is not specified, the MAC address in the xxxxxxxxxxxx format is used. NOTE: This option is available only when MAC authentication is enabled.	Enterprise, Personal, and Open security levels.
Uppercase support	Set to Enabled to allow the OAW-IAP to use uppercase letters in MAC address string for MAC authentication. NOTE: This option is available only if MAC authentication is enabled.	Enterprise, Personal, and Open security levels.

Table 23: Configuration Parameters for WLAN Security Settings in an Employee or Voice Network

Parameter	Description	Security Level
Upload Certificate	Click Upload Certificate and browse to upload a certificate file for the internal server. For more information on certificates, see Uploading Certificates on page 177 .	Enterprise, Personal, and Open security levels
Fast Roaming	<p>You can configure the following fast roaming options for the WLAN SSID:</p> <ul style="list-style-type: none"> • Opportunistic Key Caching: You can enable Opportunistic Key Caching (OKC) when WPA-2 Enterprise and Both (WPA2 & WPA) encryption types are selected. If OKC is enabled, a cached pairwise master key (PMK) is used when the client roams to a new OAW-IAP. This allows faster roaming of clients without the need for a complete 802.1X authentication. • 802.11r: Selecting this check box enables fast BSS transition. The Fast BSS Transition mechanism minimizes the delay when a client transitions from one BSS to another within the same cluster. This option is available only when WPA-2 Enterprise and WPA-2 personal encryption keys are selected. • 802.11k: Selecting this check box enables 802.11k roaming on the SSID profile. The 802.11k protocol enables OAW-IAPs and clients to dynamically measure the available radio resources. When 802.11k is enabled, OAW-IAPs and clients send neighbor reports, beacon reports, and link measurement reports to each other. • 802.11v: Selecting this check box enables the 802.11v-based BSS transition. 802.11v standard defines mechanisms for wireless network management enhancements and BSS transition management. It allows client devices to exchange information about the network topology and RF environment. The BSS transition management mechanism enables an OAW-IAP to request a voice client to transition to a specific OAW-IAP, or suggest a set of preferred OAW-IAPs to a voice client, due to network load balancing or BSS termination. It also helps the voice client identify the best OAW-IAP to transition to as they roam. 	Enterprise, Personal, and Open security levels.

4. Click **Next** to configure access rules. For more information, see [Configuring Access Rules for a WLAN SSID Profile on page 96](#).

In the CLI

To configure enterprise security settings for the Employee and Voice users:

```
(Instant AP) (config)# wlan ssid-profile <name>
(Instant AP) (SSID Profile <name>)# opmode {wpa2-aes|wpa-tkip,wpa2-aes|dynamic-wep}
(Instant AP) (SSID Profile <name>)# leap-use-session-key
(Instant AP) (SSID Profile <name>)# termination
(Instant AP) (SSID Profile <name>)# auth-server <server-name>
(Instant AP) (SSID Profile <name>)# external-server
(Instant AP) (SSID Profile <name>)# server-load-balancing
(Instant AP) (SSID Profile <name>)# blacklist
(Instant AP) (SSID Profile <name>)# mac-authentication
(Instant AP) (SSID Profile <name>)# l2-auth-failthrough
(Instant AP) (SSID Profile <name>)# auth-survivability
(Instant AP) (SSID Profile <name>)# radius-accounting
```

```
(Instant AP) (SSID Profile <name>)# radius-accounting-mode {user-association|user-
authentication}
(Instant AP) (SSID Profile <name>)# radius-interim-accounting-interval <minutes>
(Instant AP) (SSID Profile <name>)# radius-reauth-interval <minutes>
(Instant AP) (SSID Profile <name>)# max-authentication-failures <number>
(Instant AP) (SSID Profile <name>)# no okc-disable
(Instant AP) (SSID Profile <name>)# dot11r
(Instant AP) (SSID Profile <name>)# dot11k
(Instant AP) (SSID Profile <name>)# dot11v
(Instant AP) (SSID Profile <name>)# exit
(Instant AP) (config)# auth-survivability cache-time-out
(Instant AP) (config)# end
(Instant AP)# commit apply
```

To configure personal security settings for the Employee and Voice users:

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

To configure open security settings for Employee and Voice users of a WLAN SSID profile:

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

Configuring Access Rules for a WLAN SSID Profile

This section describes the procedure for configuring security settings for Employee and Voice networks only. For information on guest network configuration, see [Captive Portal for Guest Access](#).



If you are creating a new SSID profile, complete the WLAN settings and configure VLAN and security parameters, before defining access rules. For more information, see [Configuring WLAN Settings for an SSID Profile on page 80](#), [Configuring VLAN Settings for a WLAN SSID Profile on page 85](#), and [Configuring Security Settings for a WLAN SSID Profile on page 88](#).

You can configure up to 128 access rules for an Employee, Voice, or Guest network using the AOS-W Instant UI or the CLI.

In the AOS-W Instant UI

To configure access rules for an Employee or Voice network:

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

To define an access rule:

- a. Click **New**.
 - b. Select appropriate options in the **New Rule** window.
 - c. Click **OK**.
- **Role-based**—Select this option to enable access based on user roles. For role-based access control:
 - Create a user role if required. For more information, see [Configuring User Roles](#).
 - Create access rules for a specific user role. For more information, see [Configuring ACL Rules for Network Services on page 180](#). You can also configure an access rule to enforce captive portal authentication for an SSID that is configured to use 802.1X authentication method. For more information, see [Configuring Captive Portal Roles for an SSID on page 136](#).
 - Create a role assignment rule. For more information, see [Configuring Derivation Rules on page 199](#).
2. Click **Finish**.

In the CLI

To configure access control rules for a WLAN SSID:

```
(Instant AP) (config)# wlan access-rule <name>
(Instant AP) (Access Rule <name>)# rule <dest> <mask> <match> {<protocol> <start-port> <end-
port> {permit|deny|src-nat [vlan <vlan_id>|tunnel]|dst-nat{<IP-address> <port>|<port>}}| app
<app> {permit|deny}| appcategory <appgrp>|webcategory <webgrp> {permit|deny}| webreputation
<webrep> [<option1...option9>]
(Instant AP) (Access Rule <name>)# end
(Instant AP)# commit apply
```

To configure access control rules based on the SSID:

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

To configure role assignment rules:

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

To configure a pre-authentication role:

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

To configure machine and user authentication roles:

```
(Instant AP) (config)# wlan ssid-profile <name>
(Instant AP) (SSID Profile <name>)# set-role-machine-auth <machine_only> <user_only>
(Instant AP) (SSID Profile <name>)# end
(Instant AP)# commit apply
```

To configure unrestricted access:

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

Example

The following example configures access rules for the wireless network:

```
(Instant AP) (config)# wlan access-rule WirelessRule
(Instant AP) (Access Rule "WirelessRule")# rule 192.0.2.2 255.255.255.0 match 6 4343 4343 log
classify-media
(Instant AP) (Access Rule "WirelessRule")# rule any any match app deny throttle-downstream 256
throttle-up 256
(Instant AP) (Access Rule "WirelessRule")# rule any any match appcategory collaboration permit
(Instant AP) (Access Rule "WirelessRule")# rule any any match webcategory gambling deny
(Instant AP) (Access Rule "WirelessRule")# rule any any match webcategory training-and-tools
permit
(Instant AP) (Access Rule "WirelessRule")# rule any any match webreputation well-known-sites
permit
(Instant AP) (Access Rule "WirelessRule")# rule any any match webreputation safe-sites permit
(Instant AP) (Access Rule "WirelessRule")# rule any any match webreputation benign-sites permit
(Instant AP) (Access Rule "WirelessRule")# rule any any match webreputation suspicious-sites
deny
(Instant AP) (Access Rule "WirelessRule")# rule any any match webreputation high-risk-sites
deny
(Instant AP) (Access Rule "WirelessRule")# end
(Instant AP)# commit apply
```

Configuring Per-AP SSID and Per-AP-VLAN Settings on a Wireless Profile

Starting from AOS-W Instant 6.4.4-4.2.3.0, you can set the environment variables, **per_ap_ssid** and **per_ap_vlan** on a **wlan ssid-profile** by using the CLI. The **ssid-profile-ssid** and **ssid-profile vlan** parameters must be enhanced to accept the **ssid** and **vlan** variables, respectively.

You can configure the **per-ap-ssid** and the **per-ap-vlan** settings for the **SSID** and **VLAN** profiles, respectively, by using the AOS-W Instant CLI.

In the CLI

To configure the wlan ssid-profile:

```
(Instant AP) (config)# wlan ssid-profile <ssid_profile>
```

To configure the per-ap-ssid variable:

```
(Instant AP)# per-ap-ssid <text>
```

To configure the per-ap-vlan variable:

```
(Instant AP)# per-ap-vlan <vlan>
```

To verify the per-ap-ssid and per-ap-vlan configurations:

```
(Instant AP)# show ap-env
Antenna Type:Internal
name:TechPubsAP
per_ap_ssid:PCCW
per_ap_vlan:vlan
lacp_mode:enable
```



For information on configuring a native VLAN on a wired profile, see [Configuring VLAN for a Wired Profile on page 107](#).

Configuring Fast Roaming for Wireless Clients

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

- Opportunistic Key Caching
- Fast BSS Transition (802.11r Roaming)
- Radio Resource Management (802.11k)
- BSS Transition Management (802.11v)

Opportunistic Key Caching

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



OKC roaming (when configured in the 802.1X Authentication profile) is supported on WPA-2 clients. If the wireless client (the 802.1X supplicant) does not support this feature, a complete 802.1X authentication is required whenever a client roams to a new OAW-IAP.

Configuring an OAW-IAP for OKC Roaming

You can enable OKC roaming for WLAN SSID by using the AOS-W Instant UI or the CLI.

In the AOS-W Instant UI

1. Navigate to the WLAN wizard (Go to **Network > New** OR Go to **Network > WLAN SSID** and click **edit**).
2. Click the **Security** tab.
3. Move the slider to the **Enterprise** security level. On selecting the Enterprise security level, the authentication options applicable to the Enterprise network are displayed.

The screenshot displays the 'Security Level' configuration page in the AOS-W Instant UI. The page is divided into four tabs: '1 WLAN Settings', '2 VLAN', '3 Security', and '4 Access'. The 'Security' tab is active. On the left, a vertical slider indicates the security level, with 'Enterprise' selected. The main configuration area includes the following options:

- Key management:** WPA-2 Enterprise
- Termination:** Disabled
- Authentication server 1:** InternalServer
- Reauth interval:** 0 min.
- MAC authentication:** Perform MAC authentication before 802.1X, MAC authentication fail-thru
- Internal server:** [User](#)
- Internal server:** Default certificate [Upload certificate](#)
- Blacklisting:** Disabled
- Fast Roaming:** Opportunistic Key Caching (OKC): ; 802.11r: ; 802.11k: ; 802.11v:

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

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

In the CLI

To disable OKC roaming on a WLAN SSID:

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

To enable OKC roaming on a WLAN SSID:

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

Fast BSS Transition (802.11r Roaming)

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

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



Fast BSS Transition is operational only if the wireless client supports 802.11r standard. If the client does not support 802.11r standard, it falls back to the normal WPA-2 authentication method.

Configuring an OAW-IAP for 802.11r support

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

In the AOS-W Instant UI

1. Navigate to the WLAN wizard (Go to **Network > New** OR Go to **Network > WLAN SSID** and click **edit**).
2. Click the **Security** tab.
3. Under **Fast Roaming**, select the **802.11r** check box.
4. Click **Next** and then click **Finish**.

In the CLI

To enable 802.11r roaming on a WLAN SSID:

```
(Instant AP) (config)# wlan ssid-profile <name>
(Instant AP) (SSID Profile <name>)# dot11r
(Instant AP) (config)# end
(Instant AP)# commit apply
```

Example

```
(Instant AP) (config)# wlan ssid-profile dot11r-profile
(Instant AP) (SSID Profile "dot11r-profile")# dot11r
(Instant AP) (config)# end
(Instant AP)# commit apply
```

Radio Resource Management (802.11k)

The 802.11k standard provides mechanisms for OAW-IAPs and clients to dynamically measure the available radio resources and enables stations to query and manage their radio resources. In an 802.11k-enabled network, OAW-IAPs and clients can share radio and link measurement information, neighbor reports, and beacon reports with each other. This allows the WLAN network infrastructural elements and clients to assess resources and make optimal mobility decisions to ensure Quality of Service (QoS) and seamless continuity.

AOS-W Instant supports the following radio resource management information elements with 802.11k support enabled:

- *Power Constraint IE*—The power constraint element contains the information necessary to allow a client to determine the local maximum transmit power in the current channel.
- *AP Channel Report IE*—The OAW-IAP channel report element contains a list of channels in a regulatory class where a client is likely to find an OAW-IAP, including the OAW-IAP transmitting the OAW-IAP channel report.
- *Radio Resource Management (RRM) Enabled Capabilities IE*—The RRM-enabled capabilities element signals support for radio measurements in a device. The clients use this IE to specify their radio measurement capabilities.
- *BSS Load Element*—The BSS load element contains information on the density of clients and traffic levels in the QBSS.
- *Transmit Power Control (TPC) Report IE*—The TPC IE contains transmit power and link margin information.
- *Quiet IE*: The Quiet IE defines an interval during which no transmission occurs in the current channel. This interval may be used to assist in making channel measurements without interference from other stations in the BSS.
- *Extended Capabilities IE*—The extended capabilities IE carries information about the capabilities of an IEEE 802.11 station.

Beacon Report Requests and Probe Responses

The beacon request frame is sent by an OAW-IAP to request a client to report the list of beacons detected by the client on all channels.

- The beacon request is sent using the radio measurement request action frame.
- It is sent only to those clients that have the capability to generate beacon reports. The clients indicate their capabilities through the *RRM enabled capabilities IE* sent in the association request frames.
- By default, the beacon request frames are sent at a periodicity of 60 seconds.

Configuring a WLAN SSID for 802.11k Support

You can enable 802.11k support on a WLAN SSID by using the AOS-W Instant UI or the CLI.

In the AOS-W Instant UI

1. Navigate to the WLAN wizard (Go to **Network > New** OR Go to **Network > WLAN SSID** and click **edit**).
2. Click the **Security** tab.
3. Under **Fast Roaming**, select the **802.11k** check box.
4. Click **Next** and then click **Finish**.



To allow the OAW-IAP and clients to exchange neighbor reports, ensure that Client match is enabled through **RF > ARM > Client match > Enabled** in the UI or by executing the **client-match** command in the **arm** configuration subcommand mode.

In the CLI

To enable 802.11k profile:

```
(Instant AP) (config)# wlan ssid-profile <name>
(Instant AP) (SSID Profile <name>)# dot11k
(Instant AP) (config)# end
(Instant AP)# commit apply
```

To view the beacon report details:

```
(Instant AP)# show ap dot11k-beacon-report <mac>
```

To view the neighbor details:

```
(Instant AP)# show ap dot11k-nbrs
```

Example

```
(Instant AP) (config)# wlan ssid-profile dot11k-profile
(Instant AP) (SSID Profile "dot11k-profile")# dot11k
(Instant AP) (config)# end
(Instant AP)# commit apply
```

BSS Transition Management (802.11v)

The 802.11v standard provides Wireless Network Management enhancements to the IEEE 802.11 MAC and PHY. It extends radio measurements to define mechanisms for wireless network management of stations including BSS transition management.

OAW-IAPs support the generation of the BSS transition management request frames to the 802.11k clients when a suitable OAW-IAP is identified for a client through Client Match.

Configuring a WLAN SSID for 802.11v Support

You can enable 802.11v support on a WLAN SSID by using the AOS-W Instant UI or the CLI.

In the AOS-W Instant UI

1. Navigate to the WLAN wizard (Go to **Network > New** OR Go to **Network > WLAN SSID** and click **edit**).
2. Click the **Security** tab.
3. Under **Fast Roaming**, select the **802.11v** check box.
4. Click **Next** and then click **Finish**.

In the CLI

To enable 802.11v profile:

```
(Instant AP) (config)# wlan ssid-profile <name>
(Instant AP) (SSID Profile <name>)# dot11v
(Instant AP) (config)# end
(Instant AP)# commit apply
```

Example

```
(Instant AP) (config)# wlan ssid-profile dot11v-profile
(Instant AP) (SSID Profile "dot11v-profile")# dot11v
(Instant AP) (config)# end
(Instant AP)# commit apply
```

Configuring Modulation Rates on a WLAN SSID

OAW-IAPs allow you to enable or disable modulation rates for a radio band; High Throughput (HT) Modulation and Coding Scheme (MCS) set; and Very High Throughput (VHT) MCS rates set, when configuring a WLAN SSID profile. For example, the 802.11g band supports the modulation rate including 1, 2, 5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps and 802.11a band supports a modulation rate set including 6, 9, 12, 18, 24, 36, 48, 54 Mbps.

The 802.11 radio profiles support basic modulation and transmission rates. The 802.11g basic modulation rates determine the 802.11b/g rates for the data that are advertised in beacon frames and probe response and 802.11g transmission rates determine the 802.11b/g rates at which the OAW-IAP can transmit data.

For 802.11n clients, you can now configure an HT MCS rate set so that the SSID does not broadcast the disabled MCS rates list.

For 802.11ac clients, only 10 MCS rates supported in the 802.11ac mode and OAW-IAPs use a combination of VHT MCSs and spatial streams to convey the supported MCS rates.

In the AOS-W Instant 6.4.3.4-4.2.1.0 release, the modulation rates can be configured only through the OAW-IAP CLI.

To configure modulation rates:

```
(Instant AP)# config terminal
(Instant AP)(config)# wlan ssid-profile <ssid_profile>
(Instant AP)(SSID Profile "<ssid_profile>")# a-basic-rates 6 9 12 18
(Instant AP)(SSID Profile "<ssid_profile>")# a-tx-rates 36 48 54
(Instant AP)(SSID Profile "<ssid_profile>")# supported-mcs-set 1,3,6,7
(Instant AP)(SSID Profile "<ssid_profile>")# vht-support-mcs-map 7, 9, 8
(Instant AP)(SSID Profile "<ssid_profile>")# end
(Instant AP)# commit apply
```

Multi-User-MIMO

The Multi-User Multiple-Input Multiple-Output (MU-MIMO) feature allows the 802.11ac Wave 2 OAW-IAPs to send multiple frames to multiple clients simultaneously over the same frequency spectrum. With MU-MIMO, OAW-IAPs can support simultaneous directional Radio Frequency (RF) links and up to four simultaneous full-rate Wi-Fi connections (For example, smart phone, tablet, laptop, multimedia player, or other client device).

The MU-MIMO feature is enabled by default on WLAN SSIDs to allow OAW-IAPs to use the MU beamformer bit in beacon frames to broadcast to clients. When disabled, the MU beamformer bit is set to unsupported.

Enabling or Disabling MU-MIMO

The MU-MIMO feature is enabled by default on WLAN SSIDs. To disable this feature:

```
(host)(config)# wlan ssid-profile <ssid_profile>
(host)(SSID Profile "<ssid_profile>")# vht-mu-txbf-disable
(host)(SSID Profile "<ssid_profile>")# end
(host)# commit apply
```

To re-enable MU-MIMO:

```
(host)(config)# wlan ssid-profile <ssid_profile>
(host)(SSID Profile "<ssid_profile>")# no vht-mu-txbf-disable
(host)(SSID Profile "<ssid_profile>")# end
(host)# commit apply
```

RTS/CTS Flow Control

The (Request to Send) RTS / (Clear to Send) CTS mechanism allows devices to reserve the RF medium and minimize the frame collisions introduced by hidden stations. When RTS is enabled, a higher number of retransmissions occurring on the WLAN triggers the RTS/CTS handshake and the transmitter station sends an RTS frame to the receiver station. The receiver station responds with a CTS frame. The RTS/CTS frames are sent only when the packet size exceeds the RTS threshold. By default, the RTS threshold is set to 2333 octets.

Configuring RTS/CTS Threshold

You can set the RTS/CTS threshold value within the range of 0–2347 octets. By default, the RTS/CTS threshold is set to 2333.

To configure the RTS/CTS threshold:

```
(Instant AP) (config)# wlan ssid-profile <ssid_profile>
(Instant AP) (SSID Profile "<ssid_profile>")# rts-threshold <threshold>
(Instant AP) (SSID Profile "<ssid_profile>")# end
(Instant AP)# commit apply
```

To disable RTS/CTS, set the RTS threshold value to 0.

Management Frame Protection

AOS-W Instant supports the IEEE 802.11w standard, also known as Management Frame Protection (MFP). MFP increases the security by providing data confidentiality of management frames. MFP uses 802.11i (Robust Security Network) framework that establishes encryption keys between the client and OAW-IAP.

To enable MFP on the OAW-IAP:

```
(Instant AP) (config)# wlan ssid-profile myAP
(Instant AP) (SSID Profile "myAP")# mfp-capable
(Instant AP) (SSID Profile "myAP")# mfp-required
(Instant AP) (SSID Profile "myAP")# end
(Instant AP)# commit apply
```

If the *mfp-required* parameter is enabled, the SSID supports only the clients that exhibit the MFP functionality.

If the *mfp-capable* parameter enabled, the SSID supports management frame protection (MFP) capable clients and non-MFP clients.



The MFP configuration is a per-SSID configuration.

Disabling Short Preamble for Wireless Client

To improve the network performance and communication between the OAW-IAP and its clients, you can enable or disable the transmission and reception of short preamble frames. If the short preamble is optional for the wireless devices connecting to an SSID, you can disable short preamble through the OAW-IAP CLI. Short preamble is enabled by default.

To disable the short preamble:

```
(Instant AP)# config terminal
(Instant AP) (config)# wlan ssid-profile <ssid_profile>
(Instant AP) (SSID Profile "<ssid_profile>")# short-preamble-disable
(Instant AP) (SSID Profile "<ssid_profile>")# end
(Instant AP)# commit apply
```

Editing Status of a WLAN SSID Profile

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

In the AOS-W Instant UI

To modify the status of a WLAN SSID profile:

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

In the CLI

To disable an SSID:

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

To enable an SSID:

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

Editing a WLAN SSID Profile

To edit a WLAN SSID profile:

1. On the **Network** tab, select the network that you want to edit. The **edit** link is displayed.
2. Click the **edit** link. The **Edit network** window is displayed.
3. Modify the settings as required. Click **Next** to move to the next tab.
4. Click **Finish** to save the changes.

Deleting a WLAN SSID Profile

To delete a WLAN SSID profile:

1. On the **Network** tab, click the network that you want to delete. A **x** link is displayed beside the network to be deleted.
2. Click **x**. A delete confirmation window is displayed.
3. Click **Delete Now**.

This chapter describes the following procedures:

- [Configuring a Wired Profile on page 106](#)
- [Assigning a Profile to Ethernet Ports on page 111](#)
- [Editing a Wired Profile on page 111](#)
- [Deleting a Wired Profile on page 112](#)
- [Link Aggregation Control Protocol on page 112](#)
- [Understanding Hierarchical Deployment on page 113](#)

Configuring a Wired Profile

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

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

1. [Configuring Wired Settings on page 106](#)
2. [Configuring VLAN for a Wired Profile on page 107](#)
3. [Configuring Security Settings for a Wired Profile on page 108](#)
4. [Configuring Access Rules for a Wired Profile on page 109](#)

For information on creating a wired profile for guest network, see [Captive Portal for Guest Access](#).

Configuring Wired Settings

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

In the AOS-W Instant UI

1. Click the **Wired** link under **More** on the AOS-W Instant main window. The **Wired** window is displayed.
2. Click **New** under **Wired Networks**. The **New Wired Network** window is displayed.
3. Click the **Wired Settings** tab and configure the following parameters:
 - a. **Name**—Specify a name for the profile.
 - b. **Primary Usage**—Select **Employee** or **Guest**.
 - c. **Speed/Duplex**—Ensure that appropriate values are selected for **Speed/Duplex**. Contact your network administrator if you need to assign speed and duplex parameters.
 - d. **POE**—Set **POE** to **Enabled** to enable Power over Ethernet.
 - e. **Admin Status**—Ensure that an appropriate value is selected. The **Admin Status** indicates if the port is up or down.
4. Click **Show advanced options** and configure the following parameters as required:
 - a. **Content Filtering**—To ensure that all DNS requests to non-corporate domains on this wired network are sent to OpenDNS, select **Enabled** for **Content Filtering**.
 - b. **Uplink**—Select **Enabled** to configure uplink on this wired profile. If **Uplink** is set to **Enabled** and this network profile is assigned to a specific port, the port will be enabled as Uplink port. For more

information on assigning a wired network profile to a port, see [Assigning a Profile to Ethernet Ports on page 111](#).

- c. **Spanning Tree**—Select the **Spanning Tree** check box to enable Spanning Tree Protocol (STP) on the wired profile. STP ensures that there are no loops in any bridged Ethernet network and operates on all downlink ports, regardless of forwarding mode. STP will not operate on the uplink port and is supported only on OAW-IAPs with three or more ports. By default, Spanning Tree is disabled on wired profiles.
 - d. **Inactivity Timeout**—Specify the time out interval within the range of 60–86,400 seconds for inactive wired clients. The default interval is 1000 seconds.
5. Click **Next**. The **VLAN** tab details are displayed.
 6. Configure VLAN for the wired profile. For more information, see [Configuring VLAN for a Wired Profile on page 107](#).

In the CLI

To configure the settings for a wired profile:

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

Configuring VLAN for a Wired Profile



If you are creating a new wired profile, complete the Wired Settings procedure before configuring the VLAN settings. For more information, see [Configuring Wired Settings on page 106](#).

You can configure VLAN using the AOS-W Instant UI or the CLI.

In the AOS-W Instant UI

To configure a VLAN:

1. In the **VLAN** tab, enter the following information.
 - a. **Mode**—You can specify any of the following modes:
 - **Access**—Select this mode to allow the port to carry a single VLAN specified as the native VLAN.
 - **Trunk**—Select this mode to allow the port to carry packets for multiple VLANs specified as allowed VLANs.
 - b. Specify any of the following values for **Client IP Assignment**:
 - **Virtual Controller Assigned**: Select this option to allow the VC to assign IP addresses to the wired clients. When the VC assignment is used, the source IP address is translated for all client traffic that goes through this interface. The VC can also assign a guest VLAN to a wired client.
 - **Network Assigned**: Select this option to allow the clients to receive an IP address from the network to which the VC is connected. On selecting this option, the **New** button to create a VLAN is displayed. Create a new VLAN if required.
 - c. If the **Trunk** mode is selected:
 - Specify the VLAN in **Allowed VLAN**, enter a list of comma separated digits or ranges, for example, 1,2,5 or 1–4, or all. The Allowed VLAN refers to the VLANs carried by the port in Access mode.

- If **Client IP Assignment** is set to **Network Assigned**, specify a value for **Native VLAN**. A VLAN that does not have a VLAN ID tag in the frames is referred to as Native VLAN. You can specify a value within the range of 1–4093.
- d. If the **Access** mode is selected:
- If **Client IP Assignment** is set to **Virtual Controller Assigned**, proceed to step 2.
 - If **Client IP Assignment** is set to **Network Assigned**, specify a value for **Access VLAN** to indicate the VLAN carried by the port in the **Access** mode.
2. Click **Next**. The **Security** tab details are displayed.
 3. Configure security settings for the wired profile. For more information, see [Configuring Security Settings for a Wired Profile on page 108](#).

In the CLI

To configure VLAN settings for a wired profile:

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

To configure a new VLAN assignment rule:

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

Configuring Security Settings for a Wired Profile



If you are creating a new wired profile, complete the Wired Settings and VLAN procedures before specifying the security settings. For more information, see [Configuring Wired Settings on page 106](#) and [Configuring VLAN Settings for a WLAN SSID Profile on page 85](#).

Configuring Security Settings for a Wired Employee Network

You can configure security parameters for the Employee network by using the AOS-W Instant UI or the CLI.

In the AOS-W Instant UI

To configure security parameters for the Employee network:

1. Configure the following parameters in the **Security** tab.
 - **Port type**—To support trusted ports in an OAW-IAP, select **Trusted**. When the Port type is trusted, MAC and 802.1X authentication parameters cannot be configured. The Port Type is **Untrusted** by default. In a trusted mode, OAW-IAPs will not create any user entry. A predefined ACL is applied to the trusted port in order to control the client traffic that needs to be source NATed.
 - **MAC authentication**—To enable MAC authentication, select **Enabled**. The MAC authentication is disabled by default.
 - **802.1X authentication**—To enable 802.1X authentication, select **Enabled**. The 802.1X authentication is disabled by default.
 - **MAC authentication fail-thru**—To enable authentication fail-thru, select **Enabled**. When this feature is enabled, 802.1X authentication is attempted when MAC authentication fails. The **MAC**

authentication fail-thru check box is displayed only when both **MAC authentication** and **802.1X authentication** are **Enabled**.

- Select any of the following options for **Authentication server 1**:
 - **New**—On selecting this option, an external RADIUS server must be configured to authenticate the users. For information on configuring an external server, see [Configuring an External Server for Authentication on page 154](#).
 - **Internal server**— If an internal server is selected, add the clients that are required to authenticate with the internal RADIUS server. Click the **Users** link to add users. For information on adding a user, see [Managing OAW-IAP Users on page 141](#).
 - **Accounting**—Select any of the following options:
 - **Disabled**—Disables accounting.
 - **Use authentication servers**—When selected, the authentication servers configured for the wired profile are used for accounting purposes.
 - **Use separate servers**—Allows you to configure separate accounting servers.
 - **Accounting interval**—Allows you set an accounting interval within the range of 0–60 minutes for sending interim accounting information to the RADIUS server.
 - **Reauth interval**—Specify the interval at which all associated and authenticated clients must be reauthenticated.
 - **Load balancing**—Set this to **Enabled** if you are using two RADIUS authentication servers, so that the load across the two RADIUS servers is balanced. For more information on the dynamic load balancing mechanism, see [Dynamic Load Balancing between Two Authentication Servers on page 154](#).
2. Click **Next**. The **Access** tab details are displayed.

In the CLI

To configure security settings for an employee network:

```
(Instant AP) (config)# wired-port-profile <name>
(Instant AP) (wired ap profile <name>)# mac-authentication
(Instant AP) (wired ap profile <name>)# l2-auth-failthrough
(Instant AP) (wired ap profile <name>)# auth-server <name>
(Instant AP) (wired ap profile <name>)# server-load-balancing
(Instant AP) (wired ap profile <name>)# radius-accounting
(Instant AP) (wired ap profile <name>)# radius-accounting-mode {user-association|user-
authentication}
(Instant AP) (wired ap profile <name>)# radius-interim-accounting-interval <minutes>
(Instant AP) (wired ap profile <name>)# radius-reauth-interval <Minutes>
(Instant AP) (wired ap profile <name>)# trusted
(Instant AP) (wired ap profile <name>)# end
(Instant AP)# commit apply
```

Configuring Access Rules for a Wired Profile

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



If you are creating a new wired profile, complete the Wired Settings and configure the VLAN and security parameters before defining access rules. For more information, see [Configuring Wired Settings on page 106](#), [Configuring VLAN for a Wired Profile on page 107](#), and [Configuring Security Settings for a Wired Profile on page 108](#).

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

In the AOS-W Instant UI

To configure access rules:

1. On the **Access** tab, configure the following access rule parameters.
 - a. Select any of the following types of access control:
 - **Role-based**—Allows the users to obtain access based on the roles assigned to them.
 - **Unrestricted**—Allows the users to obtain unrestricted access on the port.
 - **Network-based**—Allows the users to be authenticated based on access rules specified for a network.
 - b. If the **Role-based** access control is selected, perform the following steps:
 - Under **Roles**, select an existing role for which you want to apply the access rules, or click **New** and add the required role. The list of roles defined for all networks is displayed under **Roles**.



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

- Select the access rule associated with a specific role and modify if required. To add a new access rule, click **New** in the **Access Rules** window. You can configure up to 64 access rules. For more information on configuring access rules, see [Configuring ACL Rules for Network Services on page 180](#).
- Configure rules to assign roles for an authenticated client. You can also configure rules to derive VLANs for the wired network profile. For more information on role assignment rules and VLAN derivation rules, see [Configuring Derivation Rules on page 199](#) and [Configuring VLAN Derivation Rules on page 204](#).
- Select the **Assign pre-authentication role** check box to add a pre-authentication role that allows some access to the users before client authentication.
- Select the **Enforce Machine Authentication** check box, to configure access rights to clients based on whether the client device supports machine authentication. Select the **Machine auth only** and **User auth only** rules. Machine Authentication is only supported on Windows devices and devices such as iPads.



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

2. Click **Finish**.

In the CLI

To configure access rules for a wired profile:

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

To configure role assignment rules:

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

To configure a pre-authentication role:

```
(Instant AP) (config)# wired-port-profile <name>
(Instant AP) (wired ap profile <name>)# set-role-pre-auth <role>
```

```
(Instant AP) (wired ap profile <name>)# end
(Instant AP) # commit apply
```

To configure machine and user authentication roles:

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

To configure unrestricted access:

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

Assigning a Profile to Ethernet Ports

You can assign profiles to Ethernet ports using the AOS-W Instant UI or the CLI.

In the AOS-W Instant UI

To assign profiles to Ethernet ports:

1. Click the **Wired** link under **More** on the AOS-W Instant main window. The **Wired** window is displayed.
2. To assign an Ethernet downlink profile to Ethernet 0 port:
 - a. Ensure that the wired bridging on the port is enabled. For more information, see [Configuring Wired Bridging on Ethernet 0 for Mesh Point on page 337](#).
 - b. Select and assign a profile from the **0/0** drop-down list.
 - c. To assign a wired profile to Ethernet 0/1 port, select the profile from the **0/1** drop-down list.
 - d. If the OAW-IAP supports E2, E3, and E4 ports, assign profiles to other Ethernet ports by selecting a profile from the **0/2**, **0/3**, and **0/4** drop-down lists.

In the CLI

To assign profiles to Ethernet ports:

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

Editing a Wired Profile

To edit a wired profile:

1. Click the **Wired** link under **More** on the AOS-W Instant main window. The **Wired** window is displayed.
2. In the **Wired** window, select the wired profile to modify.
3. Click **Edit**. The **Edit Wired Network** window is displayed.
4. Modify the required settings.
5. Click **Finish** to save the modifications.

Deleting a Wired Profile

To delete a wired profile:

1. Click the **Wired** link under **More** on the AOS-W Instant main window. The **Wired** window is displayed.
2. In the **Wired** window, select the wired profile to delete.
3. Click **Delete**. The wired profile is deleted.

Link Aggregation Control Protocol

The OAW-IAP220 Series access points and OAW-IAP270 Series support the IEEE 802.11ac standard for high-performance WLAN. To support maximum traffic, port aggregation is required as it increases throughput and enhances reliability. To support port aggregation, AOS-W Instant supports Link Aggregation Control Protocol (LACP) based on the IEEE 802.3ad standard. The 802.3ad standard for Ethernet aggregation uses LACP as a method to manage link configuration and balance traffic among aggregated ports.

LACP provides a standardized means for exchanging information with partner systems to form a dynamic link aggregation group. The LACP feature is automatically enabled during OAW-IAP boots and it dynamically detects the OAW-IAP if connected to a partner system with LACP capability, by checking if there is any LACP Protocol Data Unit (PDU) received on either Ethernet 0 or Ethernet 1 port.

If a switch in the cluster has the LACP capability, you can combine Ethernet 0 or Ethernet 1 interfaces into the link aggregation group to form a single logical interface (port-channel). Port-channels can be used to provide additional bandwidth or link redundancy between two devices. OAW-IAP supports link aggregation using either standard port-channel (configuration based) or Link Aggregation Control Protocol (protocol signaling based). You can deploy OAW-IAP22x Series or OAW-IAP27x Series access points with LACP configuration to benefit from the higher (greater than 1 Gbps) aggregate throughput capabilities of the two radios.



The LACP feature is supported only on OAW-IAP22x Series and OAW-IAP27x Series access points.

Verifying LACP Configuration on the OAW-IAP

There is no configuration required on the OAW-IAP for enabling LACP support. However, you can view the status of LACP on OAW-IAPs by using the following command:

```
(Instant AP)# show lacp status
AP LACP Status
-----
Link Status   LACP Rate   Num Ports   Actor Key   Partner Key   Partner MAC
-----
Up            slow        2           17          1             70:81:05:11:3e:80
Slave Interface Status
-----
Slave I/f Name   Permanent MAC Addr   Link Status   Member of LAG   Link Fail Count
-----
eth0              6c:f3:7f:c6:76:6e    Up            Yes              0
eth1              6c:f3:7f:c6:76:6f    Up            Yes              0
Traffic Sent on Enet Ports
-----
Radio Num   Enet 0 Tx Count   Enet 1 Tx Count
-----
0           0                  0
1           0                  0
non-wifi    2                  17
```


Enabling Static LACP Configuration

When OAW-IAPs connect to switches which have the LACP capability, the LACP feature does not work as expected. To enable a static LACP configuration, new commands are introduced.

OAW-IAPs support the dynamic LACP configuration according to a peer switch. When the peer switch enables LACP configuration, the OAW-IAPs form the LACP. Users can enable, disable, and remove the static LACP configuration in the OAW-IAP. When the OAW-IAP boots up, it forms the LACP according to the static configuration.



The static LACP mode is supported on OAW-IAP225, OAW-IAP275, and OAW-IAP325 access points.

To enable the static LACP mode on OAW-IAPs:

```
(Instant AP)# lACP-mode enable
```

To disable the static LACP mode on OAW-IAPs:

```
(Instant AP)# lACP-mode disable
```

Verifying Static LACP Mode

To verify the static LACP configuration, execute the following command in the OAW-IAP CLI:

```
(Instant AP)# show ap-env  
Antenna Type:Internal  
name:TechPubsAP  
per_ap_ssid:1234  
per_ap_vlan:abc  
lACP_mode:enable
```

Understanding Hierarchical Deployment

An OAW-IAP with more than one wired port) can be connected to the downlink wired port of another OAW-IAP (Ethernet X). An OAW-IAP with a single Ethernet port (like OAW-IAP90 or OAW-IAP100 Series access points) can be provisioned to use Ethernet bridging, so that Ethernet 0 port is converted to a downlink wired port.

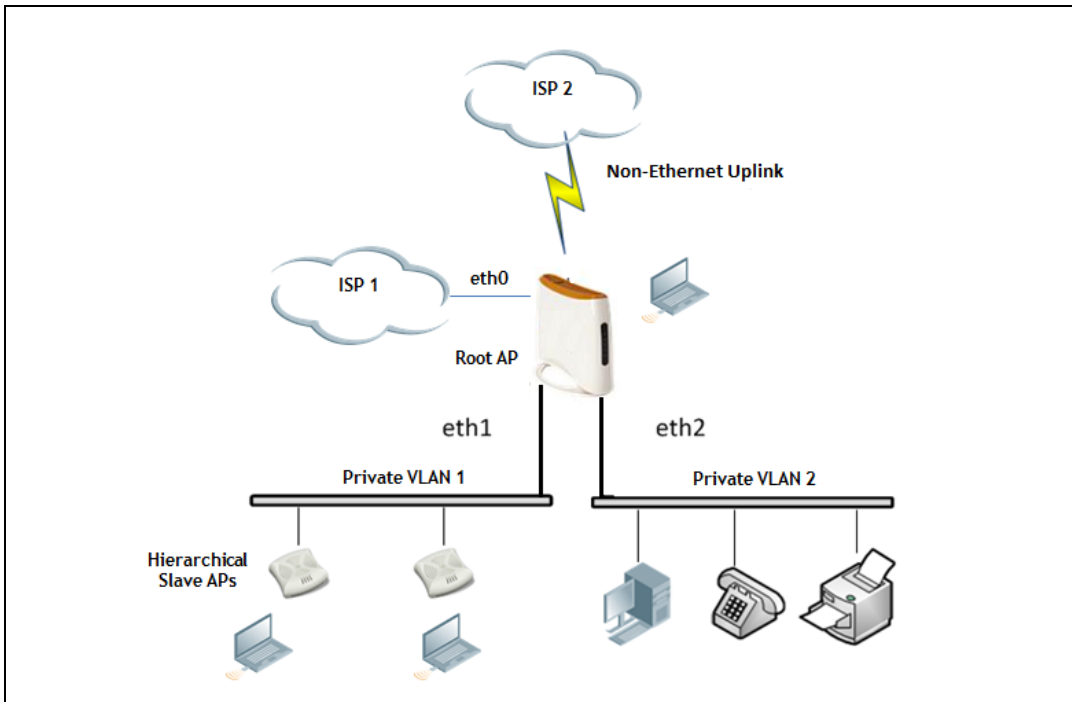
You can also form an OAW-IAP network by connecting the downlink port of an OAW-IAP to other OAW-IAPs. Only one OAW-IAP in the network uses its downlink port to connect to the other OAW-IAPs. This OAW-IAP (called the root OAW-IAP) acts as the wired device for the network, provides DHCP service and an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

A typical hierarchical deployment consists of the following:

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

The following figure illustrates a hierarchical deployment scenario:

Figure 31 Hierarchical Deployment



This chapter provides the following information:

- [Understanding Captive Portal on page 115](#)
- [Configuring a WLAN SSID for Guest Access on page 116](#)
- [Configuring Wired Profile for Guest Access on page 122](#)
- [Configuring Internal Captive Portal for Guest Network on page 124](#)
- [Configuring External Captive Portal for a Guest Network on page 127](#)
- [Configuring Facebook Login on page 133](#)
- [Configuring Guest Logon Role and Access Rules for Guest Users on page 134](#)
- [Configuring Captive Portal Roles for an SSID on page 136](#)
- [Configuring Walled Garden Access on page 139](#)
- [Disabling Captive Portal Authentication on page 140](#)

Understanding Captive Portal

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

The AOS-W Instant captive portal solution consists of the following:

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

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

Types of Captive Portal

AOS-W Instant supports the following types of captive portal authentication:

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

- **External captive portal**—For external captive portal authentication, an external portal on the cloud or on a server outside the enterprise network is used.

Walled Garden

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

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

Configuring a WLAN SSID for Guest Access

You can create an SSID for guest access by using the AOS-W Instant UI or the CLI:

In the AOS-W Instant UI

1. On the **Network** tab of the AOS-W Instant main window, click the **New** link. The **New WLAN** window is displayed.
2. Enter a name that uniquely identifies a wireless network in the **Name (SSID)** text box.
3. Select the **Guest** option for **Primary usage**.
4. Click the **Show advanced options** link. The advanced options for configuration are displayed.
5. Enter the required values for the following configuration parameters:

Table 24: WLAN Configuration Parameters

Parameter	Description
Broadcast filtering	<p>Select any of the following values:</p> <ul style="list-style-type: none"> ● All—When set to All, the OAW-IAP drops all broadcast and multicast frames except DHCP and ARP, IGMP group queries, and IPv6 neighbor discovery protocols. ● ARP—When set to ARP, the OAW-IAP drops all broadcast and multicast frames except DHCP and ARP, IGMP group queries, and IPv6 neighbor discovery protocols and additionally converts ARP requests to unicast and send frames directly to the associated client. ● Unicast-ARP-Only — When set to Unicast-ARP-Only, the OAW-IAP allows all broadcast and multicast frames as it is, however the ARP requests are converted to unicast frames and sends them to the associated clients. The broadcast filtering is set to Unicast-ARP-Only by default when an SSID profile is created. ● Disabled— When set to Disabled, all broadcast and multicast traffic is forwarded to the wireless interfaces.
Multicast transmission optimization	<p>Select Enabled if you want the OAW-IAP to select the optimal rate for sending broadcast and multicast frames based on the lowest of unicast rates across all associated clients. When this option is enabled, multicast traffic can be sent at up to 24 Mbps. The default rate for sending frames for 2.4 GHz is 1 Mbps and 5 GHz is 6 Mbps. This option is disabled by default.</p>
Dynamic multicast optimization	<p>Select Enabled to allow OAW-IAP to convert multicast streams into unicast streams over the wireless link. Enabling Dynamic Multicast Optimization (DMO) enhances the quality and reliability of streaming video, while preserving the bandwidth available to the non-video clients.</p> <p>NOTE: When you enable DMO on multicast SSID profiles, ensure that the DMO feature is enabled on all SSIDs configured in the same VLAN.</p>
DMO channel utilization threshold	<p>Specify a value to set a threshold for DMO channel utilization. With DMO, the OAW-IAP converts multicast streams into unicast streams as long as the channel utilization does not exceed this threshold. The default value is 90% and the maximum threshold value is 100%. When the threshold is reached or exceeds the maximum value, the OAW-IAP sends multicast traffic over the wireless link.</p>
Transmit Rates	<p>Specify the following parameters:</p> <ul style="list-style-type: none"> ● 2.4 GHz—If the 2.4 GHz band is configured on the OAW-IAP, specify the minimum and maximum transmission rate. The default value for minimum transmission rate is 1 Mbps and maximum transmission rate is 54 Mbps. ● 5 GHz—If the 5 GHz band is configured on the OAW-IAP, specify the minimum and maximum transmission rate. The default value for minimum transmission rate is 6 Mbps and maximum transmission rate is 54 Mbps.
Band	<p>Select a value to specify the band at which the network transmits radio signals. You can set the band to 2.4 GHz, 5 GHz, or All. The All option is selected by default.</p>

Table 24: WLAN Configuration Parameters

Parameter	Description
DTIM interval	The DTIM interval indicates the delivery traffic indication message (DTIM) period in beacons, which can be configured for every WLAN SSID profile. The DTIM interval determines how often the OAW-IAP should deliver the buffered broadcast and multicast frames to associated clients in the powersave mode. The default value is 1, which means the client checks for buffered data on the OAW-IAP at every beacon. You can also configure a higher DTIM value for power saving.
Min RSSI probe request	Sets a minimum Received signal strength indication (RSSI) threshold for probe requests.
Min RSSI auth request	Sets a minimum RSSI threshold for authentication requests.
Very high throughput	Enables VHT function on OAW-IAP devices that support VHT. For 802.11ac OAW-IAPs, the VHT function is enabled by default. However, you can disable the VHT function if you want the 802.11ac OAW-IAPs to function as 802.11n OAW-IAPs. If VHT is configured or disabled on an SSID, the changes will apply only to the SSID on which it is enabled or disabled.
Zone	Specify the zone for the SSID. When the zone is defined in SSID profile and if the same zone is defined on an OAW-IAP, the SSID is created on that OAW-IAP. For more information on configuring zone details, see Configuring Zone Settings on an OAW-IAP on page 65 . The following constraints apply to the zone configuration: <ul style="list-style-type: none"> • An OAW-IAP can belong to only one zone and only one zone can be configured on an SSID. • If an SSID belongs to a zone, all OAW-IAPs in this zone can broadcast this SSID. If no OAW-IAP belongs to the zone configured on the SSID, the SSID is not broadcast. • If an SSID does not belong to any zone, all OAW-IAPs can broadcast this SSID.
Time Range	Click Edit , select a Time Range Profile from the list and specify if the profile must be enabled or disabled for the SSID, and then click OK .
Bandwidth Limits	Under Bandwidth Limits : <ul style="list-style-type: none"> • Airtime—Select this check box to specify an aggregate amount of airtime that all clients in this network can use for sending and receiving data. Specify the airtime percentage. • Each radio—Select this check box to specify an aggregate amount of throughput that each radio is allowed to provide for the connected clients. • Downstream and Upstream—Specify the downstream and upstream rates within a range of 1 to 65,535 Kbps for the SSID users. If the assignment is specific for each user, select the Peruser check box.
Wi-Fi Multimedia (WMM) traffic management	Configure the following options for WMM traffic management. WMM supports voice, video, best effort, and background access categories. To allocate bandwidth for the following types of traffic, specify a percentage value under Share . To configure DSCP mapping, specify a value under DSCP Mapping . <ul style="list-style-type: none"> • Background WMM—For background traffic such as file downloads or print jobs.

Table 24: WLAN Configuration Parameters

Parameter	Description
	<ul style="list-style-type: none"> • Best effort WMM—For best effort traffic such as traffic from legacy devices or traffic from applications or devices that do not support QoS. • Video WMM—For video traffic generated from video streaming. • Voice WMM— For voice traffic generated from the incoming and outgoing voice communication. <p>For more information on WMM traffic and DSCP mapping, see Wi-Fi Multimedia Traffic Management on page 275</p> <p>For voice traffic and Spectralink Voice Prioritization, configure the following parameters:</p> <ul style="list-style-type: none"> • Traffic Specification (TSPEC)—To prioritize time-sensitive traffic such as voice traffic initiated by the client, select the Traffic Specification (TSPEC) check box. • TSPEC Bandwidth—To reserve bandwidth, set the TPSEC bandwidth to the desired value within the range of 200–600,000 Kbps. The default value is 2000 Kbps. • Spectralink Voice Protocol (SVP)—Select the check box to prioritize voice traffic for SVP handsets.
Content filtering	Select Enabled to route all DNS requests for the non-corporate domains to OpenDNS on this network.
Inactivity timeout	Specify an interval for session timeout in seconds, minutes or hours. If a client session is inactive for the specified duration, the session expires and the users are required to log in again. You can specify a value within the range of 60-86,400 seconds or up to 24 hours for a client session. The default value is 1000 seconds.
Deauth Inactive Clients	Select Enabled to allow the OAW-IAP to send a deauthentication frame to the inactive client and clear client entry.
SSID	<p>Select the Hide check box if you do not want the SSID (network name) to be visible to users.</p> <p>Select the Disable check box if you want to disable the SSID. On selecting this, the SSID will be disabled, but will not be removed from the network. By default, all SSIDs are enabled.</p>
Out of service (OOS)	<p>Enable or disable the SSID based on the following out-of-service states of the OAW-IAP:</p> <ul style="list-style-type: none"> • VPN down • Uplink down • Internet down • Primary uplink down <p>The network will be out of service when selected event occurs and the SSID is enabled or disabled as per the configuration settings applied. For example, if you select the VPN down option from the drop-down list and set the status to enabled, the SSID is enabled when the VPN connection is down and is disabled when the VPN connection is restored.</p>

Table 24: WLAN Configuration Parameters

Parameter	Description
OOS time (global)	Configure a hold time interval in seconds within a range of 30 to 300 seconds, after which the out-of-service operation is triggered. For example, if the VPN is down and the configured hold time is 45 seconds, the effect of this out-of-service state impacts the SSID availability after 45 seconds.
Max clients threshold	Specify the maximum number of clients that can be configured for each BSSID on a WLAN. You can specify a value within the range of 0 to 255. The default value is 64.
SSID Encoding	To encode the SSID, select UTF8. By default, the SSIDs are not encoded.
Deny inter user bridging	When enabled, the bridging traffic between two clients connected to the same SSID on the same VLAN is disabled. The clients can connect to the Internet, but cannot communicate with each other, and the bridging traffic between the clients is sent to the upstream device to make the forwarding decision.
ESSID	Enter the ESSID. If the value defined for ESSID value is not the same as profile name, the SSIDs can be searched based on the ESSID value and not by its profile name.

6. Click **Next** to configure VLAN settings. The VLAN tab contents are displayed.
7. Select any for the following options for **Client IP assignment**:
 - **Virtual Controller assigned**—On selecting this option, the client obtains the IP address from the VC.
 - **Network assigned**—On selecting this option, the IP address is obtained from the network.
8. Based on the type client IP assignment mode selected, you can configure the VLAN assignment for clients as described in the following table:

Table 25: IP and VLAN Assignment for WLAN SSID Clients

Client IP Assignment	Client VLAN Assignment
Virtual Controller assigned	<p>If the Virtual Controller assigned is selected for client IP assignment, the VC creates a private subnet and VLAN on the OAW-IAP for the wireless clients. The network address translation for all client traffic that goes out of this interface is carried out at the source. This setup eliminates the need for complex VLAN and IP address management for a multi-site wireless network.</p> <p>On selecting this option, the following client VLAN assignment options are displayed:</p> <ul style="list-style-type: none"> • Default: When selected, the default VLAN as determined by the VC is assigned for clients. • Custom: When selected, you can specify a custom VLAN assignment option. You can select an existing DHCP scope for client IP and VLAN assignment or you can create a new DHCP scope by selecting New. For more information on DHCP scopes, see Configuring DHCP Scopes on page 209.
Network assigned	<p>If the Network assigned is selected, you can specify any of the following options for the Client VLAN assignment.</p> <ul style="list-style-type: none"> • Default—On selecting this option, the client obtains the IP address in the same subnet as the OAW-IAPs. By default, the client VLAN is assigned to the native VLAN on the wired network. • Static—On selecting this option, you need to specify a single VLAN, a comma separated list of VLANS, or a range of VLANs for all clients on this network. Select this option for configuring VLAN pooling. • Dynamic—On selecting this option, you can assign the VLANs dynamically from a Dynamic Host Configuration Protocol (DHCP) server. To create VLAN assignment rules, click New to assign the user to a VLAN. In the New VLAN Assignment Rule window, enter the following information: <ul style="list-style-type: none"> • Attribute—Select an attribute returned by the RADIUS server during authentication. • Operator—Select an operator for matching the string. • String—Enter the string to match • VLAN—Enter the VLAN to be assigned.

9. Click **Next** to configure [internal](#) or [external captive portal authentication, roles, and access rules](#) for the guest users.



If the client IP assignment mode is set to **Network assigned** in a guest SSID profile, the guest clients can log out of the captive portal network by accessing the <https://securelogin.arubanetworks.com/auth/logout.html> URL.

In the CLI

To configure WLAN settings for an SSID profile:

```
(Instant AP) (config)# wlan ssid-profile <name>
(Instant AP) (SSID Profile <name>)# essid <ESSID-name>
(Instant AP) (SSID Profile <name>)# type <Guest>
(Instant AP) (SSID Profile <name>)# broadcast-filter <type>
(Instant AP) (SSID Profile <name>)# dtim-period <number-of-beacons>
(Instant AP) (SSID Profile <name>)# multicast-rate-optimization
(Instant AP) (SSID Profile <name>)# dynamic-multicast-optimization
(Instant AP) (SSID Profile <name>)# dmo-channel-utilization-threshold
```

```
(Instant AP) (SSID Profile <name>)# a-max-tx-rate <rate>
(Instant AP) (SSID Profile <name>)# a-min-tx-rate <rate>
(Instant AP) (SSID Profile <name>)# g-max-tx-rate <rate>
(Instant AP) (SSID Profile <name>)# g-min-tx-rate <rate>
(Instant AP) (SSID Profile <name>)# zone <zone>
(Instant AP) (SSID Profile <name>)# bandwidth-limit <limit>
(Instant AP) (SSID Profile <name>)# per-user-bandwidth-limit <limit>
(Instant AP) (SSID Profile <name>)# air-time-limit <limit>
(Instant AP) (SSID Profile <name>)# wmm-background-share <percentage-of-traffic_share>
(Instant AP) (SSID Profile <name>)# wmm-best-effort-share<percentage-of-traffic-share>
(Instant AP) (SSID Profile <name>)# wmm-video-share <percentage-of-traffic_share>
(Instant AP) (SSID Profile <name>)# wmm-voice-share <percentage-of-traffic_share>
(Instant AP) (SSID Profile <name>)# rf-band {<2.4>|<5.0>|<all>}
(Instant AP) (SSID Profile <name>)# content-filtering
(Instant AP) (SSID Profile <name>)# hide-ssid
(Instant AP) (SSID Profile <name>)# inactivity-timeout <interval>
(Instant AP) (SSID Profile <name>)# local-probe-req-thresh <threshold>
(Instant AP) (SSID Profile <name>)# max-clients-threshold <number-of-clients>
```

To manually assign VLANs for WLAN SSID users:

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

To create a new VLAN assignment rule:

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

Configuring Wired Profile for Guest Access

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

In the AOS-W Instant UI

1. Click the **Wired** link under **More** on the AOS-W Instant main window. The **Wired** window is displayed.
2. Click **New** under **Wired Networks**. The **New Wired Network** window is displayed.
3. Click the **Wired Settings** tab and enter the following information:
 - a. **Name**—Specify a name for the profile.
 - b. **Primary Usage**—Select **Employee** or **Guest**.
 - c. **Speed/Duplex**—Ensure that appropriate values are selected for **Speed/Duplex**. Contact your network administrator if you need to assign speed and duplex parameters.
 - d. **POE**—Set **POE to Enabled** to enable Power over Ethernet.
 - e. **Admin Status**—Ensure that an appropriate value is selected. The **Admin Status** indicates if the port is up or down.
 - f. **Content Filtering**—To ensure that all DNS requests to non-corporate domains on this wired network are sent to OpenDNS, select **Enabled** for **Content Filtering**.
 - g. **Uplink**—Select **Enabled** to configure uplink on this wired profile. If **Uplink** is set to **Enabled** and this network profile is assigned to a specific port, the port will be enabled as Uplink port. For more information on assigning a wired network profile to a port, see [Assigning a Profile to Ethernet Ports on page 111](#).
 - h. **Spanning Tree**—Select the **Spanning Tree** check box to enable Spanning Tree Protocol (STP) on the wired profile. STP ensures that there are no loops in any bridged Ethernet network and operates on all downlink ports, regardless of forwarding mode. STP will not operate on the uplink port and is supported only on OAW-IAPs with three or more ports. By default Spanning Tree is disabled on wired profiles.
4. Click **Next**. The VLAN tab details are displayed.

5. Enter the following information.
 - a. **Mode**—You can specify any of the following modes:
 - **Access**—Select this mode to allow the port to carry a single VLAN specified as the native VLAN.
 - **Trunk**—Select this mode to allow the port to carry packets for multiple VLANs specified as allowed VLANs.
 - b. Specify any of the following values for **Client IP Assignment**:
 - **Virtual Controller Assigned**: Select this option to allow the VC to assign IP addresses to the wired clients. When the VC assignment is used, the source IP address is translated for all client traffic that goes through this interface. The VC can also assign a guest VLAN to a wired client.
 - **Network Assigned**: Select this option to allow the clients to receive an IP address from the network to which the VC is connected. On selecting this option, the **New** button to create a VLAN is displayed. Create a new VLAN if required.
 - c. If the **Trunk** mode is selected:
 - Specify the **Allowed VLAN**, enter a list of comma separated digits or ranges: for example, 1,2,5 or 1–4, or all. The Allowed VLAN refers to the VLANs carried by the port in Access mode.
 - If the **Client IP Assignment** is set to **Network Assigned**, specify a value for **Native VLAN**. A VLAN that does not have a VLAN ID tag in the frames is referred to as Native VLAN. You can specify a value within the range of 1–4093.
 - d. If the **Access** mode is selected:
 - If the **Client IP Assignment** is set to **Virtual Controller Assigned**, proceed to step 2.
 - If the **Client IP Assignment** is set to **Network Assigned**, specify a value for **Access VLAN** to indicate the VLAN carried by the port in the **Access** mode.
6. Click **Next** to configure [internal](#) or [external captive portal authentication, roles, and access rules](#) for the guest users.

In the CLI

To configure the settings for the wired profile:

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

To configure VLAN settings for a wired profile:

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

To configure a new VLAN assignment rule:

```
(Instant AP) (config)# wired-port-profile <name>
(Instant AP) (wired ap profile <name>)# set-vlan <attribute>{equals|not-equals|starts-with|ends-with|contains|matches-regular-expression} <operator> <VLAN-ID>|value-of}
```

Configuring Internal Captive Portal for Guest Network

For internal captive portal authentication, an internal server is used for hosting the captive portal service. You can configure internal captive portal authentication when adding or editing a guest network created for wireless or wired profile through the AOS-W Instant UI or the CLI.

In the AOS-W Instant UI

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

Table 26: Internal Captive Portal Configuration Parameters

Parameter	Description
Splash page type	Select any of the following from the drop-down list. <ul style="list-style-type: none">• Internal - Authenticated—When Internal Authenticated is enabled, the guest users are required to authenticate in the captive portal page to access the Internet. The guest users who are required to authenticate must already be added to the user database.• Internal - Acknowledged—When Internal Acknowledged is enabled, the guest users are required to accept the terms and conditions to access the Internet.
MAC authentication	Select Enabled from the Mac Authentication drop-down list to enable MAC authentication.
Delimiter character	Specify a character (for example, colon or dash) as a delimiter for the MAC address string. When configured, the OAW-IAP will use the delimiter in the MAC authentication request. For example, if you specify colon as the delimiter, MAC addresses in the xx:xx:xx:xx:xx:xx format are used. If the delimiter is not specified, the MAC address in the xxxxxxxxxxxx format is used. NOTE: This option is available only when MAC authentication is enabled.
Uppercase support	Set to Enabled to allow the OAW-IAP to use uppercase letters in MAC address string for MAC authentication. NOTE: This option is available only if MAC authentication is enabled.
WISPr (Applicable for WLAN SSIDs only.)	Select Enabled if you want to enable WISPr authentication. For more information on WISPr authentication, see Configuring WISPr Authentication on page 173 . NOTE: The WISPr authentication is applicable only for Internal-Authenticated splash pages and is not applicable for wired profiles.
Auth server 1 Auth server 2	Select any one of the following: <ul style="list-style-type: none">• A server from the list of servers, if the server is already configured.

Table 26: Internal Captive Portal Configuration Parameters

Parameter	Description
	<ul style="list-style-type: none">• Internal Server to authenticate user credentials at run time.• Select New for configuring a new external RADIUS or LDAP server for authentication.
Load balancing	Select Enabled to enable load balancing if two authentication servers are used.
Reauth interval	Select a value to allow the OAW-IAPs to periodically reauthenticate all associated and authenticated clients.
Blacklisting (Applicable for WLAN SSIDs only.)	If you are configuring a wireless network profile, select Enabled to enable blacklisting of the clients with a specific number of authentication failures.
Accounting mode (Applicable for WLAN SSIDs only)	Select an accounting mode from the Accounting mode drop-down list for posting accounting information at the specified accounting interval. When the accounting mode is set to Authentication , the accounting starts only after client authentication is successful and stops when the client logs out of the network. If the accounting mode is set to Association , the accounting starts when the client associates to the network successfully and stops when the client is disconnected.

Table 26: Internal Captive Portal Configuration Parameters

Parameter	Description
Accounting interval	Configure an accounting interval in minutes within the range of 0-60, to allow OAW-IAPs to periodically post accounting information to the RADIUS server.
Encryption (Applicable for WLAN SSIDs only.)	Select Enabled to configure encryption parameters. Select an encryption and configure a passphrase.
Splash Page Design	<p>Under Splash Page Visuals, use the editor to specify display text and colors for the initial page that will be displayed to the users when they connect to the network. The initial page asks for user credentials or email, depending on the splash page type (Internal - Authenticated or Internal - Acknowledged).</p> <p>To customize the splash page design, perform the following steps:</p> <ul style="list-style-type: none"> • To change the color of the splash page, click the Splash page rectangle and select the required color from the Background Color palette. • To change the welcome text, click the first square box in the splash page, type the required text in the Welcome text box, and click OK. Ensure that the welcome text does not exceed 127 characters. • To change the policy text, click the second square box in the splash page, type the required text in the Policy text box, and click OK. Ensure that the policy text does not exceed 255 characters. • To upload a custom logo, click Upload your own custom logo image, browse the image file, and click upload image. Ensure that the image file size does not exceed 16 KB. • To redirect users to another URL, specify a URL in Redirect URL. • Click Preview to preview the captive portal page. <p>NOTE: You can customize the captive portal page using double-byte characters. Traditional Chinese, Simplified Chinese, and Korean are a few languages that use double-byte characters. Click the banner, term, or policy in the Splash Page Visuals to modify the text in the red box. These fields accept double-byte characters or a combination of English and double-byte characters.</p>

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

In the CLI

To configure internal captive portal authentication:

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

To configure internal captive portal for a wired profile:

```
(Instant AP) (config)# wired-port-profile <name>
(Instant AP) (wired ap profile <name>)# type <guest>
(Instant AP) (wired ap profile <name>)# captive-portal {<internal-authenticated>|<internal-acknowledged>} exclude-uplink {3G|4G|Wifi|Ethernet}
(Instant AP) (wired ap profile <name>)# mac-authentication
(Instant AP) (wired ap profile <name>)# auth-server <server1>
(Instant AP) (wired ap profile <name>)# radius-reauth-interval <Minutes>
(Instant AP) (wired ap profile <name>)# end
(Instant AP)# commit apply
```

To customize internal captive portal splash page:

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

To upload a customized logo from a TFTP server to the OAW-IAP:

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

Configuring External Captive Portal for a Guest Network

This section provides the following information:

- [External Captive Portal Profiles on page 127](#)
- [Creating a Captive Portal Profile on page 127](#)
- [Configuring an SSID or Wired Profile to Use External Captive Portal Authentication on page 129](#)
- [External Captive Portal Redirect Parameters](#)

External Captive Portal Profiles

You can now configure external captive portal profiles and associate these profiles to a user role or SSID. You can create a set of captive portal profiles in the **External Captive Portal** window (accessed from the **Security** tab) and associate these profiles with an SSID or a wired profile. You can also create a new captive portal profile on the **Security** tab of the WLAN wizard or a Wired Network window. In the current release, you can configure up to 16 external captive portal profiles.

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

Creating a Captive Portal Profile

You can create a captive portal profile using the AOS-W Instant UI or the CLI.

In the AOS-W Instant UI

1. Go to **Security > External Captive Portal**.
2. Click **New**. The **New** popup window is displayed.
3. Specify values for the following parameters:

Table 27: Captive Portal Profile Configuration Parameters

Parameter	Description
Name	Enter a name for the profile.
Type	Select any one of the following types of authentication: <ul style="list-style-type: none"> ● Radius Authentication—Select this option to enable user authentication against a RADIUS server. ● Authentication Text—Select this option to specify an authentication text. The specified text will be returned by the external server after a successful user authentication.
IP or hostname	Enter the IP address or the host name of the external splash page server.
URL	Enter the URL for the external captive portal server.
Port	Enter the port number.
Use https (Available only if RADIUS Authentication is selected)	Select Enabled to enforce clients to use HTTPS to communicate with the captive portal server.
Captive Portal failure	Allows you to configure Internet access for the guest clients when the external captive portal server is not available. Select Deny Internet to prevent clients from using the network, or Allow Internet to allow the guest clients to access Internet when the external captive portal server is not available.
Automatic URL Whitelisting	Select Enabled to enable the automatic whitelisting of URLs. On selecting the check box for the external captive portal authentication, the URLs that are allowed for the unauthenticated users to access are automatically whitelisted. The automatic URL whitelisting is disabled by default.
Auth Text (Available only if Authentication Text is selected)	If the External Authentication splash page is selected, specify the authentication text to be returned by the external server after successful authentication.
Server Offload	Select Enabled to enable server offload. The server offload feature ensures that the non-browser client applications are not unnecessarily redirected to the external portal server and thereby reducing the load on the external captive portal server. The Server Offload option is Disabled by default.
Prevent frame overlay	When the Prevent frame overlay option is enabled, a frame can display a page only if it is in the same domain as the main page. This option is Enabled by default and can be used to prevent the overlay of frames.
Switch IP	Sends the IP address of the VC in the redirection URL when external captive portal servers are used. This option is disabled by default.
Redirect URL	Specify a redirect URL if you want to redirect the users to another URL.

In the CLI

To configure an external captive portal profile:

```
(Instant AP) (config)# wlan external-captive-portal [profile_name]
(Instant AP) (External Captive Portal)# server <server>
(Instant AP) (External Captive Portal)# port <port>
(Instant AP) (External Captive Portal)# url <url>
(Instant AP) (External Captive Portal)# https
(Instant AP) (External Captive Portal)# redirect-url <url>
(Instant AP) (External Captive Portal)# server-fail-through
(Instant AP) (External Captive Portal)# no auto-whitelist-disable
(Instant AP) (External Captive Portal)# server-offload
(Instant AP) (External Captive Portal)# switch-ip
(Instant AP) (External Captive Portal)# prevent-frame-overlay
(Instant AP) (External Captive Portal)# end
(Instant AP)# commit apply
```

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

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

In the AOS-W Instant UI

1. Navigate to the WLAN wizard or Wired window.
 - To configure external captive portal authentication for a WLAN SSID, on the **Network** tab, click **New** to create a new network profile or **edit** to modify an existing profile.
 - To configure external captive portal authentication for a wired profile, Go to **More > Wired**. In the **Wired** window, click **New** under **Wired Networks** to create a new network, or click **Edit** to select an existing profile.
2. On the **Security** tab, select **External** from the **Splash page type** drop-down list.
3. From the **Captive Portal Profile** drop-down list, select a profile. You can select and modify a default profile, or an already existing profile, or click **New** and [create a new profile](#).
4. Configure the following parameters based on the type of splash page you selected.

Table 28: External Captive Portal Configuration Parameters

Parameter	Description
Captive-portal proxy server	If required, configure a captive portal proxy server or a global proxy server to match your browser configuration by specifying the IP address and port number in the Captive-portal proxy server text box.
WISPr	Select Enabled if you want to enable WISPr authentication. For more information on WISPr authentication, see Configuring WISPr Authentication on page 173 . NOTE: The WISPr authentication is applicable only for the External and Internal-Authenticated splash pages and is not applicable for wired profiles.
MAC authentication	Select Enabled if you want to enable MAC authentication. For information on MAC authentication, see Configuring MAC Authentication for a Network Profile on page 169 .

Table 28: External Captive Portal Configuration Parameters

Parameter	Description
Delimiter character	<p>Specify a character (for example, colon or dash) as a delimiter for the MAC address string. When configured, the OAW-IAP will use the delimiter in the MAC authentication request. For example, if you specify colon as the delimiter, MAC addresses in the xx:xx:xx:xx:xx:xx format are used. If the delimiter is not specified, the MAC address in the xxxxxxxxxxxx format is used.</p> <p>NOTE: This option is available only when MAC authentication is enabled.</p>
Uppercase support	<p>Set to Enabled to allow the OAW-IAP to use uppercase letters in MAC address string for MAC authentication.</p> <p>NOTE: This option is available only if MAC authentication is enabled.</p>
Authentication server	<p>To configure an authentication server, select any of the following options:</p> <ul style="list-style-type: none">• If the server is already configured, select the server from the list.• To create new external RADIUS server, select New. For more information, see Configuring an External Server for Authentication on page 154.
Reauth interval	<p>Specify a value for the reauthentication interval at which the OAW-IAPs periodically reauthenticate all associated and authenticated clients.</p>
Accounting mode	<p>Select an accounting mode from the Accounting mode drop-down list for posting accounting information at the specified Accounting interval. When the accounting mode is set to Authentication, the accounting starts only after client authentication is successful and stops when the client logs out of the network. If the accounting mode is set to Association, the accounting starts when the client associates to the network successfully and stops when the client is disconnected.</p>
Accounting interval	<p>Configure an accounting interval in minutes within the range of 0–60, to allow OAW-IAPs to periodically post accounting information to the RADIUS server.</p>
Blacklisting	<p>If you are configuring a wireless network profile, select Enabled to enable blacklisting of the clients with a specific number of authentication failures.</p>
Max authentication failures	<p>If you are configuring a wireless network profile and Blacklisting is enabled, specify the maximum number of authentication failures after which users who fail to authenticate must be dynamically blacklisted.</p>
Walled garden	<p>Click the link to open the Walled Garden window. The walled garden configuration determines access to the websites. For more information, see Configuring Walled Garden Access on page 139.</p>
Disable if uplink type is	<p>Select the type of the uplink to exclude.</p>
Encryption	<p>Select Enabled to configure encryption settings and specify the encryption parameters.</p>

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

In the CLI

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

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

To configure security settings for guest users of the wired profile:

```
(Instant AP) (config)# wired-port-profile <name>
(Instant AP) (wired ap profile <name>)# type <Guest>
(Instant AP) (wired ap profile <name>)# captive-portal{<type>[exclude-uplink <types>]|external
[exclude-uplink <types>] profile <name>[exclude-uplink <types>]]}
(Instant AP) (wired ap profile <name>)# mac-authentication
(Instant AP) (wired ap profile <name>)# end
(Instant AP)# commit apply
```

External Captive Portal Redirect Parameters

If the external captive portal redirection is enabled on a network profile, OAW-IAP sends an HTTP response with the redirect URL to display the splash page and enforce captive portal authentication by clients. The HTTP response from the OAW-IAP includes the following parameters:

Table 29: External Captive Portal Redirect Parameters

Parameter	Example Value	Description
cmd	login	Type of operation
mac	34:02:86:c6:d2:3e	Client MAC address
ssid	guest-ecp-109	ESSID
ip	192.0.2.0	Client IP address
apname	9c:1c:12:cb:a2:90	OAW-IAP host name
apmac	9c:1c:12:cb:a2:90	OAW-IAP MAC address
vcname	instant-C8:1D:DA"	VC name
switchip	securelogin.arubanetworks.com	Captive portal domain used for external captive portal authentication
url	http://www.google.com/	original URL

Configuring External Captive Portal Authentication Using ClearPass Guest

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

Creating a Web Login Page in ClearPass Guest

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

For more information on setting up the RADIUS web login page, refer to the *RADIUS Services* section in the *ClearPass Guest Deployment Guide*.

Configuring RADIUS Server in AOS-W Instant UI

To configure AOS-W Instant to point to ClearPass Guest as an external captive portal server:

1. Select the WLAN SSID for which you want to enable external captive portal authentication with ClearPass Policy Manager. You can also configure the RADIUS server when configuring a new SSID profile.
2. On the **Security** tab, select **External** from the **Splash page type** drop-down list.
3. Select **New** from the **Captive portal profile** drop-down list and update the following:
 - a. Enter the IP address of the ClearPass Guest server in the **IP or hostname** text box. Obtain the ClearPass Guest IP address from your system administrator.
 - b. Enter **/page_name.php** in the **URL** text box. This URL must correspond to the **Page Name** configured in the ClearPass Guest RADIUS Web Login page. For example, if the Page Name is **Alcatel-Lucent**, the URL should be **/Alcatel-Lucent.php** in the AOS-W Instant UI.
 - c. Enter the **Port** number (generally should be **80**). The ClearPass Guest server uses this port for HTTP services.
 - d. Click **OK**.
4. To create an external RADIUS server, select **New** from the **Authentication server 1** drop-down list. For information on authentication server configuration parameters, see [Configuring an External Server for Authentication on page 154](#).
5. Click **Next** and then click **Finish**.
6. Click the updated SSID in the **Network** tab.
7. Open any browser and type any URL. AOS-W Instant redirects the URL to ClearPass Guest login page.
8. Log in to the network with the username and password specified while configuring the RADIUS server.

Configuring RADIUS Attribute for ClearPass Policy Manager Server Load Balancing

Starting from AOS-W Instant 6.4.3.4-4.2.1.0, the administrators can configure a RADIUS server IP address as one of the parameters on ClearPass Policy Manager server for external captive portal user authentication. Configuring a RADIUS server attribute for guest user authentication allows the administrators to balance the load on the ClearPass Policy Manager servers.

When the RADIUS server IP address is configured under **Extra Fields** in the ClearPass Guest login page, the RADIUS server IP parameter is submitted to the server as part of the HTTP or HTTPS POST data when the guest users initiate an HTTP or HTTPS request. The OAW-IAP intercepts this information to perform the actual RADIUS authentication with the server IP defined in the POST message. For more information on guest registration customization on ClearPass Guest, refer to the *ClearPass Guest User Guide*.

Configuring Facebook Login

AOS-W Instant supports the Facebook Wi-Fi feature that allows the captive portal clients using a Facebook account to authenticate on an OAW-IAP. You can configure a guest network to use a customized Facebook page as an external captive portal URL and allow the OAW-IAP to redirect clients to a Facebook page when it receives an HTTP request. The users can select the appropriate option to authenticate and access the Internet. By configuring the Facebook login feature, businesses can pair their network with the Facebook Wi-Fi service, so that the users logging into Wi-Fi hotspots are presented with a business page, before gaining access to the network.

The Facebook Wi-Fi integration with the OAW-IAP includes the following procedures:

- [Setting up a Facebook Page](#)
- [Configuring an SSID](#)
- [Configuring the Facebook Portal Page](#)
- [Accessing the Portal Page](#)

Setting up a Facebook Page

To enable integration with the OAW-IAP, ensure that you have a Facebook page created as a local business with a valid location.

- For more information on creating a Facebook page, see the online help available at <https://www.facebook.com/help>.
- For more information on setting up and using Facebook Wi-Fi service, see <https://www.facebook.com/help/126760650808045>.

Configuring an SSID

You can configure a guest network profile and enable Facebook login through the AOS-W Instant UI or the CLI.

In the AOS-W Instant UI

To enable Facebook login:

1. Navigate to **Network > New** to create a new network profile.
2. Enter a name for the SSID.
3. Select **Guest** under **Primary usage**.
4. Configure other required parameters in the **WLAN Settings** and **VLAN** tabs.
5. On the **Security** tab, select **Facebook** from the **Splash page type** drop-down list.
6. Click **Next**. The **Access** tab contents are displayed.
7. Click **OK**. The SSID with the Facebook option is created. After the SSID is created, the OAW-IAP automatically registers with Facebook. If the OAW-IAP registration is successful, the **Facebook configuration** link is displayed in the **Security** tab of the WLAN wizard.

In the CLI

To configure an account for captive portal authentication:

```
(Instant AP) (config)# wlan ssid-profile <name>
(Instant AP) (SSID Profile <name>)# captive-portal {<type>[exclude-uplink <types>]|external
[exclude-uplink <types>]|profile <name>[exclude-uplink <types>]]}
(Instant AP) (SSID Profile <name>)# end
(Instant AP)# commit apply
```

Example

The following example configures a Facebook account for captive portal authentication:

```
(Instant AP) (config)# wlan ssid-profile guestNetwork
(Instant AP) (SSID Profile "guestNetwork")# captive-portal facebook
(Instant AP) (SSID Profile "guestNetwork")# end
(Instant AP)# commit apply
```

Configuring the Facebook Portal Page

To bind the VC with the Facebook portal:

1. Open the SSID with the Facebook option enabled, navigate to the **Security** tab and click the **Facebook configuration** link. The Facebook page is displayed.



The **Facebook configuration** link is displayed only if the OAW-IAP is successfully registered with Facebook.

2. Log in with your Facebook credentials. The **Facebook Wi-Fi Configuration** page is displayed.
3. Select the Facebook page.
4. Under **Bypass Mode**, select any of the following options:
 - **Skip Check-in link**—When selected, the users are not presented with your business Facebook page, but are allowed to access the Internet by clicking the **Skip Check-in** link.
 - **Require Wi-Fi code**—When selected, the users are assigned a Wi-Fi code to gain access to the Facebook page.
5. Customize the session length and terms of service if required.
6. Click **Save Settings**.

Accessing the Portal Page

To access the portal page:

1. Connect to the SSID with the Facebook option enabled.
2. Launch a web browser. The browser opens the Facebook Wi-Fi page. If the Wi-Fi-code based login is enabled, the users are prompted to enter the Wi-Fi code. If the **Skip Check-in** link is displayed, click the link to skip checking in to the Facebook business page and proceed to access the Internet.
3. If you want to check in the business page, click **Check In** and provide your credentials. After checking in, click **Continue Browsing** to access the web page that was originally requested.

Configuring Guest Logon Role and Access Rules for Guest Users

For captive portal profile, you can create any the following types of roles:

- A pre-authenticated role—This role is assigned before the captive portal authentication. The user can only access certain destinations with this role.
- A guest role—This role is assigned after user authentication.
- A captive-portal role—This role can be assigned to any network such as Employee, Voice, or Guest. When the user is assigned with this role, a splash page is displayed after opening a browser and the users may need to authenticate.

You can configure up to 128 access rules for guest user roles through the AOS-W Instant UI or the CLI.

In the AOS-W Instant UI

To configure roles and access rules for the guest network:

1. On the **Access Rules** tab, set the slider to any of the following types of access control:
 - **Unrestricted**—Select this to set unrestricted access to the network.
 - **Network-based**—Set the slider to **Network-based** to set common rules for all users in a network. The **Allow any to all destinations** access rule is enabled by default. This rule allows traffic to all destinations. To define an access rule:
 - a. Click **New**.
 - b. Select appropriate options in the **New Rule** window.
 - c. Click **OK**.
 - **Role-based**—Select **Role-based** to enable access based on user roles.

For role-based access control:

- Create a user role if required. For more information, see [Configuring User Roles](#).
- Create access rules for a specific user role. For more information, see [Configuring ACL Rules for Network Services on page 180](#). You can also configure an access rule to enforce captive portal authentication for an SSID with the 802.1X authentication method. For more information, see [Configuring Captive Portal Roles for an SSID on page 136](#).
- Create a role assignment rule. For more information, see [Configuring Derivation Rules on page 199](#). AOS-W Instant supports role derivation based on the DHCP option for captive portal authentication. When the captive portal authentication is successful, a new user role is assigned to the guest users based on DHCP option configured for the SSID profile instead of the pre-authenticated role.

2. Click **Finish**.

In the CLI

To configure access control rules for a WLAN SSID:

```
(Instant AP) (config)# wlan access-rule <name>
(Instant AP) (Access Rule <name>)# rule <dest> <mask> <match> {<protocol> <start-port> <end-
port> {permit|deny|src-nat|dst-nat{<IP-address> <port>|<port>}}| app <app> {permit|deny}|
appcategory <appgrp>|webcategory <webgrp> {permit|deny}|webreputation <webrep>
[<option1...option9>]
(Instant AP) (Access Rule <name>)# end
(Instant AP)# commit apply
```

To configure access control rules based on the SSID:

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

To configure role assignment rules:

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

To configure a pre-authentication role:

```
(Instant AP) (config)# wlan ssid-profile <name>
(Instant AP) (SSID Profile <name>)# set-role-pre-auth <role>
```

```
(Instant AP) (SSID Profile <name>)# end
(Instant AP)# commit apply
```

To configure machine and user authentication roles:

```
(Instant AP) (config)# wlan ssid-profile <name>
(Instant AP) (SSID Profile <name>)# set-role-machine-auth <machine_only> <user_only>
(Instant AP) (SSID Profile <name>)# end
(Instant AP)# commit apply
```

To configure unrestricted access:

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

Example

The following example configures access rules for the wireless network:

```
(Instant AP) (config)# wlan access-rule WirelessRule
(Instant AP) (Access Rule "WirelessRule")# rule 192.0.2.2 255.255.255.0 match 6 4343 4343 log
classify-media
(Instant AP) (Access Rule "WirelessRule")# rule any any match app deny throttle-downstream 256
throttle-up 256
(Instant AP) (Access Rule "WirelessRule")# rule any any match appcategory collaboration permit
(Instant AP) (Access Rule "WirelessRule")# rule any any match webcategory gambling deny
(Instant AP) (Access Rule "WirelessRule")# rule any any match webcategory training-and-tools
permit
(Instant AP) (Access Rule "WirelessRule")# rule any any match webreputation well-known-sites
permit
(Instant AP) (Access Rule "WirelessRule")# rule any any match webreputation safe-sites permit
(Instant AP) (Access Rule "WirelessRule")# rule any any match webreputation benign-sites permit
(Instant AP) (Access Rule "WirelessRule")# rule any any match webreputation suspicious-sites
deny
(Instant AP) (Access Rule "WirelessRule")# rule any any match webreputation high-risk-sites
deny
(Instant AP) (Access Rule "WirelessRule")# end
(Instant AP)# commit apply
```

Configuring Captive Portal Roles for an SSID

You can configure an access rule to enforce captive portal authentication for SSIDs that use 802.1X authentication to authenticate clients. You can configure rules to provide access to external or internal captive portal, so that some of the clients using this SSID can derive the captive portal role.

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

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

You can create a captive portal role for both **Internal** and **External** splash page types.

To enforce the captive portal role, use the AOS-W Instant UI or the CLI.

In the AOS-W Instant UI

To create a captive portal role:

1. Select an SSID profile from the **Network** tab. The **Edit <WLAN-Profile>** window is displayed.

2. On the **Access** tab, move the slider to **Role-based** access control by using the scroll bar.
3. Select a role or create a new one if required.
4. Click **New** to add a new rule. The **New Rule** window is displayed.
5. In the **New Rule** window, specify the following parameters. The following figures show the parameters for captive portal role configuration:

Figure 32 Captive Portal Rule for **Internal** Splash Page Type

The screenshot shows the 'New Rule' configuration window. At the top, 'Rule type' is set to 'Captive portal' and 'Splash page type' is set to 'Internal'. Below this, there is a section for 'Splash Page Visuals' which includes a preview of a splash page. The preview shows a header 'Welcome to Guest Network' in an orange bar, followed by two columns of text: 'New to the Stream network?' and 'No User Policy'. Below the preview is a link to 'Upload your own custom logo image' and a note to 'Click thumbnail above to edit'. A 'Preview' button is located to the right. At the bottom, there is a 'Redirect URL' field with '(optional)' next to it. 'OK' and 'Cancel' buttons are at the bottom right.

Figure 33 Captive Portal Rule for **External** Splash Page Type

The screenshot shows the 'New Rule' configuration window. At the top, 'Rule type' is set to 'Captive portal', 'Splash page type' is set to 'External', and 'Captive portal profile' is set to '-- Select Profile --'. 'OK' and 'Cancel' buttons are at the bottom right.

Table 30: Captive Portal Rule Configuration Parameters

Parameter	Description
Rule type	Select Captive Portal from the RuleType drop-down list.
Splash Page Type	Select any of the following attributes: <ul style="list-style-type: none"> • Select Internal to configure a rule for internal captive portal authentication. • Select External to configure a rule for external captive portal authentication.
Internal	If Internal is selected as splash page type, perform the following steps: <ul style="list-style-type: none"> • Under Splash Page Visuals, use the editor to specify display text and colors for the initial page that would be displayed to users connecting to the network. The initial page asks for user credentials or email, depending on the splash page type configured. • To change the color of the splash page, click the Splash page rectangle and select the required color from the Background Color palette.

Table 30: Captive Portal Rule Configuration Parameters

Parameter	Description
	<ul style="list-style-type: none"> To change the welcome text, click the first square box in the splash page, type the required text in the Welcome text box, and then click OK. Ensure that the welcome text does not exceed 127 characters. To change the policy text, click the second square box in the splash page, type the required text in the Policy text box, and click OK. Ensure that the policy text does not exceed 255 characters. Specify the URL to which you want to redirect the guest users. To upload a custom logo, click Upload your own custom logo image, browse the image file, and click upload image. To preview the captive portal page, click Preview.
External	<p>If External is selected, perform the following steps:</p> <ul style="list-style-type: none"> Select a profile from the Captive portal profile drop-down list. If you want to edit the profile, click Edit and update the following parameters: <ul style="list-style-type: none"> Type—Select either Radius Authentication (to enable user authentication against a RADIUS server) or Authentication Text (to specify the authentication text to be returned by the external server after a successful user authentication). IP or hostname— Enter the IP address or the host name of the external splash page server. URL— Enter the URL for the external splash page server. Port—Enter the port number. Redirect URL—Specify a redirect URL if you want to redirect the users to another URL. Captive Portal failure—The Captive Portal failure drop-down list allows you to configure Internet access for the guest clients when the external captive portal server is not available. Select Deny Internet to prevent clients from using the network, or Allow Internet to allow the guest clients to access Internet when the external captive portal server is not available. Automatic URL Whitelisting—Select Enabled or Disabled to enable or disable automatic whitelisting of URLs. On selecting the check box for the external captive portal authentication, the URLs allowed for the unauthenticated users to access are automatically whitelisted. The automatic URL whitelisting is disabled by default. Auth Text—Indicates the authentication text returned by the external server after a successful user authentication.

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

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

In the CLI

To create a captive portal role:

```
(Instant AP) (config)# wlan access-rule <Name>
(Instant AP) (Access Rule <Name>)# captive-portal {external [profile <name>]|internal}
(Instant AP) (Access Rule <Name>)# end
(Instant AP)# commit apply
```

Configuring Walled Garden Access

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

The users who do not sign up for the Internet service can view the allowed websites (typically hotel property websites). The website names must be DNS-based and support the option to define wildcards. When a user attempts to navigate to other websites that are not in the whitelist of the walled garden profile, the user is redirected to the login page. OAW-IAP supports walled garden only for the HTTP requests. For example, if you add yahoo.com in walled garden whitelist and the client sends an HTTPS request (https://yahoo.com), the requested page is not displayed and the users are redirected to the captive portal login page.

In addition, a blacklisted walled garden profile can also be configured to explicitly block the unauthenticated users from accessing some websites.

You can create a walled garden access in AOS-W Instant UI or the CLI.

In the AOS-W Instant UI

To create a walled garden access:

1. Click the **Security** link at the top of the AOS-W Instant main window. The **Security** window is displayed.
2. Click **Walled Garden**. The **Walled Garden** tab contents are displayed.
3. To allow the users to access a specific domain, click **New** and enter the domain name or URL in the **Whitelist** section of the window. This allows access to a domain while the user remains unauthenticated. Specify a POSIX regular expression (regex(7)). For example:
 - yahoo.com matches various domains such as news.yahoo.com, travel.yahoo.com and finance.yahoo.com
 - www.apple.com/library/test is a subset of www.apple.com site corresponding to path /library/test/*
 - favicon.ico allows access to /favicon.ico from all domains.
4. To deny users access to a domain, click **New** and enter the domain name or URL in the **Blacklist** section of the window. This prevents the unauthenticated users from viewing specific websites. When a URL specified in the blacklist is accessed by an unauthenticated user, OAW-IAP sends an HTTP 403 response to the client with an error message. If the requested URL does not appear on the blacklist or whitelist, the request is redirected to the external captive portal.
5. To modify the list, select the domain name/URL and click **Edit** . To remove an entry from the list, select the URL from the list and click **Delete**.
6. Click **OK** to apply the changes.

In the CLI

To create a walled garden access:

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

Disabling Captive Portal Authentication

To disable captive portal authentication:

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



You can also customize splash page design on the **Security** tab of **New WLAN** (WLAN wizard) and **New Wired Network** (wired profile window) when configuring a new profile.

2. Navigate to the **Security** tab.
3. Select **None** from the **Splash page type** drop-down list. Although the splash page is disabled, you can enable MAC authentication, configure authentication servers, set accounting parameters, blacklist clients based on MAC authentication failures, and configure encryption keys for authorized access.
4. If required, configure the security parameters.
5. Click **Next** and then click **Finish** to apply the changes.

This chapter provides the following information:

- [Managing OAW-IAP Users on page 141](#)
- [Supported Authentication Methods on page 146](#)
- [Supported EAP Authentication Frameworks on page 148](#)
- [Configuring Authentication Servers on page 149](#)
- [Understanding Encryption Types on page 163](#)
- [Configuring Authentication Survivability on page 164](#)
- [Configuring 802.1X Authentication for a Network Profile on page 166](#)
- [Enabling 802.1X Supplicant Support on page 168](#)
- [Configuring MAC Authentication for a Network Profile on page 169](#)
- [Configuring MAC Authentication with 802.1X Authentication on page 171](#)
- [Configuring MAC Authentication with Captive Portal Authentication on page 172](#)
- [Configuring WISPr Authentication on page 173](#)
- [Blacklisting Clients on page 174](#)
- [Uploading Certificates on page 177](#)

Managing OAW-IAP Users

The OAW-IAP users can be classified as follows:

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

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

Table 31: *User Privileges*

User Category	AMP in Management Mode	OAW-IAP in Monitor Mode or without AMP
administrator	Access to local user database only	Complete access to the OAW-IAP
read-only administrator	No write privileges	No write privileges
guest administrator	Access to local user database only	Access to local user database only

Configuring OAW-IAP Users

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

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

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



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

The local user database of OAW-IAPs can support up to 512 user entries.

In the AOS-W Instant UI

To configure users:

1. Click the **Security** link located directly above the Search bar in the AOS-W Instant main window.
2. Click **Users for Internal Server**. The following figure shows the contents of the **Users for Internal Server** tab.

Figure 34 Adding a User

The screenshot shows a web-based interface for configuring users. At the top, there is a blue header bar with the word "Security" on the left and a "Help" link on the right. Below the header, there are several tabs: "Authentication Servers", "Users for Internal Server" (which is selected), "Roles", "Blacklisting", "Firewall Settings", and "Walled Garden". The main content area is divided into two sections. On the left, there is a table with the heading "Users(0)" and a column labeled "Type". The table is currently empty. Below the table are three buttons: "Edit", "Delete", and "Delete All". On the right side of the main content area, there is a section titled "Add new user:". This section contains four input fields: "Username:", "Password:", "Retype:", and "Type". The "Type" field is a drop-down menu currently set to "Guest". Below these fields is an "Add" button. At the bottom right of the entire interface, there are "OK" and "Cancel" buttons.

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

Edit or Delete User Settings

1. To edit user settings:
 - a. Select the user you want to modify from the **Users** list in the table.
 - b. Click **Edit** to modify user settings.
 - c. Click **OK**.
2. To delete a user:
 - a. Select the user you want to delete from the **Users** list in the table.
 - b. Click **Delete**.
 - c. Click **OK**.
3. To delete all or multiple users at a time:
 - a. Select multiple users you want to delete from the **Users** list in the table.
 - b. Click **Delete All**.
 - c. Click **OK**.



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

In the CLI

To configure an employee user:

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

To configure a guest user:

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

Configuring Authentication Parameters for Management Users

You can configure RADIUS or Terminal Access Controller Access Control System (TACACS) authentication servers to authenticate and authorize the management users of an OAW-IAP. The authentication servers determine if the user has access to administrative interface. The privilege level for different types of management users is defined on the RADIUS or TACACS server instead of the OAW-IAP. The OAW-IAPs map the management users to the corresponding privilege level and provide access to the users based on the attributes returned by the RADIUS or TACACS server.

You can configure authentication parameters for local admin, read-only, and guest management administrator account settings through the AOS-W Instant UI or the CLI.

In the AOS-W Instant UI

1. Navigate to **System > Admin**. The **Admin** tab details are displayed.

Table 32: Authentication Parameters for Management Users

Type of User	Authentication Options	Steps to Follow
Local administrator	Internal	Select Internal if you want to specify a single set of user credentials. If using an internal authentication server: <ol style="list-style-type: none"> Specify the Username and Password. Retype the password to confirm.
	Authentication server	Select the RADIUS or TACACS authentication servers. You can also create a new server by selecting New from the Authentication server drop-down list. <ul style="list-style-type: none"> Authentication server w/ fallback to internal—Select Authentication server w/ fallback to internal option if you want to use both internal and external servers. When enabled, the authentication switches to Internal if there is no response from the RADIUS server (RADIUS server timeout). To use this option, select the authentication servers and configure the user credentials for internal-server-based authentication. Load balancing—If two servers are configured, users can use them in the primary or backup mode, or load balancing mode. To enable load balancing, select Enabled from the Load balancing drop-down list. For more information on load balancing, see Dynamic Load Balancing between Two Authentication Servers on page 154. TACACS accounting—If a TACACS server is selected, enable TACACS accounting to report management commands if required.
Administrator with Read-Only Access	Internal	Select Internal to specify a single set of user credentials. If using an internal authentication server: <ol style="list-style-type: none"> Specify the Username and Password. Retype the password to confirm.
	Authentication server	If a RADIUS or TACACS server is configured, select Authentication server for authentication.
Guest	Internal	Select Internal to specify a single set of user credentials. If using an internal authentication server: <ol style="list-style-type: none"> Specify the Username and Password. Retype the password to confirm.
	Authentication server	If a RADIUS or TACACS server is configured, select Authentication server for authentication.

3. Click **OK**.

In the CLI

To configure a local admin user:

```
(Instant AP) (config) # mgmt-user <username> [password]
```

To configure guest management administrator credentials:

```
(Instant AP) (config) # mgmt-user <username> [password] guest-mgmt
```

To configure a user with read-only privilege:

```
(Instant AP) (config) # mgmt-user <username> [password] read-only
```

To configure management authentication settings:

```
(Instant AP) (config) # mgmt-auth-server <server1>  
(Instant AP) (config) # mgmt-auth-server <server2>  
(Instant AP) (config) # mgmt-auth-server-load-balancing  
(Instant AP) (config) # mgmt-auth-server-local-backup
```

To enable TACACS accounting:

```
(Instant AP) (config) # mgmt-accounting command all
```

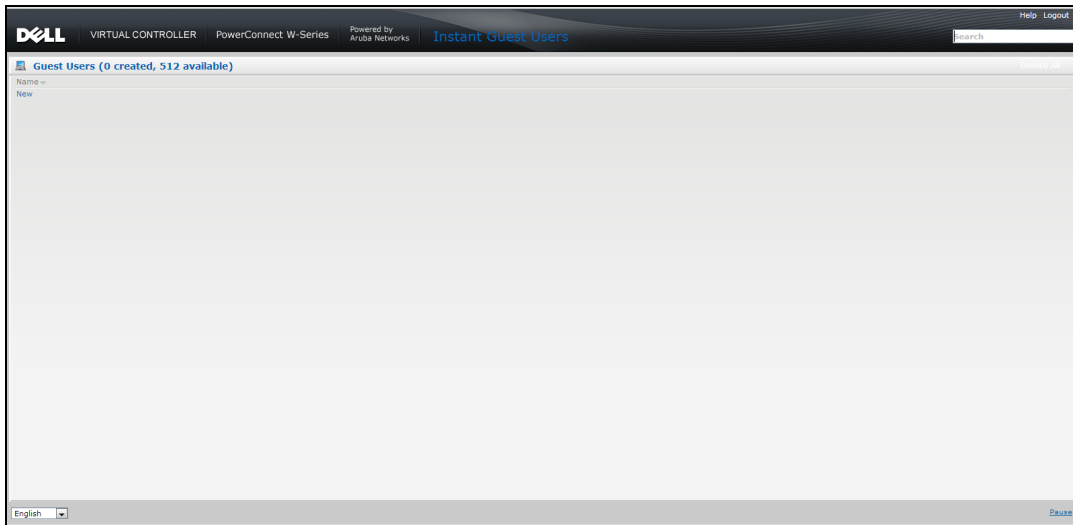
Adding Guest Users through the Guest Management Interface

To add guest users through the Guest Management interface:

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

Figure 35 *Guest Management Interface*





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

Supported Authentication Methods

Authentication is a process of identifying a user through a valid username and password or based on the user's MAC addresses. The following authentication methods are supported in AOS-W Instant:

- [802.1X Authentication](#)
- [MAC Authentication](#)
- [MAC Authentication with 802.1X Authentication](#)
- [Captive Portal Authentication](#)
- [MAC Authentication with Captive Portal Authentication](#)
- [802.1X Authentication with Captive Portal Role](#)
- [WISPr Authentication](#)

802.1X Authentication

802.1X is an IEEE standard that provides an authentication framework for WLANs. The 802.1X standard uses the Extensible Authentication Protocol (EAP) to exchange messages during the authentication process. The authentication protocols that operate inside the 802.1X framework include EAP-Transport Layer Security (EAP-TLS), Protected EAP (PEAP), and EAP-Tunneled TLS (EAP-TTLS). These protocols allow the network to authenticate the client while also allowing the client to authenticate the network. For more information on EAP authentication framework supported by the OAW-IAPs, see [Supported EAP Authentication Frameworks on page 148](#).

The 802.1X authentication method allows an OAW-IAP to authenticate the identity of a user before providing network access to the user. The Remote Authentication Dial In User Service (RADIUS) protocol 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 a successful 802.1X authentication.

For more information on configuring an OAW-IAP to use 802.1X authentication, see [Configuring 802.1X Authentication for a Network Profile on page 166](#).

MAC Authentication

MAC authentication is used for authenticating devices based on their physical MAC addresses. MAC authentication requires that the MAC address of a machine matches a manually defined list of addresses. This authentication method is not recommended for scalable networks and the networks that require stringent security settings. For more information on configuring an OAW-IAP to use MAC authentication, see [Configuring MAC Authentication for a Network Profile on page 169](#).

MAC Authentication with 802.1X Authentication

This authentication method has the following features:

- MAC authentication precedes 802.1X authentication—The administrators can enable MAC authentication for 802.1X authentication. MAC authentication shares all the authentication server configurations with 802.1X authentication. If a wireless or wired client connects to the network, MAC authentication is performed first. If MAC authentication fails, 802.1X authentication does not trigger. If MAC authentication is successful, 802.1X authentication is attempted. If 802.1X authentication is successful, the client is assigned an 802.1X authentication role. If 802.1X authentication fails, the client is assigned a **deny-all** role or **mac-auth-only** role.
- MAC authentication only role—Allows you to create a **mac-auth-only** role to allow role-based access rules when MAC authentication is enabled for 802.1X authentication. The **mac-auth-only** role is assigned to a client when the MAC authentication is successful and 802.1X authentication fails. If 802.1X authentication is successful, the **mac-auth-only** role is overwritten by the final role. The **mac-auth-only** role is primarily used for wired clients.
- L2 authentication fall-through—Allows you to enable the **l2-authentication-fallthrough** mode. When this option is enabled, the 802.1X authentication is allowed even if the MAC authentication fails. If this option is disabled, 802.1X authentication is not allowed. The **l2-authentication-fallthrough** mode is disabled by default.

For more information on configuring an OAW-IAP to use MAC as well as 802.1X authentication, see [Configuring MAC Authentication with 802.1X Authentication on page 171](#).

Captive Portal Authentication

Captive portal authentication is used for authenticating guest users. For more information on captive portal authentication, see [Captive Portal for Guest Access on page 115](#).

MAC Authentication with Captive Portal Authentication

You can enforce MAC authentication for captive portal clients. For more information on configuring an OAW-IAP to use MAC authentication with captive portal authentication, see [Configuring MAC Authentication with Captive Portal Authentication on page 172](#).

802.1X Authentication with Captive Portal Role

This authentication mechanism allows you to configure different captive portal settings for clients on the same SSID. For example, you can configure an 802.1X SSID and create a role for captive portal access, so that some of the clients using the SSID derive the captive portal role. You can configure rules to indicate access to external or internal captive portal, or none. For more information on configuring captive portal roles for an SSID with 802.1X authentication, see [Configuring Captive Portal Roles for an SSID on page 136](#).

WISPr Authentication

Wireless Internet Service Provider roaming (WISPr) authentication allows the smart clients to authenticate on the network when they roam between wireless Internet service providers, even if the wireless hotspot uses an Internet Service Provider (ISP) with whom the client may not have an account.

If a hotspot is configured to use WISPr authentication in a specific ISP and a client attempts to access the Internet at that hotspot, the WISPr AAA server configured for the ISP authenticates the client directly and allows the client to access the network. If the client only has an account with a *partner* ISP, the WISPr AAA server forwards the client's credentials to the partner ISP's WISPr AAA server for authentication. When the client is authenticated on the partner ISP, it is also authenticated on the hotspot's own ISP as per their service agreements. The OAW-IAP assigns the default WISPr user role to the client when the client's ISP sends an authentication message to the OAW-IAP. For more information on WISPr authentication, see [Configuring WISPr Authentication on page 173](#).

Supported EAP Authentication Frameworks

The following EAP authentication frameworks are supported in the AOS-W Instant network:

- EAP-TLS—The Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) method supports the termination of EAP-TLS security using the internal RADIUS server. The EAP-TLS requires both server and certification authority (CA) certificates installed on the OAW-IAP. The client certificate is verified on the VC (the client certificate must be signed by a known CA) before the username is verified on the authentication server.
- EAP-TTLS (MS-CHAPv2)—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 (MS-CHAPv2)—EAP-PEAP is an 802.1X authentication method that uses server-side public key certificates to authenticate clients with server. The PEAP authentication creates an encrypted SSL/TLS tunnel between the client and the authentication server. Exchange of information is encrypted and stored in the tunnel ensuring the user credentials are kept secure.
- LEAP—Lightweight Extensible Authentication Protocol (LEAP) uses dynamic WEP keys for authentication between the client and authentication server.

To use the OAW-IAP's internal database for user authentication, add the usernames and passwords of the users to be authenticated.



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

Authentication Termination on OAW-IAP

OAW-IAPs support EAP termination for enterprise WLAN SSIDs. The EAP termination can reduce the number of exchange packets between the OAW-IAP and the authentication servers. AOS-W Instant allows Extensible Authentication Protocol (EAP) termination for Protected Extensible Authentication Protocol-Generic Token Card (PEAP-GTC) and Protected Extensible Authentication Protocol-Microsoft Challenge Handshake Authentication Protocol version 2 (PEAP-MS-CHAV2). PEAP-GTC termination allows authorization against a Lightweight Directory Access Protocol (LDAP) server and external RADIUS server while PEAP-MS-CHAV2 allows authorization against an external RADIUS server.

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

- EAP-Generic Token Card (GTC)—This EAP method permits the transfer of unencrypted usernames and passwords from the client to the server. The main uses for EAP-GTC are procuring one-time token cards such as SecureID and using LDAP or RADIUS as the user authentication server. You can also enable caching of user credentials on the OAW-IAP to an external authentication server for user data backup.
- EAP-Microsoft Challenge Authentication Protocol version 2 (MS-CHAPv2)—This EAP method is widely supported by Microsoft clients. A RADIUS server must be used as the back-end authentication server.

Configuring Authentication Servers

This section describes the following procedures:

- [Configuring an External Server for Authentication on page 154](#)
- [Enabling RADIUS Communication over TLS on page 159](#)
- [Configuring Dynamic RADIUS Proxy Parameters on page 161](#)

Supported Authentication Servers

Based on the security requirements, you can configure internal or external authentication servers. This section describes the types of servers that can be configured for client authentication:

- [Internal RADIUS Server on page 149](#)
- [External RADIUS Server on page 149](#)
- [Dynamic Load Balancing between Two Authentication Servers on page 154](#)

Starting from AOS-W Instant 6.4.0.2-4.1 release, you can configure TACACS+ server for authenticating management users. For more information on management users and TACACS+ server-based authentication, see [Configuring Authentication Parameters for Management Users](#).

Internal RADIUS Server

Each OAW-IAP has an instance of free RADIUS server operating locally. When you enable the internal RADIUS server option for the network, the client on the OAW-IAP sends a RADIUS packet to the local IP address. The internal RADIUS server listens and replies to the RADIUS packet. Instant serves as a RADIUS server for 802.1X authentication. However, the internal RADIUS server can also be configured as a backup RADIUS server for an external RADIUS server.

External RADIUS Server

In the external RADIUS server, the IP address of the VC is configured as the NAS IP address. AOS-W Instant RADIUS is implemented on the VC and this eliminates the need to configure multiple NAS clients for every OAW-IAP on the RADIUS server for client authentication. AOS-W 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 the clients are allowed or denied access to the network depending on the response from the RADIUS server. When you enable an external RADIUS server for the network, the client on the OAW-IAP sends a RADIUS packet to the local IP address. The external RADIUS server then responds to the RADIUS packet.

AOS-W Instant supports the following external authentication servers:

- RADIUS
- LDAP
- ClearPass Policy Manager Server for AirGroup CoA

To use an LDAP server for user authentication, configure the LDAP server on the VC, and configure user IDs and passwords. To use a RADIUS server for user authentication, configure the RADIUS server on the VC.

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.

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

- AP-Group
- AP-Name

- ARAP-Features
- ARAP-Security
- ARAP-Security-Data
- ARAP-Zone-Access
- Acct-Authentic
- Acct-Delay-Time
- Acct-Input-Gigawords
- Acct-Input-Octets
- Acct-Input-Packets
- Acct-Interim-Interval
- Acct-Link-Count
- Acct-Multi-Session-Id
- Acct-Output-Gigawords
- Acct-Output-Octets
- Acct-Output-Packets
- Acct-Session-Id
- Acct-Session-Time
- Acct-Status-Type
- Acct-Terminate-Cause
- Acct-Tunnel-Packets-Lost
- Add-Port-To-IP-Address
- Aruba-AP-Group
- Aruba-AP-IP-Address
- Aruba-AS-Credential-Hash
- Aruba-AS-User-Name
- Aruba-Admin-Path
- Aruba-Admin-Role
- Aruba-AirGroup-Device-Type
- Aruba-AirGroup-Shared-Group
- Aruba-AirGroup-Shared-Role
- Aruba-AirGroup-Shared-User
- Aruba-AirGroup-User-Name
- Aruba-AirGroup-Version
- Aruba-Auth-SurvMethod
- Aruba-Auth-Survivability
- Aruba-CPPM-Role
- Aruba-Calea-Server-Ip
- Aruba-Device-Type
- Aruba-Essid-Name
- Aruba-Framed-IPv6-Address
- Aruba-Location-Id
- Aruba-Mdps-Device-Iccid

- Aruba-Mdps-Device-Imei
- Aruba-Mdps-Device-Name
- Aruba-Mdps-Device-Product
- Aruba-Mdps-Device-Profile
- Aruba-Mdps-Device-Serial
- Aruba-Mdps-Device-Udid
- Aruba-Mdps-Device-Version
- Aruba-Mdps-Max-Devices
- Aruba-Mdps-Provisioning-Settings
- Aruba-Named-User-Vlan
- Aruba-Network-SSO-Token
- Aruba-No-DHCP-Fingerprint
- Aruba-Port-Bounce-Host
- Aruba-Port-Id
- Aruba-Priv-Admin-User
- Aruba-Template-User
- Aruba-User-Group
- Aruba-User-Role
- Aruba-User-Vlan
- Aruba-WorkSpace-App-Name
- Authentication-Sub-Type
- Authentication-Type
- CHAP-Challenge
- Callback-Id
- Callback-Number
- Chargeable-User-Identity
- Class
- Connect-Info
- Connect-Rate
- Crypt-Password
- DB-Entry-State
- Digest-Response
- Domain-Name
- EAP-Message
- Error-Cause
- Event-Timestamp
- Exec-Program
- Exec-Program-Wait
- Expiration
- Fall-Through
- Filter-Id
- Framed-AppleTalk-Link

- Framed-AppleTalk-Network
- Framed-AppleTalk-Zone
- Framed-Compression
- Framed-IP-Address
- Framed-IP-Netmask
- Framed-IPX-Network
- Framed-IPv6-Pool
- Framed-IPv6-Prefix
- Framed-IPv6-Route
- Framed-Interface-Id
- Framed-MTU
- Framed-Protocol
- Framed-Route
- Framed-Routing
- Full-Name
- Group
- Group-Name
- Hint
- Huntgroup-Name
- Idle-Timeout
- Location-Capable
- Location-Data
- Location-Information
- Login-IP-Host
- Login-IPv6-Host
- Login-LAT-Node
- Login-LAT-Port
- Login-LAT-Service
- Login-Service
- Login-TCP-Port
- Menu
- Message-Auth
- NAS-IPv6-Address
- NAS-Port-Type
- Operator-Name
- Password
- Password-Retry
- Port-Limit
- Prefix
- Prompt
- Rad-Authenticator
- Rad-Code

- Rad-Id
- Rad-Length
- Reply-Message
- Requested-Location-Info
- Revoke-Text
- Server-Group
- Server-Name
- Service-Type
- Session-Timeout
- Simultaneous-Use
- State
- Strip-User-Name
- Suffix
- Termination-Action
- Termination-Menu
- Tunnel-Assignment-Id
- Tunnel-Client-Auth-Id
- Tunnel-Client-Endpoint
- Tunnel-Connection-Id
- Tunnel-Medium-Type
- Tunnel-Preference
- Tunnel-Private-Group-Id
- Tunnel-Server-Auth-Id
- Tunnel-Server-Endpoint
- Tunnel-Type
- User-Category
- User-Name
- User-Vlan
- Vendor-Specific
- fw_mode
- dhcp-option
- dot1x-authentication-type
- mac-address
- mac-address-and-dhcp-options

TACACS Servers

You can now configure a TACACS server as the authentication server to authenticate and authorize all types of management users, and account user sessions. When configured, the TACACS server allows a remote access server to communicate with an authentication server to determine if the user has access to the network. The OAW-IAP users can create several TACACS server profiles and associate these profiles to the user accounts to enable authentication of the management users.

TACACS supports the following types of authentication:

- ASCII

- PAP
- CHAP
- ARAP
- MS-CHAP



The TACACS server cannot be attributed to any SSID or wired profile in general as the authentication server and is configured only for the OAW-IAP management users.

Dynamic Load Balancing between Two Authentication Servers

You can configure two authentication servers to serve as a primary and backup RADIUS server and enable load balancing between these servers. Load balancing of authentication servers ensures that the authentication load is split across multiple authentication servers and enables the OAW-IAPs to perform load balancing of authentication requests destined to authentication servers such as RADIUS or LDAP.

The load balancing in OAW-IAP is performed based on outstanding authentication sessions. If there are no outstanding sessions and if the rate of authentication is low, only primary server will be used. The secondary is used only if there are outstanding authentication sessions on the primary server. With this, the load balance can be performed across RADIUS servers of asymmetric capacity without the need to obtain inputs about the server capabilities from the administrators.

Configuring an External Server for Authentication

You can configure RADIUS, TACACS, LDAP, and ClearPass Policy Manager servers through the AOS-W Instant UI or the CLI.

In the AOS-W Instant UI

To configure an external authentication server:

1. Navigate to **Security > Authentication Servers**. The **Security** window is displayed.
2. To create a new server, click **New**. A window for specifying details for the new server is displayed.
3. Configure parameters based on the type of sever.
 - **RADIUS**—To configure a RADIUS server, specify the attributes described in the following table:

Table 33: RADIUS Server Configuration Parameters

Parameter	Description
Name	Enter a name for the server.
Server address	Enter the host name or the IP address of the external RADIUS server.
RadSec	<p>Set RadSec to Enabled to enable secure communication between the RADIUS server and OAW-IAP clients by creating a TLS tunnel between the OAW-IAP and the server.</p> <p>If RadSec is enabled, the following configuration options are displayed:</p> <ul style="list-style-type: none"> • RadSec port—Communication port number for RadSec TLS connection. By default, the port number is set to 2083. • RFC 3576 • RFC 5997 • NAS IP address

Table 33: RADIUS Server Configuration Parameters

Parameter	Description
	<ul style="list-style-type: none"> NAS identifier <p>For more information on RadSec configuration, see Enabling RADIUS Communication over TLS on page 159.</p>
Auth port	Enter the authorization port number of the external RADIUS server within the range of 1–65,535. The default port number is 1812.
Accounting port	Enter the accounting port number within the range of 1–65,535. This port is used for sending accounting records to the RADIUS server. The default port number is 1813.
Shared key	Enter a shared key for communicating with the external RADIUS server.
Retype key	Re-enter the shared key.
Timeout	Specify a timeout value in seconds. The value determines the timeout for one RADIUS request. The OAW-IAP retries to send the request several times (as configured in the Retry count) before the user gets disconnected. For example, if the Timeout is 5 seconds, Retry counter is 3, user is disconnected after 20 seconds. The default value is 5 seconds.
Retry count	Specify a number between 1 and 5. Indicates the maximum number of authentication requests that are sent to the server group, and the default value is 3 requests.
RFC 3576	Select Enabled to allow the OAW-IAPs to process RFC 3576-compliant Change of Authorization (CoA) and disconnect messages from the RADIUS server. Disconnect messages cause a user session to be terminated immediately, whereas the CoA messages modify session authorization attributes such as data filters.
RFC 5997	<p>This helps to detect the server status of the RADIUS server. Every time there is an authentication or accounting request timeout, the OAW-IAP will send a status request enquiry to get the actual status of the RADIUS server before confirming the status of the server to be DOWN.</p> <ul style="list-style-type: none"> Authentication—Select this checkbox to ensure the OAW-IAP sends a status-server request to determine the actual state of the authentication server before marking the server as unavailable. Accounting—Select this checkbox to ensure the OAW-IAP sends a status-server request to determine the actual state of the accounting server before marking the server as unavailable. <p>NOTE: You can choose to select either the Authentication or Accounting checkboxes or select both checkboxes to support RFC5997.</p>
NAS IP address	<p>Allows you to configure an arbitrary IP address to be used as RADIUS attribute 4, NAS IP Address, without changing source IP Address in the IP header of the RADIUS packet.</p> <p>NOTE: If you do not enter the IP address, the VC IP address is used by default when Dynamic RADIUS Proxy is enabled.</p>

Table 33: RADIUS Server Configuration Parameters

Parameter	Description
NAS Identifier	Allows you to configure strings for RADIUS attribute 32, NAS Identifier, to be sent with RADIUS requests to the RADIUS server.
Dead Time	Specify a dead time for authentication server in minutes. When two or more authentication servers are configured on the OAW-IAP and a server is unavailable, the dead time configuration determines the duration for which the authentication server would be available if the server is marked as unavailable.
Dynamic RADIUS proxy parameters	Specify the following dynamic RADIUS proxy (DRP) parameters: <ul style="list-style-type: none"> • DRP IP—IP address to be used as source IP for RADIUS packets. • DRP Mask—Subnet mask of the DRP IP address. • DRP VLAN—VLAN in which the RADIUS packets are sent. • DRP Gateway—Gateway IP address of the DRP VLAN. For more information on dynamic RADIUS proxy parameters and configuration procedure, see Configuring Dynamic RADIUS Proxy Parameters on page 161 .

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



You can also add an external RADIUS server by selecting the **New** option when configuring a WLAN or wired profile. For more information, see [Configuring Security Settings for a WLAN SSID Profile on page 88](#) and [Configuring Security Settings for a Wired Profile on page 108](#).

- **LDAP**—To configure an LDAP server, select the **LDAP** option and configure the attributes described in the following table:

Table 34: LDAP Server Configuration Parameters

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

Table 34: LDAP Server Configuration Parameters

Parameter	Description
Key Attribute	Specify the attribute to use as a key while searching for the LDAP server. For Active Directory, the value is sAMAccountName
Timeout	Enter a value between 1 and 30 seconds. The default value is 5.
Retry count	Enter a value between 1 and 5. The default value is 3.
Dead Time	Specify a dead time for the authentication server in minutes within the range of 1–1440 minutes. The default dead time interval is 5 minutes. When two or more authentication servers are configured on the OAW-IAP and a server is unavailable, the dead time configuration determines the duration for which the authentication server would be available if the server is marked as unavailable.

- **TACACS**—To configure TACACS server, select the **TACACS** option and configure the following parameters:

Table 35: TACACS Configuration Parameters

Parameter	Description
Name	Enter a name for the server.
IP address	Enter the IP address of the TACACS server.
Auth Port	Enter a TCPIP port used by the server. The default port number is 49.
Shared Key	Enter a secret key of your choice to authenticate communication between the TACACS+ client and the server.
Retype Key	Re-enter the shared key.
Timeout	Enter a number between 1 and 30 seconds to indicate the timeout period for TACACS+ requests. The default value is 20 seconds.
Retry Count	Enter a number between 1 and 5 to indicate the maximum number of authentication attempts. The default value is 3.
Dead time	Specify a dead time in minutes within the range of 1–1440 minutes. The default dead time interval is 5 minutes.
Session authorization	Enables or disables session authorization. When enabled, the optional authorization session is turned on for the admin users. By default, session authorization is disabled.



You can also add TACACS server by selecting the **New** option when configuring authentication parameters for management users. For more information, see [Configuring Authentication Parameters for Management Users on page 143](#).

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

Table 36: ClearPass Policy Manager Server Configuration Parameters for AirGroup CoA

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

4. Click **OK**.



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

In the CLI

To configure a RADIUS server with DRP parameters:

```
(Instant AP) (config)# wlan auth-server <profile-name>
(Instant AP) (Auth Server <profile-name>)# ip <host>
(Instant AP) (Auth Server <profile-name>)# key <key>
(Instant AP) (Auth Server <profile-name>)# port <port>
(Instant AP) (Auth Server <profile-name>)# acctport <port>
(Instant AP) (Auth Server <profile-name>)# nas-id <NAS-ID>
(Instant AP) (Auth Server <profile-name>)# nas-ip <NAS-IP-address>
(Instant AP) (Auth Server <profile-name>)# timeout <seconds>
(Instant AP) (Auth Server <profile-name>)# retry-count <number>
(Instant AP) (Auth Server <profile-name>)# rfc3576
(Instant AP) (Auth Server <profile-name>)# rfc5997 {auth-only|acct-only}
(Instant AP) (Auth Server <profile-name>)# deadtime <minutes>
(Instant AP) (Auth Server <profile-name>)# drp-ip <IP-address> <mask> vlan <vlan> gateway
<gateway-IP-address>
(Instant AP) (Auth Server <profile-name>)# end
(Instant AP)# commit apply
```

To enable RadSec:

```
(Instant AP) (config)# wlan auth-server <profile-name>
(Instant AP) (Auth Server "name")# ip <host>
(Instant AP) (Auth Server "name")# radsec [port <port>]
(Instant AP) (Auth Server "name")# rfc3576
(Instant AP) (Auth Server "name")# rfc5997 {auth-only|acct-only}
(Instant AP) (Auth Server "name")# nas-id <id>
(Instant AP) (Auth Server "name")# nas-ip <ip>
(Instant AP) (Auth Server "name")# end
(Instant AP)# commit apply
```

To configure an LDAP server:

```
(Instant AP) (config)# wlan ldap-server <profile-name>
(Instant AP) (LDAP Server <profile-name>)# ip <IP-address>
(Instant AP) (LDAP Server <profile-name>)# port <port>
(Instant AP) (LDAP Server <profile-name>)# admin-dn <name>
(Instant AP) (LDAP Server <profile-name>)# admin-password <password>
(Instant AP) (LDAP Server <profile-name>)# base-dn <name>
```

```
(Instant AP) (LDAP Server <profile-name>)# filter <filter>
(Instant AP) (LDAP Server <profile-name>)# key-attribute <key>
(Instant AP) (LDAP Server <profile-name>)# timeout <seconds>
(Instant AP) (LDAP Server <profile-name>)# retry-count <number>
(Instant AP) (LDAP Server <profile-name>)# deadtime <minutes>
(Instant AP) (LDAP Server <profile-name>)# end
(Instant AP)# commit apply
```

To configure a TACACS+ server:

```
(Instant AP) (config)# wlan tacacs-server <profile-name>
(Instant AP) (TACACS Server <profile-name>)# ip <IP-address>
(Instant AP) (TACACS Server <profile-name>)# port <port>
(Instant AP) (TACACS Server <profile-name>)# key <key>
(Instant AP) (TACACS Server <profile-name>)# timeout <seconds>
(Instant AP) (TACACS Server <profile-name>)# retry-count <number>
(Instant AP) (TACACS Server <profile-name>)# deadtime <minutes>
(Instant AP) (TACACS Server <profile-name>)# end
(Instant AP)# commit apply
```

To configure a ClearPass Policy Manager server used for AirGroup CoA:

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

Enabling RADIUS Communication over TLS

You can configure an OAW-IAP to use Transport Layer Security (TLS) tunnel and to enable secure communication between the RADIUS server and OAW-IAP clients. Enabling RADIUS communication over TLS increases the level of security for authentication that is carried out across the cloud network. When configured, this feature ensures that RadSec protocol is used for safely transmitting the authentication and accounting data between the OAW-IAP clients and the RADIUS server in cloud.

The following configuration conditions apply to RadSec configuration:

- When the TLS tunnel is established, RADIUS packets will go through the tunnel and server adds CoA on this tunnel.
- By default, the TCP port 2083 is assigned for RadSec. Separate ports are not used for authentication, accounting, and dynamic authorization changes.
- AOS-W Instant supports dynamic CoA (RFC 3576) over RadSec and the RADIUS server uses an existing TLS connection opened by the OAW-IAP to send the request.
- For authentication between the OAW-IAP clients and the TLS server, RadSec certificate must be uploaded to OAW-IAP. For more information on uploading certificates, see [Uploading Certificates on page 177](#).

Configuring RadSec Protocol

You can configure RadSec Protocol using the AOS-W Instant UI or the CLI;

In the AOS-W Instant UI

To configure the RadSec protocol in the UI:

1. Navigate to **Security > Authentication Servers**. The **Security** window is displayed.
2. To create a new server, click **New**. A popup window for specifying details for the new server is displayed.
3. Under **RADIUS Server**, configure the following parameters:
 - a. Enter the name of the server.

- b. Enter the host name or the IP address of the server.
 - c. Select **Enabled** to enable RadSec.
 - d. Ensure that the port defined for RadSec is correct. By default, the port number is set to 2083.
 - e. To allow the OAW-IAPs to process RFC 3576-compliant Change of Authorization (CoA) and disconnect messages from the RADIUS server, set **RFC 3576** to **Enabled**. Disconnect messages cause a user session to be terminated immediately, whereas the CoA messages modify session authorization attributes such as data filters.
 - f. If **RFC 3576** is enabled, specify an AirGroup CoA port if required.
 - g. Enter the NAS IP address.
 - h. Specify the NAS identifier to configure strings for RADIUS attribute 32 and to send it with RADIUS requests to the RADIUS server.
4. Click **OK**.

In the CLI

To configure the RadSec protocol:

```
(Instant AP) (config)# wlan auth-server <profile-name>
(Instant AP) (Auth Server "name")# ip <host>
(Instant AP) (Auth Server "name")# radsec [port <port>]
(Instant AP) (Auth Server "name")# rfc3576
(Instant AP) (Auth Server "name")# nas-id <id>
(Instant AP) (Auth Server "name")# nas-ip <ip>
(Instant AP) (Auth Server "name")# end
(Instant AP) (Auth Server "name")# commit apply
```

Associate the Server Profile with a Network Profile

You can associate the server profile with a network profile using the AOS-W Instant UI or the CLI.

In the AOS-W Instant UI

To associate an authentication server in the AOS-W Instant UI:

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

You can also associate the authentication servers when creating a new WLAN or wired profile.

2. Click the **Security** tab and select a splash page profile.
3. Select an authentication type.
4. From the **Authentication Server 1** drop-down list, select the server name on which RadSec is enabled.
5. Click **Next** and then click **Finish**.

In the CLI

To associate an authentication server to a WLAN SSID:

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

To associate an authentication server to a wired profile:

```
(Instant AP) (config)# wired-port-profile <name>
(Instant AP) (wired ap profile <name>)# auth-server <name>
(Instant AP) (wired ap profile <name>)# end
```



```
(Instant AP)# commit apply
```

Configuring Dynamic RADIUS Proxy Parameters

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



The dynamic RADIUS proxy parameters configuration is not required if RadSec is enabled in the RADIUS server profile.

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

1. [Enable dynamic RADIUS proxy.](#)
2. [Configure dynamic RADIUS proxy IP, VLAN, netmask, and gateway for each authentication server.](#)
3. [Associate the authentication servers to SSID or a wired profile to which the clients connect.](#)

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

Enabling Dynamic RADIUS Proxy

You can enable RADIUS server support using the AOS-W Instant UI or the CLI.

In the AOS-W Instant UI

To enable RADIUS server support:

1. In the AOS-W Instant main window, click the **System** link. The **System** window is displayed.
2. On the **General** tab of the **System** window, select the **RADIUS** check box for **Dynamic Proxy**.
3. Click **OK**.

When dynamic RADIUS proxy is enabled, the VC network uses the IP Address of the VC for communication with external RADIUS servers. Ensure that the VC IP Address is set as a NAS IP when configuring RADIUS server attributes with dynamic RADIUS proxy enabled. For more information on configuring RADIUS server attributes, see [Configuring an External Server for Authentication on page 154](#).



In case of VPN deployments, the tunnel IP received when establishing a VPN connection is used as the NAS IP. In such cases, the VC IP need not be configured for the external RADIUS servers.

In the CLI

To enable the dynamic RADIUS proxy feature:

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

Configuring Dynamic RADIUS Proxy Parameters

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

In the AOS-W Instant UI

To configure dynamic RADIUS proxy in the AOS-W Instant UI:

1. Go to **Security > Authentication Servers**.

- To create a new server, click **New** and configure the required RADIUS server parameters as described in [Table 33](#).
- Ensure that the following dynamic RADIUS proxy parameters are configured:
 - **DRP IP**—IP address to be used as source IP for RADIUS packets.
 - **DRP Mask**—Subnet mask of the DRP IP address.
 - **DRP VLAN**—VLAN in which the RADIUS packets are sent.
 - **DRP Gateway**—Gateway IP address of the DRP VLAN.
- Click **OK**.

In the CLI

To configure dynamic RADIUS proxy parameters:

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

Associate Server Profiles to a Network Profile

To associate the authentication server profiles with a network profile:

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

You can also associate the authentication servers when creating a new WLAN or wired profile.

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



You can also add an external RADIUS server by selecting **New** for Authentication Server when configuring a WLAN or wired profile. For more information, see [Configuring Security Settings for a WLAN SSID Profile on page 88](#) and [Configuring Security Settings for a Wired Profile on page 108](#).

In the CLI

To associate an authentication server to a WLAN SSID:

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

To associate an authentication server to a wired profile:

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

Understanding Encryption Types

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

AOS-W Instant supports the following types of encryption:

- **WEP**—Wired Equivalent Privacy (WEP) is an authentication method where all users share the same key. WEP is not as secure as other encryption types such as TKIP.
- **TKIP**—Temporal Key Integrity Protocol (TKIP) uses the same encryption algorithm as WEP. However, TKIP is more secure and has an additional message integrity check (MIC).
- **AES**—The Advanced Encryption Standard (AES) encryption algorithm is a widely supported encryption type for all wireless networks that contain any confidential data. AES in Wi-Fi leverages 802.1X or PSKs to generate per-station keys for all devices. AES provides a high level of security like IP Security (IPsec) clients.



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

WPA and WPA-2

WPA is created based on the draft of 802.11i, which allowed users to create more secure WLANs. WPA-2 encompasses the full implementation of the 802.11i standard. WPA-2 is a superset that encompasses the full WPA feature set.

The following table summarizes the differences between the two certifications:

Table 37: WPA and WPA-2 Features

Certification	Authentication	Encryption
WPA	<ul style="list-style-type: none"> • PSK • IEEE 802.1X with Extensible Authentication Protocol (EAP) 	TKIP with message integrity check (MIC)
WPA-2	<ul style="list-style-type: none"> • PSK • IEEE 802.1X with EAP 	AES—Counter Mode with Cipher Block Chaining Message Authentication Code (AESCCMP)

WPA and WPA-2 can be further classified as follows:

- **Personal**—Personal is also called Pre-Shared Key (PSK). In this type, a unique key is shared with each client in the network. Users have to use this key to securely log in to the network. The key remains the same until it is changed by authorized personnel. You can also configure key change intervals .
- **Enterprise**—Enterprise is more secure than WPA Personal. In this type, every client automatically receives a unique encryption key after securely logging in to the network. This key is automatically updated at regular intervals. WPA uses TKIP and WPA-2 uses the AES algorithm.

Recommended Authentication and Encryption Combinations

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

Table 38: *Recommended Authentication and Encryption Combinations*

Network Type	Authentication	Encryption
Employee	802.1X	AES
Guest Network	Captive portal	None
Voice Network or Handheld devices	802.1X or PSK as supported by the device	AES if possible, TKIP or WEP if necessary (combine with security settings assigned for a user role).

Configuring Authentication Survivability

The authentication survivability feature supports a survivable authentication framework against any remote link failures when working with external authentication servers. When enabled, this feature allows the OAW-IAPs to authenticate the previously connected clients against the cached credentials if the connection to the authentication server is temporarily lost.

AOS-W Instant supports the following EAP standards for authentication survivability:

- **EAP-PEAP:** The Protected Extensible Authentication Protocol, also known as Protected EAP or PEAP, is a protocol that encapsulates EAP within a potentially encrypted and authenticated Transport Layer Security (TLS) tunnel. The EAP-PEAP supports MS-CHAPv2 and GTC methods.
- **EAP-TLS:** EAP-Transport Layer Security (EAP-TLS) is an IETF open standard that uses the Transport Layer Security (TLS) protocol.

When the authentication survivability feature is enabled, the following authentication process is used:

1. The client associates to an OAW-IAP and authenticates to the external authentication server. The external authentication server can be either ClearPass Policy Manager (for EAP-PEAP) or RADIUS server (EAP-TLS).
2. Upon successful authentication, the associated OAW-IAP caches the authentication credentials of the connected clients for the configured duration. The cache expiry duration for authentication survivability can be set within the range of 1–99 hours, with 24 hours being the default cache timeout duration.
3. If the client roams or tries to reconnect to the OAW-IAP and the remote link fails due to the unavailability of the authentication server, the OAW-IAP uses the cached credentials in the internal authentication server to authenticate the user. However, if the client tries to reconnect after the cache expiry, the authentication fails.
4. When the authentication server is available and if the client tries to reconnect, the OAW-IAP detects the availability of server and allows the client to authenticate to the server. Upon successful authentication, the OAW-IAP cache details are refreshed.

Enabling Authentication Survivability

You can enable authentication survivability for a wireless network profile through the UI or the CLI.

In the AOS-W Instant UI

To configure authentication survivability for a wireless network:

1. On the **Network** tab, click **New** to create a new network profile or select an existing profile for which you want to enable authentication survivability and click **edit**.
2. In the **Edit <profile-name>** or the **New WLAN** window, ensure that all required WLAN and VLAN attributes are defined, and then click **Next**.
3. On the **Security** tab, under **Enterprise** security settings, select an existing authentication server or create a new server by clicking **New**.
4. To enable authentication survivability, select **Enabled** from the **Authentication survivability** drop-down list. On enabling this, the OAW-IAP authenticates the previously connected clients using EAP-PEAP and EAP-TLS authentication when connection to the external authentication server is temporarily lost.
5. Specify the cache timeout duration, after which the cached details of the previously authenticated clients expire. You can specify a value within the range of 1–99 hours and the default cache timeout duration is 24 hours.
6. Click **Next** and then click **Finish** to apply the changes.

Important Points to Remember

- Any client connected through ClearPass Policy Manager and authenticated through OAW-IAP remains authenticated with the OAW-IAP even if the client is removed from the ClearPass Policy Manager server during the ClearPass Policy Manager downtime.
- Do not make any changes to the authentication survivability cache timeout duration when the authentication server is down.
- For EAP-PEAP authentication, ensure that the ClearPass Policy Manager 6.0.2 or later version is used for authentication. For EAP-TLS authentication, any external or third-party server can be used.
- For EAP-TLS authentication, ensure that the server and CA certificates from the authentication servers are uploaded on the OAW-IAP. For more information, see [Uploading Certificates on page 177](#).

In the CLI

To configure authentication survivability for a wireless network:

```
(Instant AP) (config)# wlan ssid-profile <name>
(Instant AP) (SSID Profile <name>)# type {<Employee>|<Voice>|<Guest>}
(Instant AP) (SSID Profile <name>)# auth-server <server-name1>
(Instant AP) (SSID Profile <name>)# auth-survivability
(Instant AP) (SSID Profile <name>)# exit
(Instant AP) (config)# auth-survivability cache-time-out <hours>
(Instant AP) (config)# end
(Instant AP)# commit apply
```

To view the cache expiry duration:

```
(Instant AP)# show auth-survivability time-out
```

To view the information cached by the OAW-IAP:

```
(Instant AP)# show auth-survivability cached-info
```

To view logs for debugging:

```
(Instant AP)# show auth-survivability debug-log
```

Configuring 802.1X Authentication for a Network Profile

This section consists of the following procedures:

- [Configuring 802.1X Authentication for Wireless Network Profiles on page 166](#)
- [Configuring 802.1X Authentication for Wired Profiles on page 167](#)

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

The steps involved in 802.1X authentication are as follows:

1. The NAS requests authentication credentials from a wireless client.
2. The wireless client sends authentication credentials to the NAS.
3. The NAS sends these credentials to a RADIUS server.
4. The RADIUS server checks the user identity and authenticates the client if the user details are available in its database. The RADIUS server sends an **Access-Accept** message to the NAS. If the RADIUS server cannot identify the user, it stops the authentication process and sends an **Access-Reject** message to the NAS. The NAS forwards this message to the client and the client must re-authenticate with appropriate credentials.
5. After the client is authenticated, the RADIUS server forwards the encryption key to the NAS. The encryption key is used for encrypting or decrypting traffic sent to and from the client.



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

Configuring 802.1X Authentication for Wireless Network Profiles

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

In the AOS-W Instant UI

To enable 802.1X authentication for a wireless network:

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

By default, for 802.1X authentication, the client conducts an EAP exchange with the RADIUS server, and the OAW-IAP acts as a relay for this exchange. When **Termination** is enabled, the OAW-IAP by itself acts as an authentication server and terminates the outer layers of the EAP protocol, only relaying the innermost layer to the external RADIUS server.

6. Specify the type of authentication server to use and configure other required parameters. You can also configure two different authentication servers to function as primary and backup servers when

Termination is enabled. For more information on RADIUS authentication configuration parameters, see [Configuring an External Server for Authentication on page 154](#).

7. Click **Next** to define access rules, and then click **Finish** to apply the changes.

In the CLI

To configure 802.1X authentication for a wireless network:

```
(Instant AP) (config)# wlan ssid-profile <name>
(Instant AP) (SSID Profile <name>)# type {<Employee>|<Voice>}
(Instant AP) (SSID Profile <name>)# opmode {wpa2-aes|wpa-tkip|wpa-tkip,wpa2-aes|dynamic-wep}
(Instant AP) (SSID Profile <name>)# leap-use-session-key
(Instant AP) (SSID Profile <name>)# termination
(Instant AP) (SSID Profile <name>)# auth-server <server1>
(Instant AP) (SSID Profile <name>)# auth-server <server2>
(Instant AP) (SSID Profile <name>)# radius-reauth-interval <minutes>
(Instant AP) (SSID Profile <name>)# auth-survivability
(Instant AP) (SSID Profile <name>)# exit
(Instant AP) (config)# auth-survivability cache-time-out <hours>
(Instant AP) (config)# end
(Instant AP) # commit apply
```

Configuring 802.1X Authentication for Wired Profiles

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

In the AOS-W Instant UI

To enable 802.1X authentication for a wired profile:

1. Click the **Wired** link under **More** in the main window. The **Wired** window is displayed.
2. Click **New** under **Wired Networks** to create a new network or select an existing profile for which you want to enable 802.1X authentication and then click **Edit**.
3. In the **New Wired Network** or the **Edit Wired Network** window, ensure that all the required Wired and VLAN attributes are defined, and then click **Next**.
4. On the **Security** tab, select **Enabled** from the **802.1X authentication** drop-down list.
5. Specify the type of authentication server to use and configure other required parameters. For more information on configuration parameters, see [Configuring Security Settings for a Wired Profile on page 108](#).
6. Click **Next** to define access rules, and then click **Finish** to apply the changes.
7. Assign the profile to an Ethernet port. For more information, see [Assigning a Profile to Ethernet Ports on page 111](#).

In the CLI

To enable 802.1X authentication for a wired profile:

```
(Instant AP) (config)# wired-port-profile <name>
(Instant AP) (wired ap profile <name>)# type {<employee>|<guest>}
(Instant AP) (wired ap profile <name>)# dot1x
(Instant AP) (wired ap profile <name>)# auth-server <server1>
(Instant AP) (wired ap profile <name>)# auth-server <server2>
(Instant AP) (wired ap profile <name>)# server-load-balancing
(Instant AP) (wired ap profile <name>)# radius-reauth-interval <Minutes>
(Instant AP) (wired ap profile <name>)# end
(Instant AP) # commit apply
```

Enabling 802.1X Supplicant Support

The 802.1X authentication protocol prevents the unauthorized clients from gaining access to the network through publicly accessible ports. If the ports to which the OAW-IAPs are connected, are configured to use the 802.1X authentication method, ensure that you configure the OAW-IAPs to function as an 802.1X client or supplicant. If your network requires all wired devices to authenticate using PEAP or TLS protocol, you need to configure the OAW-IAP uplink ports for 802.1X authentication, so that the switch grants access to the OAW-IAP only after completing the authentication as a valid client.

To enable the 802.1X supplicant support on an OAW-IAP, ensure that the 802.1X authentication parameters are configured on all OAW-IAPs in the cluster and are stored securely in the OAW-IAP flash.



The 802.1X supplicant support feature is not supported with mesh and Wi-Fi uplink.

Configuring an OAW-IAP for 802.1X Supplicant Support

To enable 802.1X supplicant support, configure 802.1X authentication parameters on every OAW-IAP using the AOS-W Instant UI or the CLI.

In the UI

1. To use PEAP protocol-based 802.1X authentication method, complete the following steps:
 - a. In the **Access Points** tab, click the OAW-IAP on which you want to set the variables for 802.1X authentication, and then click the **edit** link.
 - b. In the **Edit Access Point** window, click the **Uplink** tab.
 - c. Under PEAP user, enter the username, password, and retype the password for confirmation. The OAW-IAP username and password are stored in OAW-IAP flash. When the OAW-IAP boots, the */tmp/ap1xuser* and */tmp/ap1xpassword* files are created based on these two variables.



The default inner authentication protocol for PEAP is MS-CHAPV2.

2. To upload server certificates for validating the authentication server credentials, complete the following steps:
 - a. Click **Upload New Certificate**.
 - b. Specify the URL from where you want to upload the certificates and select the type of certificate.
3. Click **OK**.
4. To configure 802.1X authentication on uplink ports of an OAW-IAP, complete the following steps:
 - a. Go to **System > Show advanced options > Uplink**.
 - b. Click AP1X.
 - c. Select PEAP or TLS as the authentication type.
 - d. If you want to validate the server credentials using server certificate, select the **Validate Server** check box. Ensure that the server certificates for validating server credentials are uploaded to OAW-IAP database.
 - e. Click **OK**.
5. Reboot the OAW-IAP.

In the CLI

To set username and password variable used by the PEAP protocol-based 802.1X authentication:

```
(Instant AP) # ap1x-peap-user <ap1xuser> <password>
```


To set the PEAP 802.1X authentication type:

```
(Instant AP) (config) # ap1x peap [validate-server]
(Instant AP) (config) # end
(Instant AP) # commit apply
```

To set TLS 802.1X authentication type:

```
(Instant AP) (config) # ap1x tls <tpm|user> [validate-server]
(Instant AP) (config) # end
(Instant AP) # commit apply
```

To upload user or CA certificates for PEAP or TLS authentication:

```
(Instant AP) # copy tftp <addr> <file> ap1x {ca|cert <password>} format pem
```

To download user or server certificates from a TFTP, FTP, or web server:

```
(Instant AP) # download ap1x <url> format pem [psk <psk>]
(Instant AP) # download ap1xca <url> format pem
```

To view the certificate details:

```
(Instant AP) # show ap1xcert
```

To verify the configuration, use any of the following commands:

```
(Instant AP) # show ap1x config
(Instant AP) # show ap1x debug-logs
(Instant AP) # show ap1x status
```

Configuring MAC Authentication for a Network Profile

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

This section describes the following procedures:

- [Configuring MAC Authentication for Wireless Network Profiles on page 169](#)
- [Configuring MAC Authentication for Wired Profiles on page 170](#)

Configuring MAC Authentication for Wireless Network Profiles

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

In the AOS-W Instant UI

To enable MAC Authentication for a wireless network:

1. On the **Network** tab, click **New** to create a new network profile or select an existing profile for which you want to enable MAC authentication and click **edit**.
2. In the **Edit <profile-name>** or the **New WLAN** window, ensure that all required WLAN and VLAN attributes are defined, and then click **Next**.
3. On the **Security** tab, select **Enabled** from the **MAC authentication** drop-down list for the **Personal** or the **Open** security level.
4. Specify the type of authentication server to use.
5. If an internal authentication server is used, perform the following steps to allow MAC-address-based authentication:
 - a. Click the **Users** link beside the **Internal server** parameter. The **Users** window is displayed.
 - b. Specify the client MAC address as the username and password.
 - c. Specify the type of the user (employee or guest).
 - d. Click **Add**.
 - e. Repeat the steps to add more users.

- f. Click **OK**.
6. To allow the OAW-IAP to use a delimiter in the MAC authentication request, specify a character (for example, colon or dash) as a delimiter for the MAC address string. For example, if you specify colon as the delimiter, MAC addresses in the xx:xx:xx:xx:xx:xx format are used. If the delimiter is not specified, the MAC address in the xxxxxxxxxxxx format is used.
7. To allow the OAW-IAP to use uppercase letters in the MAC address string, set **Uppercase support** to **Enabled**.
8. Configure other parameters as required.
9. Click **Next** to define access rules, and then click **Finish** to apply the changes.

In the CLI

To configure MAC-address based authentication with external server:

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

To add users for MAC authentication based on internal authentication server:

```
(Instant AP) (config)# user <username> [<password>] [portal|radius]
(Instant AP) (config)# end
(Instant AP)# commit apply
```

Configuring MAC Authentication for Wired Profiles

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

In the AOS-W Instant UI

To enable MAC authentication for a wired profile:

1. Click the **Wired** link under **More** in the main window. The **Wired** window is displayed.
2. Click **New** under **Wired Networks** to create a new network or select an existing profile for which you want to enable MAC authentication and then click **Edit**.
3. In the **New Wired Network** or the **Edit Wired Network** window, ensure that all the required Wired and VLAN attributes are defined, and then click **Next**.
4. On the **Security** tab, select **Enabled** from the **MAC authentication** drop-down list.
5. Specify the type of authentication server to use.
6. If an internal authentication server is used, perform the following steps to allow MAC-address-based authentication:
 - a. Click the **Users** link beside **Internal server**. The **Users** window is displayed.
 - b. Specify the client MAC address as the username and password.
 - c. Specify the type of the user (employee or guest).
 - d. Click **Add**.
 - e. Repeat the steps to add more users.

- f. Click **OK**.
7. Configure other parameters as required.
8. Click **Next** to define access rules, and then click **Finish** to apply the changes.

In the CLI

To configure MAC-address-based authentication with external server:

```
(Instant AP) (config)# wired-port-profile <name>
(Instant AP) (wired ap profile <name>)# type {<employee>|<guest>}
(Instant AP) (wired ap profile <name>)# mac-authentication
(Instant AP) (wired ap profile <name>)# auth-server <server-1>
(Instant AP) (wired ap profile <name>)# auth-server <server-2>
(Instant AP) (wired ap profile <name>)# server-load-balancing
(Instant AP) (wired ap profile <name>)# radius-reauth-interval <Minutes>
(Instant AP) (wired ap profile <name>)# end
(Instant AP)# commit apply
```

To add users for MAC authentication based on internal authentication server:

```
(Instant AP) (config)# user <username> [<password>] [portal|radius]
(Instant AP) (config)# end
(Instant AP)# commit apply
```

Configuring MAC Authentication with 802.1X Authentication

This section describes the following procedures:

- [Configuring MAC and 802.1X Authentications for Wireless Network Profiles on page 171](#)
- [Configuring MAC and 802.1X Authentications for Wired Profiles on page 172](#)

Configuring MAC and 802.1X Authentications for Wireless Network Profiles

You can configure MAC authentication with 802.1X authentication for a wireless network profile using the AOS-W Instant UI or the CLI.

In the AOS-W Instant UI

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

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

In the CLI

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

```
(Instant AP) (config)# wlan ssid-profile <name>
(Instant AP) (SSID Profile <name>)# type {<Employee>|<Voice>|<Guest>}
(Instant AP) (SSID Profile <name>)# mac-authentication
```

```
(Instant AP) (SSID Profile <name>)# l2-auth-failthrough
(Instant AP) (SSID Profile <name>)# auth-server <server-name1>
(Instant AP) (SSID Profile <name>)# radius-reauth-interval <minutes>
(Instant AP) (SSID Profile <name>)# auth-survivability
(Instant AP) (SSID Profile <name>)# exit
(Instant AP) (config)# auth-survivability cache-time-out <hours>
(Instant AP) (config)# end
(Instant AP)# commit apply
```

Configuring MAC and 802.1X Authentications for Wired Profiles

You can configure MAC and 802.1X authentications for a wired profile in the AOS-W Instant UI or the CLI.

In the AOS-W Instant UI

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

1. Click the **Wired** link under **More** in the main window. The **Wired** window is displayed.
2. Click **New** under **Wired Networks** to create a new network or select an existing profile for which you want to enable MAC authentication and then click **Edit**.
3. In the **New Wired Network** or the **Edit Wired Network** window, ensure that all the required Wired and VLAN attributes are defined, and then click **Next**.
4. On the **Security** tab, perform the following steps:
 - Select **Enabled** from the **MAC authentication** drop-down list.
 - Select **Enabled** from the **802.1X authentication** drop-down list.
 - Select **Enabled** from the **MAC authentication fail-thru** drop-down list.
5. Specify the type of authentication server to use and configure other required parameters. For more information on configuration parameters, see [Configuring Security Settings for a Wired Profile on page 108](#).
6. Click **Next** to define access rules, and then click **Finish** to apply the changes.

In the CLI

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

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

Configuring MAC Authentication with Captive Portal Authentication

The following configuration conditions apply to MAC + captive portal authentication method:

- If the captive portal splash page type is **Internal-Authenticated** or **External-RADIUS Server**, MAC authentication reuses the server configurations.
- If the captive portal splash page type is **Internal-Acknowledged** or **External-Authentication Text** and MAC authentication is enabled, a server configuration page is displayed.

You can configure the MAC authentication with captive portal authentication for a network profile using the AOS-W Instant UI or the CLI.

In the AOS-W Instant UI

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



To enable MAC authentication with captive portal authentication on a new WLAN SSID or wired profile, click the **Security** tab on the **New WLAN** window and the **New Wired Network** window.

2. On the **Security** tab, specify the following parameters:
 - a. Select **Enabled** from the **MAC authentication** drop-down list to enable MAC authentication for captive portal users. If the MAC authentication fails, the captive portal authentication role is assigned to the client.
 - b. To enforce MAC authentication, click the **Access** tab and select **Enforce MAC auth only role** check box.
3. Click **Next** and then click **Finish** to apply the changes.

In the CLI

To configure MAC authentication with captive portal authentication for a wireless profile:

```
(Instant AP) (config)# wlan ssid-profile <name>
(Instant AP) (SSID Profile <name>)# type <guest>
(Instant AP) (SSID Profile <name>)# mac-authentication
(Instant AP) (SSID Profile <name>)# captive-portal {<type> [exclude-uplink <types>]|external
[Profile <name>] [exclude-uplink <types>]}
(Instant AP) (SSID Profile <name>)# set-role-mac-auth <mac-only>
(Instant AP) (SSID Profile <name>)# end
(Instant AP)# commit apply
```

To configure MAC authentication with captive portal authentication for a wired profile:

```
(Instant AP) (config)# wired-port-profile <name>
(Instant AP) (wired ap profile <name>)# type <guest>
(Instant AP) (wired ap profile <name>)# mac-authentication
(Instant AP) (wired ap profile <name>)# captive-portal <type>
(Instant AP) (wired ap profile <name>)# captive-portal {<type> [exclude-uplink <types>]
|external [Profile <name>] [exclude-uplink <types>]}
(Instant AP) (wired ap profile <name>)# set-role-mac-auth <mac-only>
(Instant AP) (wired ap profile <name>)# end
(Instant AP)# commit apply
```

Configuring WISPr Authentication

AOS-W Instant supports the following smart clients:

- iPass
- Boingo

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



Wireless Internet Service Provider roaming (WISPr) authentication is supported only for the **Internal - Authenticated** and **External - RADIUS Server** captive portal authentication. Select the **Internal - Authenticated** or the **External - RADIUS Server** option from the **Splash page type** drop-down list to configure WISPr authentication for a WLAN profile.

You can configure WISPr authentication using the AOS-W Instant UI or the CLI.

In the AOS-W Instant UI

1. Click the **System** link located directly above the Search bar in the AOS-W Instant main window. The **System** window is displayed.
2. Click **Show advanced options**.
3. Click **WISPr** tab. The **WISPr** tab contents are displayed. The following figure shows the **WISPr** tab contents:

Figure 36 *Configuring WISPr Authentication*



The screenshot shows a configuration form with six input fields arranged in two columns. The left column contains: 'ISO country code:', 'E.164 area code:', and 'Operator name:'. The right column contains: 'E.164 country code:', 'SSID/Zone:', and 'Location name:'. Each label is followed by a rectangular text input box.

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

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



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

In the CLI

```
(Instant AP) (config)# wlan wispr-profile
(Instant AP) (WISPr)# wispr-location-id-ac
(Instant AP) (WISPr)# wispr-location-id-cc
(Instant AP) (WISPr)# wispr-location-id-isocc
(Instant AP) (WISPr)# wispr-location-id-network
(Instant AP) (WISPr)# wispr-location-name-location
(Instant AP) (WISPr)# wispr-location-name-operator-name
(Instant AP) (WISPr)# end
(Instant AP)# commit apply
```

Blacklisting Clients

The client blacklisting denies connection to the blacklisted clients. When a client is blacklisted, it is not allowed to associate with an OAW-IAP in the network. If a client is connected to the network when it is blacklisted, a deauthentication message is sent to force client disconnection.

This section describes the following procedures:

- [Blacklisting Clients Manually on page 175](#)
- [Blacklisting Users Dynamically on page 175](#)

Blacklisting Clients Manually

Manual blacklisting adds the MAC address of a client to the blacklist. These clients are added into a permanent blacklist. These blacklisted clients are not allowed to connect to the network unless they are removed from the blacklist.

Adding a Client to the Blacklist

You can add a client to the blacklist manually using the AOS-W Instant UI or the CLI.

In the AOS-W Instant UI

1. Click the **Security** link located directly above the Search bar in the AOS-W Instant main window.
2. Click the **Blacklisting** tab.
3. Under the **Manual Blacklisting**, click **New**.
4. Enter the MAC address of the client to be blacklisted in the **MAC address to add** text box.



For the blacklisting to take effect on the MAC address, you must enable blacklisting in the SSID profile. For more information, see [Blacklisting on page 93](#).

5. Click **OK**. The **Blacklisted Since** tab displays the time at which the current blacklisting has started for the client.
6. To delete a client from the manual blacklist, select the MAC Address of the client under the **Manual Blacklisting**, and then click **Delete**.

In the CLI

To blacklist a client:

```
(Instant AP) (config)# blacklist-client <MAC-Address>
(Instant AP) (config)# end
(Instant AP)# commit apply
```

To enable blacklisting in the SSID profile:

```
(Instant AP) (config)# wlan ssid-profile <name>
(Instant AP) (SSID Profile <name>)# blacklisting
(Instant AP) (SSID Profile <name>)# end
(Instant AP)# commit apply
```

To view the blacklisted clients:

```
(Instant AP)# show blacklist-client
Blacklisted Clients
```

```
-----
MAC                Reason          Timestamp      Remaining time(sec)  AP name
---                -
00:1c:b3:09:85:15  user-defined    17:21:29      Permanent            -
```

Blacklisting Users Dynamically

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

Authentication Failure Blacklisting

When a client takes time to authenticate and exceeds the configured failure threshold, it is automatically blacklisted by an OAW-IAP.

Session Firewall-Based Blacklisting

In session firewall-based blacklisting, an ACL rule is used to enable the option for dynamic blacklisting. When the ACL rule is triggered, it sends out blacklist information and the client is blacklisted.

Configuring Blacklist Duration

You can set the blacklist duration using the AOS-W Instant UI or the CLI.

In the AOS-W Instant UI

To set a blacklist duration:

1. Click the **Security** link located directly above the Search bar in the AOS-W Instant main window.
2. Click the **Blacklisting** tab.
3. Under **Dynamic Blacklisting**:
4. For **Auth failure blacklist time**, the duration in seconds after which the clients that exceed the authentication failure threshold must be blacklisted.
5. For **PEF rule blacklisted time**, enter the duration in seconds after which the clients can be blacklisted due to an ACL rule trigger.

You can configure a maximum number of authentication failures by the clients, after which a client must be blacklisted. For more information on configuring maximum authentication failure attempts, see [Configuring Security Settings for a WLAN SSID Profile on page 88](#).



NOTE

To enable session-firewall-based blacklisting, click **New** and navigate to **WLAN Settings > VLAN > Security > Access** window, and enable the **Blacklist** option of the corresponding ACL rule.

In the CLI

To dynamically blacklist clients:

```
(Instant AP) (config)# auth-failure-blacklist-time <seconds>
(Instant AP) (config)# blacklist-time <seconds>
(Instant AP) (config)# end
(Instant AP)# commit apply
```

To enable blacklisting in the SSID profile:

```
(Instant AP) (config)# wlan ssid-profile <name>
(Instant AP) (SSID Profile <name>)# blacklisting
(Instant AP) (SSID Profile <name>)# end
(Instant AP)# commit apply
```

To view the blacklisted clients:

```
(Instant AP)# show blacklist-client config
Blacklist Time           :60
Auth Failure Blacklist Time :60
Manually Blacklisted Clients
-----
MAC   Time
---  ----
Dynamically Blacklisted Clients
-----
MAC   Reason   Timestamp   Remaining time(sec)  AP IP
---   -
Dyn Blacklist Count   :0
```


Uploading Certificates

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

AOS-W Instant supports the following certificate files:

- Authentication server (PEM format)
- Captive portal server (PEM format)—Customized certificate for internal captive portal server
- CA certificate (PEM or DER format)
- RadSec certificate (PEM or DER format)

This section describes the following procedures:

- [Loading Certificates through AOS-W Instant UI on page 177](#)
- [Loading Certificates through AOS-W Instant CLI on page 178](#)
- [Removing Certificates on page 178](#)
- [Loading Certificates Through OmniVista on page 178](#)

Loading Certificates through AOS-W Instant UI

To load a certificate in the AOS-W Instant UI:

1. Click the **Maintenance** link located directly above the Search bar in the AOS-W Instant main window.
2. Click the **Certificates** tab. The **Certificates** tab contents are displayed.
3. To upload a certificate, click **Upload New Certificate**. The **New Certificate** window is displayed.
4. Browse and select the file to upload.
5. Select any of the following types of certificates from the **Certificate type** drop-down list:
 - CA—CA certificate to validate the identity of the client.
 - Auth Server—The authentication server certificate to verify the identity of the server to the client.
 - Captive portal server—Captive portal server certificate to verify the identity of internal captive portal server to the client.
 - RadSec—The RadSec server certificate to verify the identity of the server to the client.
 - RadSec CA—The RadSec CA certificate for mutual authentication between the OAW-IAP clients and the TLS server.
6. Select the certificate format from the **Certificate format** drop-down list.
7. If you have selected **Auth Server**, **Captive portal server**, or **RadSec** as the type of certificate, enter a passphrase in **Passphrase** and retype the passphrase. If the certificate does not include a passphrase, there is no passphrase required.
8. Click **Browse** and select the appropriate certificate file, and click **Upload Certificate**. The **Certificate Successfully Installed** message is displayed.

The OAW-IAP database can have only one authentication server certificate and one captive portal server certificate at any point in time.



When a Captive Portal server certificate is uploaded using the AOS-W Instant UI, the default management certificate on the UI is also replaced by the Captive portal server certificate.

Loading Certificates through AOS-W Instant CLI

To upload a CA, server, or captive portal certificate:

```
(Instant AP)# copy tftp <ip-address> <filename> {cpserver cert <password> format {p12|pem}|  
radsec {ca|cert <password>} format pem|system {lxca format {der|pem}| lxcert <password> format  
pem}}
```

To download RadSec certificates:

```
(Instant AP)# download-cert radsec ftp://192.0.2.7 format pem [psk <psk>]  
(Instant AP)# download-cert radsecca ftp://192.0.2.7 format pem
```

Removing Certificates

To clear a certificate:

```
(Instant AP)# clear-cert {ca|cp|radsec|radsecca|server}
```

Loading Certificates Through OmniVista

You can manage certificates using OmniVista. The AMP directly provisions the certificates and performs basic certificate verification (such as certificate type, format, version, serial number, and so on) before accepting the certificate and uploading to an OAW-IAP network. The AMP packages the text of the certificate into an HTTPS message and sends it to the VC. After the VC receives this message, it draws the certificate content from the message, converts it to the right format, and saves it on the RADIUS server.

To load a certificate in OmniVista:

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

Figure 37 Loading Certificate through OmniVista

The screenshot shows the 'Certificate' configuration window in the OmniVista interface. The window title is 'Certificate'. The navigation bar includes 'Home', 'Groups', 'APs/Devices', 'Clients', 'Reports', 'System', 'Device Setup', and 'AMP Setup'. The 'Device Setup' tab is active, and the 'Certificate' sub-tab is selected. The form contains the following fields and controls:

- Name:** A text input field.
- Certificate File:** A text input field with a 'Choose File' button and the text 'No file chosen'.
- passphrase:** A text input field.
- Confirm passphrase:** A text input field.
- Format:** A dropdown menu currently set to 'DER'.
- Type:** A dropdown menu currently set to 'Server Cert'.

At the bottom of the form are two buttons: 'Add' and 'Cancel'.

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

Figure 38 Server Certificate

The screenshot shows the 'Certificate' configuration page. The 'Name' field contains 'Test1'. The 'Certificate File' field has a 'Choose File' button and the filename 'Server.p12'. The 'passphrase' and 'Confirm passphrase' fields are masked with dots. The 'Format' dropdown is set to 'PKCS#12' and the 'Type' dropdown is set to 'Server Cert'. 'Add' and 'Cancel' buttons are located at the bottom of the form.

- After you upload the certificate, navigate to **Groups**, click the Instant **Group** and then select **Basic**. The Group name is displayed only if you have entered the **Organization** name in the AOS-W Instant UI. For more information, see [Configuring Organization String on page 312](#) for further information.

Figure 39 Selecting the Group

The screenshot shows the 'Groups' list page. A table displays the following data:

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

The **Virtual Controller Certificate** section displays the certificates (CA cert and Server).

- Click **Save** to apply the changes only to OmniVista. Click **Save and Apply** to apply the changes to the OAW-IAP.
- To clear the certificate options, click **Revert**.

This chapter describes the procedures for configuring user roles, role assignment, and firewall policies.

- [Firewall Policies on page 180](#)
- [Content Filtering on page 193](#)
- [Configuring User Roles on page 197](#)
- [Configuring Derivation Rules on page 199](#)
- [Using Advanced Expressions in Role and VLAN Derivation Rules on page 206](#)

Firewall Policies

AOS-W Instant firewall provides identity-based controls to enforce application-layer security, prioritization, traffic forwarding, and network performance policies for wired and wireless networks. Using AOS-W Instant firewall, you can enforce network access policies that define access to the network, areas of the network that users may access, and the performance thresholds of various applications.

AOS-W Instant supports a role-based stateful firewall. AOS-W Instant firewall recognizes flows in a network and keeps track of the state of sessions. Instant firewall manages packets according to the first rule that matches the packet. The firewall logs on the OAW-IAPs are generated as syslog messages.

Access Control List Rules

You can use Access Control List (ACL) rules to either permit or deny data packets passing through the OAW-IAP. You can also limit packets or bandwidth available to a set of user roles by defining access rules. By adding custom rules, you can block or allow access based on the service or application, source or destination IP addresses.

You can create access rules to allow or block data packets that match the criteria defined in an access rule. You can create rules for either inbound traffic or outbound traffic. Inbound rules explicitly allow or block the inbound network traffic that matches the criteria in the rule. Outbound rules explicitly allow or block the network traffic that matches the criteria in the rule. For example, you can configure a rule to explicitly block outbound traffic to an IP address through the firewall.

The OAW-IAP clients are associated with user roles, that determine the client's network privileges and the frequency at which clients re-authenticate.

AOS-W Instant supports the following types of ACLs:

- ACLs that permit or deny traffic based on the source IP address of the packet.
- ACLs that permit or deny traffic based on the source or destination IP address, and the source or destination port number.
- ACLs that permit or deny traffic based on network services, application, application categories, web categories, and security ratings.



You can configure up to 128 access control entries in an ACL for a user role.

The maximum configurable universal role is 4096.

Configuring ACL Rules for Network Services

This section describes the procedure for configuring ACLs to control access to network services.

- For information on configuring access rules based on application and application categories, see [Configuring ACL Rules for Application and Application Categories on page 269](#).
- For information on configuring access rules based on web categories and web reputation, see [Configuring Web Policy Enforcement Service on page 272](#).

In the AOS-W Instant UI

To configure ACL rules for a user role:

1. Navigate to **Security > Roles**. The **Roles** tab contents are displayed.

Alternatively, you can configure access rules for a wired or wireless client through the WLAN wizard or the Wired Profile window.

- a. To configure access rules through the Wired Profile window:
 - Navigate to **More > Wired**.
 - Click **Edit** and then **Edit Wired Network**.
 - Click **Access**.
 - b. To configure access rules through WLAN wizard:
 - Navigate to **Network > WLAN SSID**.
 - Click **Edit** and then **Edit WLAN**.
 - Click **Access**.
2. Select the role for which you want to configure access rules.
 3. In the **Access rules** section, click **New** to add a new rule. The **New Rule** window is displayed.
 4. Ensure that the rule type is set to **Access Control**.
 5. To configure a rule to control access to network services, select **Network** under service category and specify the following parameters:

Table 39: Access Rule Configuration Parameters

Service Category	Description
Network	<p>Select a service from the list of available services. You can allow or deny access to any or all of the services based on your requirement:</p> <ul style="list-style-type: none"> ● 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. <p>NOTE: If Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) use the same port, ensure that you configure separate access rules to permit or deny access.</p>
Action	<p>Select any of following actions:</p> <ul style="list-style-type: none"> ● Select Allow to allow access to users based on the access rule. ● Select Deny to deny access to users based on the access rule. ● Select Destination-NAT to allow making changes to the destination IP address. ● Select Source-NAT to allow making changes to the source IP address. <p>Default: All client traffic is directed to the default VLAN.</p> <p>Tunnel: The traffic from the Network Assigned clients is directed to the VPN tunnel.</p> <p>VLAN: Specify the non-default VLAN ID to which the guest traffic needs to be redirected to.</p>
Destination	<p>Select a destination option for the access rules for network services, applications, and application categories. You can allow or deny access to any the following destinations based on your requirements.</p> <ul style="list-style-type: none"> ● to all destinations— Access is allowed or denied to all destinations. ● to a particular server—Access is allowed or denied to a particular server. After selecting this option, specify the IP address of the destination server. ● except to a particular server—Access is allowed or denied to servers other than the specified server. After selecting this option, specify the IP address of the destination server. ● to a network—Access is allowed or denied to a network. After selecting this option, specify the IP address and netmask for the destination network. ● except to a network—Access is allowed or denied to networks other than the specified network. After selecting this option, specify the IP address and netmask of the destination network. ● to domain name—Access is allowed or denied to the specified domains. After selecting this option, specify the domain name in the Domain Name text box.
Log	<p>Select the Log check box if you want a log entry to be created when this rule is triggered. AOS-W Instant supports firewall-based logging. Firewall logs on the OAW-IAPs are generated as security logs.</p>

Table 39: Access Rule Configuration Parameters

Service Category	Description
Blacklist	Select the Blacklist check box to blacklist the client when this rule is triggered. The blacklisting lasts for the duration specified as Auth failure blacklist time on the Blacklisting tab of the Security window. For more information, see Blacklisting Clients on page 174 .
Classify media	Select the Classify media check box to prioritize video and voice traffic. When enabled, a packet inspection is performed on all non-NAT traffic and the traffic is marked as follows: <ul style="list-style-type: none"> • Video: Priority 5 (Critical) • Voice: Priority 6 (Internetwork Control)
Disable scanning	Select Disable scanning check box to disable ARM scanning when this rule is triggered. The selection of Disable scanning applies only if ARM scanning is enabled. For more information, see Configuring Radio Settings on page 258 .
DSCP tag	Select the DSCP tag check box to specify a DSCP value to prioritize traffic when this rule is triggered. Specify a value within the range of 0–63. To assign a higher priority, specify a higher value.
802.1p priority	Select the 802.1p priority check box to specify an 802.1p priority. Specify a value between 0 and 7. To assign a higher priority, specify a higher value.

6. Click **OK** and then click **Finish**.

In the CLI

To configure access rules:

```
(Instant AP) (config)# wlan access-rule <access-rule-name>
(Instant AP) (Access Rule <Name>)#rule <dest> <mask> <match/invert> {<protocol> <start-port>
<end-port> {permit|deny|src-nat [vlan <vlan_id>|tunnel]|dst-nat{<IP-address> <port>|<port>}}
[<option1....option9>]
(Instant AP) (Access Rule <Name>)# end
(Instant AP)# commit apply
```

Example

```
(Instant AP) (config)# wlan access-rule employee
(Instant AP) (Access Rule "employee")# rule 10.17.88.59 255.255.255.255 match 6 4343 4343 log
classify-media
(Instant AP) (Access Rule "employee")# rule 192.0.2.8 255.255.255.255 invert 6 110 110 permit
(Instant AP) (Access Rule "employee")# rule 192.0.2.2 255.255.255.0 192.0.2.7 255.255.255.0
match tcp 21 21 deny
(Instant AP) (Access Rule "employee")# rule 192.0.2.2 255.255.255.0 192.0.2.7 255.255.255.0
match udp 21 21 deny
(Instant AP) (Access Rule "employee")# rule 192.0.2.2 255.255.255.0 match 6 631 631 permit
(Instant AP) (Access Rule "employee")# rule 192.0.2.8 255.255.255.255 invert 6 21 21 deny
(Instant AP) (Access Rule "employee")# rule 192.0.2.1 255.255.255.0 invert 17 67 69 deny
(Instant AP) (Access Rule "employee")# end
(Instant AP)# commit apply
```

Configuring Network Address Translation Rules

Network Address Translation (NAT) is the process of modifying network address information when packets pass through a routing device. The routing device acts as an agent between the public (the Internet) and the private (local network), which allows translation of private network IP addresses to a public address space.

AOS-W Instant supports the NAT mechanism to allow a routing device to use the translation tables for mapping the private addresses into a single IP address. When packets are sent from this address, they appear to originate from the routing device. Similarly, if packets are sent to the private IP address, the destination address is translated as per the information stored in the translation tables of the routing device.

Configuring a Source-NAT Access Rule

The source-NAT action in access rules allows the user to override the routing profile entries. For example, when a routing profile is configured to use 0.0.0.0/0, the client traffic in L3 mode access on an SSID destined to the corporate network is sent to the tunnel. When an access rule is configured with **Source-NAT** action, the users can specify the service, protocol, or destination to which the source-NAT is applied.

You can also configure source-based routing to allow client traffic on one SSID to reach the Internet through the corporate network, while the other SSID can be used as an alternate uplink. You can create an access rule to perform source-NAT by using the AOS-W Instant UI or the CLI.

In the AOS-W Instant UI

To configure a source-NAT access rule:

1. Navigate to the WLAN wizard or the Wired settings window:
 - To configure access rules for a WLAN SSID, in the **Network** tab, click **New** to create a new network profile or click **edit** to modify an existing profile.
 - To configure access rules for a wired profile, **More > Wired**. In the **Wired** window, click **New** under **Wired Networks** to create a new network or click **Edit** to select an existing profile.
2. Click the **Access** tab.
3. To configure access rules for the network, move the slider to the **Network-based** access control type. To configure access rules for user roles, move the slider to the **Role-based** access control type.
4. To create a new rule for the network, click **New**. To create an access rule for a user role, select the user role and then click **New**. The **New Rule** window is displayed.
5. In the **New Rule** window, perform the following steps:
 - a. Select **Access control** from the **Rule type** drop-down list.
 - b. Select **Source-NAT** from the **Action** drop-down list, to allow for making changes to the source IP address.
 - c. Select a service from the list of available services.

Default: All client traffic by default will be directed to the native vlan.

Tunnel: All network-based traffic will be directed to the VPN tunnel.

VLAN: All client based traffic will be directed to the specified uplink VLAN using the IP address of the interface that OAW-IAP has on that VLAN. If the interface is not found, this option has no effect.
 - d. Select the required option from the **Destination** drop-down list.
 - e. If required, enable other parameters such as **Log**, **Blacklist**, **Classify media**, **Disable scanning**, **DSCP tag**, and **802.1p priority**.
 - f. Click **OK**.
6. Click **Finish**.

In the CLI

To configure source-NAT access rule:

```
(Instant AP) (config)# wlan access-rule <access_rule>
(Instant AP) (Access Rule "<access_rule>")# rule <dest> <mask> <match> <protocol> <sport>
<eport> src-nat [vlan <vlan_id>|tunnel]
(Instant AP) (Access Rule "<access_rule>")# end
(Instant AP)# commit apply
```

Configuring Policy-Based Corporate Access

To allow different forwarding policies for different SSIDs, you can configure policy-based corporate access. The configuration overrides the routing profile configuration and allows any destination or service to be configured to have direct access to the Internet (bypassing VPN tunnel) based on the ACL rule definition. When policy-based corporate access is enabled, the VC performs source-NAT by using its uplink IP address.

To configure policy-based corporate access:

1. Ensure that an L3 subnet with netmask, gateway, VLAN, and IP address is configured. For more information on configuring L3 subnet, see [Configuring L3-Mobility on page 340](#).
2. Ensure that the source IP address is associated with the IP address configured for the L3 subnet.
3. Create an access rule for the SSID profile with Source-NAT action as described in [Configuring a Source-NAT Access Rule on page 184](#). The source-NAT pool is configured and corporate access entry is created.

Configuring a Destination-NAT Access Rule

AOS-W Instant supports configuration of the destination-NAT rule, which can be used to redirect traffic to the specified IP address and destination port. The destination-NAT configuration is supported only in the bridge mode without VPN.

You can configure a destination-NAT access rule by using the AOS-W Instant UI or the CLI.

In the AOS-W Instant UI

To configure a destination-NAT access rule:

1. Navigate to the WLAN wizard or the Wired settings window:
 - To configure access rules for a WLAN SSID, in the **Network** tab, click **New** to create a new network profile or click **edit** to modify an existing profile.
 - To configure access rules for a wired profile, **More > Wired**. In the **Wired** window, click **New** under **Wired Networks** to create a new network or click **Edit** to select an existing profile.
2. Click the **Access** tab and perform any of the following steps:
 - To configure access rules for the network, move the slider to the **Network-based** access control type.
 - To configure access rules for user roles, move the slider to the **Role-based** access control type.
3. To create a new rule for the network, click **New**. To create an access rule for a user role, select the user role and then click **New**. The **New Rule** window is displayed.
4. In the **New Rule** window, perform the following steps:
 - a. Select **Access control** from the **Rule type** drop-down list.
 - b. Select **destination-NAT** from the **Action** drop-down list, to allow for making changes to the source IP address.
 - c. Specify the IP address and port details.
 - d. Select a service from the list of available services.
 - e. Select the required option from the **Destination** drop-down list.

- f. If required, enable other parameters such as **Log**, **Blacklist**, **Classify media**, **Disable scanning**, **DSCP tag**, and **802.1p priority**.
 - g. Click **OK**.
5. Click **Finish**.

In the CLI

To configure destination-NAT access rule:

```
(Instant AP) (config)# wlan access-rule <access_rule>
(Instant AP) (Access Rule "<access_rule>")# rule <dest> <mask> <match> <protocol> <sport>
<eport> dst-nat ip <IP-address> [<port>]
(Instant AP) (Access Rule "<access_rule>")# end
(Instant AP)# commit apply
```

Configuring ALG Protocols

You can enable or disable protocols for Application Layer Gateway (ALG) using the AOS-W Instant UI or the CLI.

In the AOS-W Instant UI

To enable or disable ALG protocols:

1. Click the **Security** link located directly above the Search bar on the AOS-W Instant main window.
2. Click the **Firewall Settings** tab. The **Firewall Settings** tab contents are displayed. The following figure shows the contents of the **Firewall Settings** tab:

Figure 40 Firewall Settings—ALG Protocols

Application Layer Gateway (ALG) Algorithms	Protection against wired attacks
SIP: <input type="text" value="Enabled"/>	Drop bad ARP: <input type="text" value="Disabled"/>
Vocera: <input type="text" value="Enabled"/>	Fix malformed DHCP: <input type="text" value="Disabled"/>
Alcatel NOE: <input type="text" value="Enabled"/>	ARP poison check: <input type="text" value="Disabled"/>
Cisco Skinny: <input type="text" value="Disabled"/>	

3. Select **Enabled** from the corresponding drop-down lists to enable SIP, VOCERA, Alcatel NOE, and Cisco Skinny protocols.
4. Click **OK**.



When the protocols for ALG are set to **Disabled**, the changes are not applied until the existing user sessions expire. Reboot the OAW-IAP and the client, or wait for a few minutes to view the changes.

In the CLI

To configure protocols for ALG:

```
(Instant AP) (config)# alg
(Instant AP) (ALG)# sccp-disable
(Instant AP) (ALG)# no sip-disable
(Instant AP) (ALG)# no ua-disable
(Instant AP) (ALG)# no vocera-disable
(Instant AP) (ALG)# end
(Instant AP)# commit apply
```

To view the ALG configuration:

```
(Instant AP)# show alg
```

```
Current ALG
-----
ALG      Status
---      -
sccp     Disabled
sip      Enabled
ua       Enabled
vocera   Enabled
```

Configuring Firewall Settings for Protection from ARP Attacks

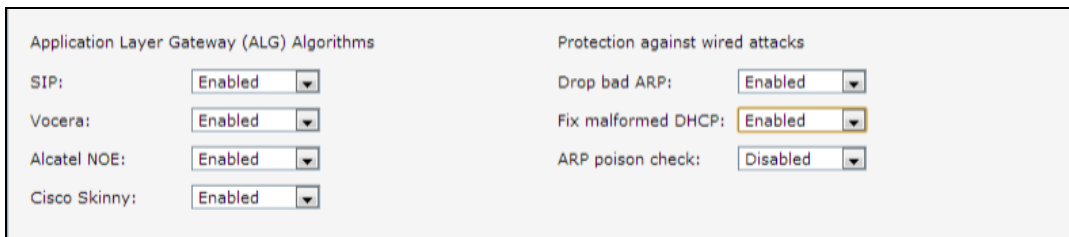
You can configure firewall settings to protect the network against attacks using the AOS-W Instant UI or the CLI.

In the AOS-W Instant UI

To configure firewall settings:

1. Click the **Security** link located directly above the Search bar on the AOS-W Instant main window.
2. Click the **Firewall Settings** tab. The **Firewall Settings** tab contents are displayed.
3. To configure protection against security attacks, select the following check boxes:
 - Select **Drop bad ARP** to enable the OAW-IAP to drop the fake ARP packets.
 - Select **Fix malformed DHCP** for the OAW-IAP to fix the malformed DHCP packets.
 - Select **ARP poison check** to enable the OAW-IAP to trigger an alert notifying the user about the ARP poisoning that may have been caused by the rogue OAW-IAPs.

Figure 41 Firewall Settings —Protection Against Wired Attacks



The screenshot shows two columns of settings. The left column is titled 'Application Layer Gateway (ALG) Algorithms' and contains four rows: SIP: Enabled, Vocera: Enabled, Alcatel NOE: Enabled, and Cisco Skinny: Enabled. The right column is titled 'Protection against wired attacks' and contains three rows: Drop bad ARP: Enabled, Fix malformed DHCP: Enabled, and ARP poison check: Disabled. The 'Fix malformed DHCP' dropdown menu is highlighted with a yellow border.

4. Click **OK**.

In the CLI

To configure firewall settings to prevent attacks:

```
(Instant AP) (config)# attack
(Instant AP) (ATTACK)# drop-bad-arp-enable
(Instant AP) (ATTACK)# fix-dhcp-enable
(Instant AP) (ATTACK)# poison-check-enable
(Instant AP) (ATTACK)# end
(Instant AP)# commit apply
```

To view the configuration status:

```
(Instant AP)# show attack config
```

```
Current Attack
-----
Attack      Status
-----
drop-bad-arp Enabled
fix-dhcp    Enabled
```

```
poison-check Enabled
```

To view the attack statistics

```
(Instant AP)# show attack stats
```

```
attack counters
-----
Counter                               Value
-----
arp packet counter                     0
drop bad arp packet counter            0
dhcp response packet counter           0
fixed bad dhcp packet counter          0
send arp attack alert counter          0
send dhcp attack alert counter         0
arp poison check counter               0
garp send check counter                0
```

Configuring Firewall Settings to Disable Auto Topology Rules

By default, the auto topology rules in an OAW-IAP are enabled. You can disable the rules by configuring firewall settings in the OAW-IAP.

In order to deny auto topology communication outside the OAW-IAP subnet, the inbound firewall settings must be enabled.

When the inbound firewall settings are enabled:

- Access Control Entities (ACEs) must be configured to block auto topology messages, as there is no default rule at the top of predefined ACLs.
- ACEs must be configured to override the guest VLAN auto-expanded ACEs. In other words, the user defined ACEs take higher precedence over guest VLAN ACEs.

For more information on inbound firewall settings, see [Managing Inbound Traffic](#).



The priority of a particular ACE is determined based on the order in which it is programmed. Ensure that you do not accidentally override the guest VLAN ACEs.

You can change the status of auto topology rules by using the AOS-W Instant UI or the CLI:

In the AOS-W Instant UI

1. Click the **Security** located directly above the Search bar in the AOS-W Instant main window.
2. Go to the **Firewall Settings** tab.
3. In **Firewall** section, select **Disabled** from the **Auto topology rules** drop-down list.
4. Click **OK**.

In the CLI

```
(Instant AP)(config)# firewall
(Instant AP)(firewall)# disable-auto-topology-rules
(Instant AP)(firewall)# end
(Instant AP)# commit apply
```

To view the configuration status:

```
Firewall
-----
Type           Value
-----
Auto topology rules  disable
```

Managing Inbound Traffic

AOS-W Instant now supports an enhanced inbound firewall by allowing the configuration of firewall rules and management subnets, and restricting corporate access through an uplink switch.

To allow flexibility in firewall configuration, AOS-W Instant supports the following features:

- Inbound firewall rules
- Configurable management subnets
- Restricted corporate access

Configuring Inbound Firewall Rules

You can now configure firewall rules for the inbound traffic coming through the uplink ports of an OAW-IAP. The rules defined for the inbound traffic are applied if the destination is not a user connected to the OAW-IAP. If the destination already has a user role assigned, the user role overrides the actions or options specified in the inbound firewall configuration. However, if a deny rule is defined for the inbound traffic, it is applied irrespective of the destination and user role. Unlike the ACL rules in a WLAN SSID or a wired profile, the inbound firewall rules can be configured based on the source subnet.

For all subnets, a deny rule is created by default as the last rule. If at least one rule is configured, the deny all rule is applied to the upstream traffic by default.



Management access to the OAW-IAP is allowed irrespective of the inbound firewall rule. For more information on configuring restricted management access, see [Configuring Management Subnets on page 191](#).

The inbound firewall is not applied to traffic coming through the GRE tunnel.

You can configure inbound firewall rules through the AOS-W Instant UI or the CLI.

In the AOS-W Instant UI

1. Navigate to **Security > Inbound Firewall**. The **Inbound Firewall** tab contents are displayed.
2. Under **Inbound Firewall Rules**, click **New**. The **New Rule** window is displayed.

Figure 42 *Inbound Firewall Rules - New Rule Window*

A screenshot of the "New Rule" configuration window. It features four dropdown menus: "Action" set to "Allow", "Service" set to "any", "Source" set to "from all sources", and "Destination" set to "to all destinations". Below these are four checkboxes under the "Options" section: "Log", "Classify media", "DSCP tag", "Blacklist", "Disable scanning", and "802.1p priority", all of which are currently unchecked. "OK" and "Cancel" buttons are located at the bottom right of the window.

3. Configure the following parameters:

Table 40: Inbound Firewall Rule Configuration Parameters

Parameter	Description
Action	<p>Select any of following actions:</p> <ul style="list-style-type: none"> • Select Allow to allow to access users based on the access rule. • Select Deny to deny access to users based on the access rule. • Select Destination-NAT to allow making changes to the destination IP address. • Select Source-NAT to allow making changes to the source IP address. <p>The destination-NAT and source-NAT actions apply only to the network services rules.</p>
Service	<p>Select a service from the list of available services. You can allow or deny access to any or all of the services based on your requirement:</p> <ul style="list-style-type: none"> • 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 the Other option is selected, ensure that an appropriate ID is entered.
Source	<p>Select any of the following options:</p> <ul style="list-style-type: none"> • from all sources—Traffic from all sources is either allowed, denied, or the IP address is translated at the source or the destination as defined in the rule. • from a host—Traffic from a particular host is either allowed, denied, or the IP address is translated at the source or the destination as defined in the rule. After selecting this option, specify the IP address of the host. • from a network—Traffic from a particular network is either allowed, denied, or the IP address is translated at the source or the destination as defined in the rule. After selecting this option, specify the IP address and netmask of the source network.
Destination	<p>Select a destination option for the access rules for network services, applications, and application categories. You can allow or deny access to any the following destinations based on your requirements.</p> <ul style="list-style-type: none"> • to all destinations—Traffic for all destinations is allowed, denied, or the IP address is translated at the source or the destination as defined in the rule. • to a particular server—Traffic to a specific server is allowed, denied, or the IP address is translated at the source or the destination as defined in the rule. After selecting this option, specify the IP address of the destination server. • except to a particular server—Access is allowed or denied to servers other than the specified server. After selecting this option, specify the IP address of the destination server. • to a network—Traffic to the specified network is allowed, denied, or the IP address is translated at the source or the destination as defined in the rule. After selecting this option, specify the IP address and netmask for the destination network. • except to a network—Access is allowed or denied to networks other than the specified network. After selecting this option, specify the IP address and netmask of the destination network. • to domain name—Traffic to the specified domain is allowed, denied, or the IP address is translated at the source or the destination as defined in the rule. After selecting this option, specify the domain name in the Domain Name text box.

Table 40: Inbound Firewall Rule Configuration Parameters

Parameter	Description
Log	Select the Log check box if you want a log entry to be created when this rule is triggered. AOS-W Instant supports firewall-based logging function. Firewall logs on the OAW-IAPs are generated as security logs.
Blacklist	Select the Blacklist check box to blacklist the client when this rule is triggered. The blacklisting lasts for the duration specified in the Auth failure blacklist time on the Blacklisting tab of the Security window. For more information, see Blacklisting Clients on page 174 .
Classify media	Select the Classify media check box to prioritize video and voice traffic. When enabled, a packet inspection is performed on all non-NAT traffic and the traffic is marked as follows: <ul style="list-style-type: none"> • Video: Priority 5 (Critical) • Voice: Priority 6 (Internetwork Control)
Disable scanning	Select Disable scanning check box to disable ARM scanning when this rule is triggered. The selection of Disable scanning applies only if ARM scanning is enabled. For more information, see Configuring Radio Settings on page 258 .
DSCP tag	Select the DSCP tag check box to specify a DSCP value to prioritize traffic when this rule is triggered. Specify a value within the range of 0–63. To assign a higher priority, specify a higher value.
802.1p priority	Select the 802.1p priority check box to specify an 802.1p priority. Specify a value between 0 and 7. To assign a higher priority, specify a higher value.

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

In the CLI

To configure inbound firewall rules:

```
(Instant AP) (config)# inbound-firewall
(Instant AP) (inbound-firewall)# rule <subnet> <smask> <dest> <mask> <protocol> <sport> <eport>
{permit|deny|src-nat|dst-nat <IP-address> <port>} [<option1...option9>]
(Instant AP) (inbound-firewall)# end
(Instant AP)# commit apply
```

Example

```
(Instant AP) (config)# inbound-firewall
(Instant AP) (inbound-firewall)# rule 192.0.2.1 255.255.255.255 any any match 6 631 631 permit
(Instant AP) (inbound-firewall)# end
(Instant AP)# commit apply
```

Configuring Management Subnets

You can configure subnets to ensure that the OAW-IAP management is carried out only from these subnets. When the management subnets are configured, access through Telnet, SSH, and UI is restricted to these subnets only.

You can configure management subnets by using the AOS-W Instant UI or the CLI.

In the AOS-W Instant UI

To configure management subnets:

1. Navigate to **Security > Inbound Firewall**. The **Inbound Firewall** tab contents are displayed.

Figure 43 Firewall Settings—Management Subnets

The screenshot displays the 'Inbound Firewall Configuration' page. At the top, there is a section for 'Inbound Firewall Rules' with a list of rules and buttons for 'New', 'Edit', 'Delete', and arrows for moving items. Below this is the 'Inbound Firewall Configuration' section. On the left, there is a table titled 'Management Subnets' with columns for 'Subnet' and 'Mask'. Below the table are 'Delete' and 'Delete All' buttons. On the right, there is an 'Add new management subnet' section with input fields for 'Subnet' and 'Mask', and an 'Add' button. Below this is a 'Restrict Corporate Access' dropdown menu currently set to 'Disabled'.

2. To add a new management subnet:
 - In the **Add new management subnet** section, enter the subnet address in **Subnet**.
 - Enter the subnet mask in **Mask**.
 - Click **Add**.
3. To add multiple subnets, repeat step 2.
4. Click **OK**.

In the CLI

To configure a management subnet:

```
(Instant AP) (config) # restricted-mgmt-access <subnet-IP-address> <subnet-mask>
(Instant AP) (config) # end
(Instant AP) # commit apply
```

Configuring Restricted Access to Corporate Network

You can configure restricted corporate access to block unauthorized users from accessing the corporate network. When restricted corporate access is enabled, corporate access is blocked from the uplink port of master OAW-IAP, including clients connected to a slave OAW-IAP. You can configure restricted corporate access by using the AOS-W Instant UI or the CLI.

In the AOS-W Instant UI

To configure restricted corporate access:

1. Navigate to **Security > Inbound Firewall**. The **Inbound Firewall** (see [Figure 43](#)) tab contents are displayed.
2. Select **Enabled** from the **Restrict Corporate Access** drop-down list.
3. Click **OK**.

In the CLI

To configure restricted management access:

```
(Instant AP) (config) # restrict-corp-access
(Instant AP) (config) # end
(Instant AP) # commit apply
```


Content Filtering

The content filtering feature allows you to route DNS requests to the OpenDNS platform and create content filtering policies.

With content filter, you can achieve the following:

- Allow all DNS requests to the non-corporate domains on a wireless or wired network to be sent to the OpenDNS server. When the OpenDNS credentials are configured, the OAW-IAP uses these credentials to access OpenDNS and provide enterprise-level content filtering. For more information, see [Configuring OpenDNS Credentials on page 295](#).
- Block certain categories of websites based on your organization policy. For example, if you block the **web-based-email** category, clients who are assigned this policy will not be able to visit email-based websites such as mail.yahoo.com.
- Prevent known malware hosts from accessing your wireless network.
- Improve employee productivity by limiting access to certain websites.
- Reduce bandwidth consumption significantly.



Regardless of whether content filtering is disabled or enabled, the DNS requests to <http://instant.alcatel-lucentnetworks.com> are always resolved internally on AOS-W Instant.

The content filtering configuration applies to all OAW-IAPs in the network and the service is enabled or disabled globally across the wireless or wired network profiles.

Enabling Content Filtering

This section describes the following procedures:

- [Enabling Content Filtering for a Wireless Profile on page 193](#)
- [Enabling Content Filtering for a Wired Profile on page 193](#)

Enabling Content Filtering for a Wireless Profile

To enable content filtering for a wireless SSID, perform the following steps:

In the AOS-W Instant UI

1. Select a wireless profile in the **Network** tab and then click the **edit** link. The window for editing the WLAN SSID profile is displayed.
2. Click **Show advanced options**.
3. Select **Enabled** from the **Content Filtering** drop-down list, and click **Next** to continue.

You can also enable content filtering while adding a new wireless profile. For more information, see [Configuring WLAN Settings for an SSID Profile on page 80](#).

In the CLI

To enable content filtering on a WLAN SSID:

```
(Instant AP) (config)# wlan ssid-profile <name>
(Instant AP) (SSID Profile <name>)# content-filtering
(Instant AP) (SSID Profile <name>)# end
(Instant AP)# commit apply
```

Enabling Content Filtering for a Wired Profile

To enable content filtering for a wired profile, perform the following steps:

In the AOS-W Instant UI

1. Click the **Wired** link under **More** in the AOS-W Instant main window. The **Wired** window is displayed.
2. In the **Wired** window, select the wired profile to modify.
3. Click **Edit**. The **Edit Wired Network** window is displayed.
4. In the **Wired Settings** tab, select **Enabled** from the **Content Filtering** drop-down list, and click **Next** to continue.

In the CLI

To enable content filtering for a wired profile in the CLI:

```
(Instant AP) (config)# wired-port-profile test
(Instant AP) (wired ap profile <name>)# content-filtering
(Instant AP) (wired ap profile <name>)# end
(Instant AP)# commit apply
```

Configuring Enterprise Domains

The enterprise domain names list displays the DNS domain names that are valid on the enterprise network. This list is used to determine how client DNS requests must be routed. When **Content Filtering** is enabled, the DNS request of the clients is verified and the domain names that do not match the names in the list are sent to the OpenDNS server.

You can configure an enterprise domain through the AOS-W Instant UI or the CLI.

In the AOS-W Instant UI

To manually add a domain:

1. Navigate to **System > General** and click **Show advanced options > Enterprise Domains**. The **Enterprise Domain** tab contents are displayed.
2. Click **New** and enter a **New Domain Name**. Using asterisk (*) as an enterprise domain causes all DNS traffic to go through the tunnel to the original DNS server of clients. If you are configuring routing profile with split-tunnel disabled, you need to add asterisk (*) to the enterprise domain list.
3. Click **OK** to apply the changes.

To delete a domain, select the domain and click **Delete**. This will remove the domain name from the list.

In the CLI

To configure an enterprise domain:

```
(Instant AP) (config)# internal-domains
(Instant AP) (domain)# domain-name <name>
(Instant AP) (domain)# end
(Instant AP)# commit apply
```

Configuring URL Filtering Policies

You can configure URL filtering policies to block certain categories of websites based on your organization specifications by defining ACL rules either through the AOS-W Instant UI or the CLI.

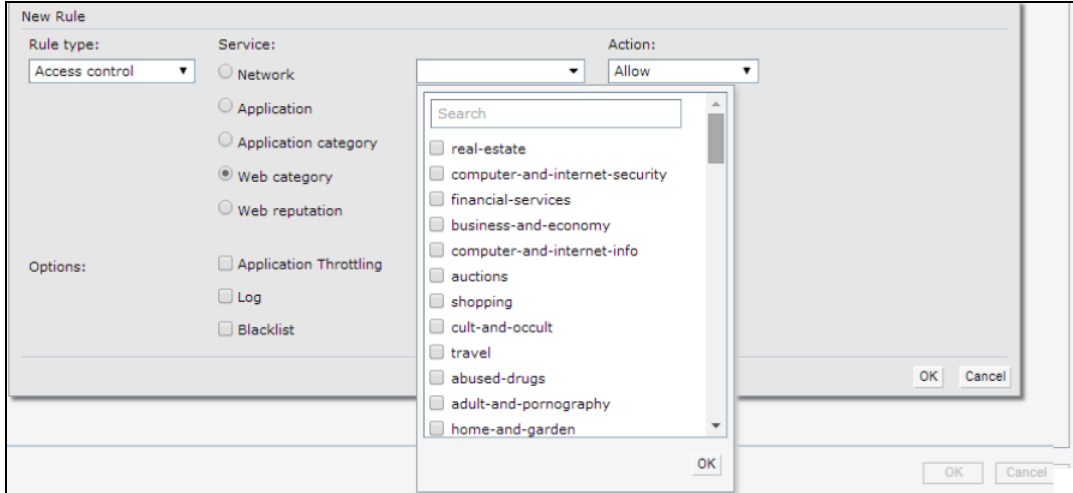
In the AOS-W Instant UI

To control access based on web categories and security settings:

1. Navigate to **Security > Roles**.
2. Select any WLAN SSID or wired profile role, and click **New** in the Access Rules section. The New Rule window appears.
3. Select **Access Control** from the **Rule Type** drop-down list.

4. To set an access policy based on the web category:
 - a. Under **Service** section, select **Web category** and expand the **Web categories** drop-down list.

Figure 44 Roles—New Rule



- b. Select the categories to which you want to deny or allow access. You can also search for a web category and select the required option.
 - c. From the **Action** drop-down list, select **Allow** or **Deny** as required.
 - d. Click **OK**.
5. To filter access based on the security ratings of the website:
 - a. Select **Web reputation** under **Service** section.
 - b. Move the slider to the required security rating level.
 - c. From the **Action** drop-down list, select **Allow** or **Deny** as required.
6. To set a bandwidth limit based on web category or web reputation score, select **Application Throttling** check box and specify the downstream and upstream rates in Kbps. For example, you can set a higher bandwidth for trusted sites and a low bandwidth rate for high-risk sites.
7. Click **OK** to save the rules.
8. Click **OK** in the **Roles** tab to save the changes to the role for which you defined ACL rules.

In the CLI

To control access based on web categories and security ratings:

```
(Instant AP) (config)# wlan access-rule <access_rule>
(Instant AP) (Access Rule "<access-rule>")# rule <dest> <mask> <match> webcategory <webgrp>
{permit| deny}[<option1...option9>]
(Instant AP) (Access Rule "<access-rule>")# rule <dest> <mask> <match> webreputation <webrep>
{permit|deny}[<option1...option9>]
(Instant AP) (Access Rule "<access-rule>")# end
(Instant AP)# commit apply
```

Example

```
(Instant AP) (config)# wlan access-rule URLFilter
(Instant AP) (Access Rule "URLFilter")# rule any any match webcategory gambling deny
(Instant AP) (Access Rule "URLFilter")# rule any any match webcategory training-and-tools
permit
(Instant AP) (Access Rule "URLFilter")# rule any any match webreputation trustworthy-sites
permit
(Instant AP) (Access Rule "URLFilter")# rule any any match webreputation suspicious-sites deny
(Instant AP) (Access Rule "URLFilter")# end
(Instant AP)# commit apply
```

Creating Custom Error Page for Web Access Blocked by AppRF Policies

You can create a list of URLs to which the users are redirected when they access blocked websites. You can define an access rule to use these redirect URLs and assign the rule to a user role in the WLAN network.

You can create a list of custom URLs and ACL rules for blocked websites either through the AOS-W Instant UI or the CLI.

Creating a List of Error Page URLs

To create a list of error page URLs:

In the AOS-W Instant UI

1. Navigate to **Security > Custom Blocked Page URL**.
2. Click **New** and enter the URL that you want to block.
3. Repeat the procedure to add more URLs. You can add up to 8 URLs to the blocked page list.
4. Click **OK**.

In the CLI

```
(Instant AP) (config)# dpi-error-page-url <idx> <url>
(Instant AP) (config)# exit
(Instant AP)# commit apply
```

Configuring ACL Rules to Redirect Blocked HTTP Websites to a Custom Error Page URL

To redirect blocked HTTP websites to a custom error page URL:

In the UI

1. Navigate to **Security > Roles**.
2. Select any WLAN SSID or Wired profile role, and click **New** in the Access Rules section.
3. In the **New Rule** window, select the rule type as **Blocked Page URL**.
4. Select the URLs from the existing list of custom redirect URLs. To add a new URL, click **New**.
5. Click **OK**.
6. Click **OK** in the **Roles** tab to save the changes.

In the CLI

To configure an ACL rule to redirect blocked HTTP websites to a custom error page URL:

```
(Instant AP) (config)# wlan access-rule <access_rule_name>
(Instant AP) (Access Rule "<access_rule_name>")# dpi-error-page-url <idx>
(Instant AP) (Access Rule "<access_rule_name>")# end
(Instant AP)# commit apply
```

Configuring ACL Rules to Redirect Blocked HTTPS Websites to a Custom Blocked Page URL

Before you configure an ACL rule for a specific WLAN SSID or Wired profile to redirect HTTPS websites to a custom error page, you must ensure that the Blocked Page URL rule is configured for the HTTP websites blocked for the same WLAN SSID or Wired profile. In this scenario, all the blocked HTTP and HTTPS websites will be redirected to the custom error page URL.



To redirect blocked HTTPS websites to a custom error page URL

In the UI

1. Navigate to **Security > Roles**.
2. Select any WLAN SSID or Wired profile role, and click **New** in the Access Rules section.

3. In the **New Rule** window, select the rule type as **Redirect Blocked HTTPS**.
4. Click **OK**.
5. Click **OK** in the **Roles** tab to save the changes.

In the CLI

To configure an ACL rule to redirect blocked HTTPS to a custom error page URL:

```
(Instant AP) (config)# wlan access-rule <access_rule_name>
(Instant AP) (Access Rule "<access_rule_name>")# dpi-error-page-url <idx>
(Instant AP) (Access Rule "<access_rule_name>")# redirect-blocked-https-traffic
Instant AP) (Access Rule "<access_rule_name>")# end
(Instant AP)# commit apply
```

Configuring User Roles

Every client in the AOS-W Instant network is associated with a user role that determines the network privileges for a client, the frequency of reauthentication, and the applicable bandwidth contracts.



AOS-W Instant allows you to configure up to 32 user roles. If the number of roles exceed 32, an error message is displayed.

The user role configuration on an OAW-IAP involves the following procedures:

- [Creating a User Role on page 197](#)
- [Assigning Bandwidth Contracts to User Roles on page 198](#)
- [Configuring Machine and User Authentication Roles on page 199](#)

Creating a User Role

You can create a user role by using the AOS-W Instant UI or the CLI.

In the AOS-W Instant UI

To create a user role:

1. Click the **Security** link located directly above the Search bar in the AOS-W Instant main window. The **Security** window is displayed.
2. Click the **Roles** tab. The Roles tab contents are displayed.
3. Under Roles, click **New**.
4. Enter a name for the new role and click **OK**.



You can also create a user role when configuring wireless or wired network profiles. For more information, see [Configuring Access Rules for a WLAN SSID Profile on page 96](#) and [Configuring Access Rules for a Wired Profile on page 109](#).

In the CLI

To configure user roles and access rules:

```
(Instant AP) (config)# wlan access-rule <access-rule-name>
(Instant AP) (Access Rule <Name>)# rule <dest> <mask> <match> <protocol> <start-port> <end-
port> {permit|deny|src-nat [vlan <vlan_id>|tunnel]|dst-nat {<IP-address> <port>|<port>}}
[<option1...option9>]
```

Assigning Bandwidth Contracts to User Roles

The administrators can manage bandwidth utilization by assigning either maximum bandwidth rates, or bandwidth contracts to user roles. The administrator can assign a bandwidth contract configured in Kbps to upstream (client to the OAW-IAP) or downstream (OAW-IAP to clients) traffic for a user role. The bandwidth contract will not be applicable to the user traffic on the bridged out (same subnet) destinations. For example, if clients are connected to an SSID, you can restrict the upstream bandwidth rate allowed for each user to 512 Kbps.

By default, all users that belong to the same role share a configured bandwidth rate for upstream or downstream traffic. The assigned bandwidth will be served and shared among all the users. You can also assign bandwidth rate per user to provide every user a specific bandwidth within a range of 1–65,535 Kbps. If there is no bandwidth contract specified for a traffic direction, unlimited bandwidth is allowed.



In the earlier releases, bandwidth contract could be assigned per SSID. In the current release, the bandwidth contract can also be assigned for each SSID user. If the bandwidth contract is assigned for an SSID in the AOS-W Instant 6.2.1.0-3.4.0.0 version, and when the OAW-IAP is upgraded to AOS-W Instant 6.5.1.0-4.3.1.0 release version, the bandwidth configuration per SSID will be treated as a per-user downstream bandwidth contract for that SSID.

In the AOS-W Instant UI

1. Click the **Security** link located directly above the Search bar in the AOS-W Instant main window. The **Security** window is displayed.
2. Click the **Roles** tab. The **Roles** tab contents are displayed.
3. Create a new role (see [Creating a User Role on page 197](#)) or select an existing role.
4. Under **Access Rules**, click **New**. The **New Rule** window is displayed.
5. Select **Bandwidth Contract** from the **Rule Type** drop-down list.

A screenshot of the "New Rule" dialog box in the AOS-W Instant UI. The dialog has a title bar "New Rule". Below the title bar, there is a "Rule type:" label followed by a dropdown menu showing "Bandwidth Contr". To the right of the dropdown, there are two rows of input fields. The first row is for "Downstream:" with a text input field, "kbps", and a "Peruser" checkbox. The second row is for "Upstream:" with a text input field, "kbps", and a "Peruser" checkbox. At the bottom right of the dialog, there are "OK" and "Cancel" buttons.

6. Specify the downstream and upstream rates in Kbps. If the assignment is specific for each user, select the **Peruser** check box.
7. Click **OK**.
8. Associate the user role to a WLAN SSID or a wired profile.

You can also create a user role and assign bandwidth contracts when [configuring an SSID](#) or a [wired profile](#).

In the CLI:

To assign a bandwidth contract in the CLI:

```
(Instant AP) (config)# wlan access-rule <name>
(Instant AP) (Access Rule <name>)# bandwidth-limit {downstream <kbps>|upstream <kbps>|peruser
{downstream <kbps>| upstream <kbps>}}
(Instant AP) (Access Rule <name>)# end
(Instant AP) # commit apply
```

To associate the access rule to a wired profile:

```
(Instant AP) (config)# wired-port-profile <name>
(Instant AP) (wired ap profile <name>)# access-rule-name <access-rule-name>
(Instant AP) (wired ap profile <name>)# end
```

```
(Instant AP) # commit apply
```

Configuring Machine and User Authentication Roles

You can assign different rights to clients based on whether their hardware device supports machine authentication. Machine authentication is only supported on Windows devices, so that this can be used to distinguish between Windows devices and other devices such as iPads.

You can create any of the following types of rules:

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

When a device does both machine and user authentication, the user obtains the default role or the derived role based on the RADIUS attribute.

You can configure machine authentication with role-based access control using the AOS-W Instant UI or the CLI.

In the AOS-W Instant UI

To configure machine authentication with role-based access control:

1. In the **Access** tab of the WLAN wizard (**New WLAN** or **Edit <WLAN-profile>**) or in the wired profile configuration window (**New Wired Network** or **Edit Wired Network**), under **Roles**, create **Machine auth only** and **User auth only** roles.
2. Configure access rules for these roles by selecting the role, and applying the rule. For more information on configuring access rules, see [Configuring ACL Rules for Network Services on page 180](#).
3. Select **Enforce Machine Authentication** and select the **Machine auth only** and **User auth only** roles.
4. Click **Finish** to apply these changes.

In the CLI

To configure machine and user authentication roles for a WLAN SSID:

```
(Instant AP) (config)# wlan ssid-profile <name>
(Instant AP) (SSID Profile <name>)# set-role-machine-auth <machine_only> <user_only>
(Instant AP) (SSID Profile <name>)# end
(Instant AP)# commit apply
```

To configure machine and user authentication roles for a wired profile:

```
(Instant AP) (config)# wired-port-profile <name>
(Instant AP) (wired ap profile <name>)# set-role-machine-auth <machine_only> <user_only>
(Instant AP) (wired ap profile <name>)# end
(Instant AP)# commit apply
```

Configuring Derivation Rules

AOS-W Instant allows you to configure role and VLAN derivation-rules. You can configure these rules to assign a user role or a VLAN to the clients connecting to an SSID or a wired profile.

Understanding Role Assignment Rule

When an SSID or a wired profile is created, a default role for the clients connecting to this SSID or wired profile is assigned. You can assign a user role to the clients connecting to an SSID by any of the following methods. The role assigned by some methods may take precedence over the roles assigned by the other methods.

RADIUS VSA Attributes

The user role can be derived from Alcatel-Lucent Vendor-Specific Attributes (VSA) for RADIUS server authentication. The role derived from an Alcatel-Lucent VSA takes precedence over roles defined by other methods.

MAC-Address Attribute

The first three octets in a MAC address are known as Organizationally Unique Identifier (OUI), and are purchased from the Institute of Electrical and Electronics Engineers, Incorporated (IEEE) Registration Authority. This identifier uniquely identifies a vendor, manufacturer, or other organization (referred to by the IEEE as the “assignee”) globally and effectively reserves a block of each possible type of derivative identifier (such as MAC addresses) for the exclusive use of the assignee.

OAW-IAPs use the OUI part of a MAC address to identify the device manufacturer and can be configured to assign a desired role for users who have completed 802.1X authentication and MAC authentication. The user role can be derived from the user attributes after a client associates with an OAW-IAP. You can configure rules to assign a user role to clients that match a MAC-address-based criteria. For example, you can assign a voice role to any client with a MAC address starting with a0:a1:a2.

Roles Based on Client Authentication

The user role can be the default user role configured for an authentication method, such as 802.1X authentication. For each authentication method, you can configure a default role for the clients who are successfully authenticated using that method.

DHCP Option and DHCP Fingerprinting

The DHCP fingerprinting allows you to identify the operating system of a device by looking at the options in the DHCP frame. Based on the operating system type, a role can be assigned to the device.

For example, to create a role assignment rule with the DHCP option, select **equals** from the **Operator** drop-down list and enter 370103060F77FC in the **String** text box. Since 370103060F77FC is the fingerprint for Apple iOS devices such as iPad and iPhone, OAW-IAP assigns Apple iOS devices to the role that you choose.

Table 41: Validated DHCP Fingerprint

Device	DHCP Option	DHCP Fingerprint
Apple iOS	Option 55	370103060F77FC
Android	Option 60	3C64686370636420342E302E3135
Blackberry	Option 60	3C426C61636B4265727279
Windows 7/Vista Desktop	Option 55	37010f03062c2e2f1f2179f92b
Windows XP (SP3, Home, Professional)	Option 55	37010f03062c2e2f1f21f92b

Device	DHCP Option	DHCP Fingerprint
Windows Mobile	Option 60	3c4d6963726f736f66742057696e646f777320434500
Windows 7 Phone	Option 55	370103060f2c2e2f
Apple Mac OS X	Option 55	370103060f775ffc2c2e2f

Creating a Role Derivation Rule

You can configure rules for determining the role that is assigned for each authenticated client.



When creating more than one role assignment rule, the first matching rule in the rule list is applied.

You can create a role assignment rule by using the AOS-W Instant UI or the CLI.

In the AOS-W Instant UI

- Navigate to the WLAN wizard or the Wired settings window:
 - To configure access rules for a WLAN SSID, in the **Network** tab, click **New** to create a new network profile or **edit** to modify an existing profile.
 - To configure access rules for a wired profile, go to **More > Wired**. In the **Wired** window, click **New** under **Wired Networks** to create a new network or click **Edit** to select an existing profile.
- Click the **Access** tab.
- Under **Role Assignment Rules**, click **New**. The **New Role Assignment** window allows you to define a match method by which the string in *Operand* is matched with the attribute value returned by the authentication server.
- Select the attribute that matches with the rule from the **Attribute** drop-down list. The list of supported attributes includes RADIUS attributes, dhcp-option, dot1x-authentication-type, mac-address, and mac-address-and-dhcp-options. For information on a list of RADIUS attributes, see [RADIUS Server Authentication with VSA on page 149](#).
- Select the operator from the **Operator** drop-down list. The following types of operators are supported:
 - contains**—The rule is applied only if the attribute value contains the string specified in *Operand*.
 - Is the role**—The rule is applied if the attribute value is the role.
 - equals**—The rule is applied only if the attribute value is equal to the string specified in *Operand*.
 - not-equals**—The rule is applied only if the attribute value is not equal to the string specified in *Operand*.
 - starts-with**—The rule is applied only if the attribute value starts with the string specified in *Operand*.
 - ends-with**—The rule is applied only if the attribute value ends with the string specified in *Operand*.
 - matches-regular-expression**—The rule is applied only if the attribute value matches the regular expression pattern specified in *Operand*. This operator is available only if the **mac-address-and-dhcp-options** attribute is selected in the **Attribute** drop-down list. The **mac-address-and-dhcp-options** attribute and **matches-regular-expression** are applicable only for the WLAN clients.
- Enter the string to match the attribute in the **String** text box.
- Select the appropriate role from the **Role** drop-down list.
- Click **OK**.



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

In the CLI

To configure role assignment rules for a WLAN SSID:

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

To configure role assignment rules for a wired profile:

```
(Instant AP) (config)# wired-port-profile <name>
(Instant AP) (wired ap profile <name>)# set-role <attribute>{{equals|not-equal|starts-with|
ends-with|contains}<operator> <role>|value-of}
(Instant AP) (wired ap profile <name>)# end
(Instant AP)# commit apply
```

Example

```
(Instant AP) (config)# wlan ssid-profile Profile1
(Instant AP) (SSID Profile "Profile1")# set-role mac-address-and-dhcp-options matches-regular-
expression \bring\b Profile1
(Instant AP) (SSID Profile"Profile1")# end
(Instant AP)# commit apply
```

Understanding VLAN Assignment

You can assign VLANs to a client based on the following configuration conditions:

- The default VLAN configured for the WLAN can be assigned to a client.
- If VLANs are configured for a WLAN SSID or an Ethernet port profile, the VLAN for the client can be derived before the authentication, from the rules configured for these profiles.
- If a rule derives a specific VLAN, it is prioritized over the user roles that may have a VLAN configured.
- The user VLANs can be derived from the default roles configured for 802.1X authentication or MAC authentication.
- After client authentication, the VLAN can be derived from Vendor-Specific Attributes (VSA) for RADIUS server authentication.
- The DHCP-based VLANs can be derived for captive portal authentication.



AOS-W Instant supports role derivation based on the DHCP option for captive portal authentication. When the captive portal authentication is successful, the role derivation based on the DHCP option assigns a new user role to the guest users, instead of the pre-authenticated role.

Vendor-Specific Attributes

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 an *Access-Accept* packet from the RADIUS server. The OAW-IAP can analyze the return message and derive the value of the VLAN which it assigns to the user.

Figure 45 RADIUS Access-Accept Packets with VSA

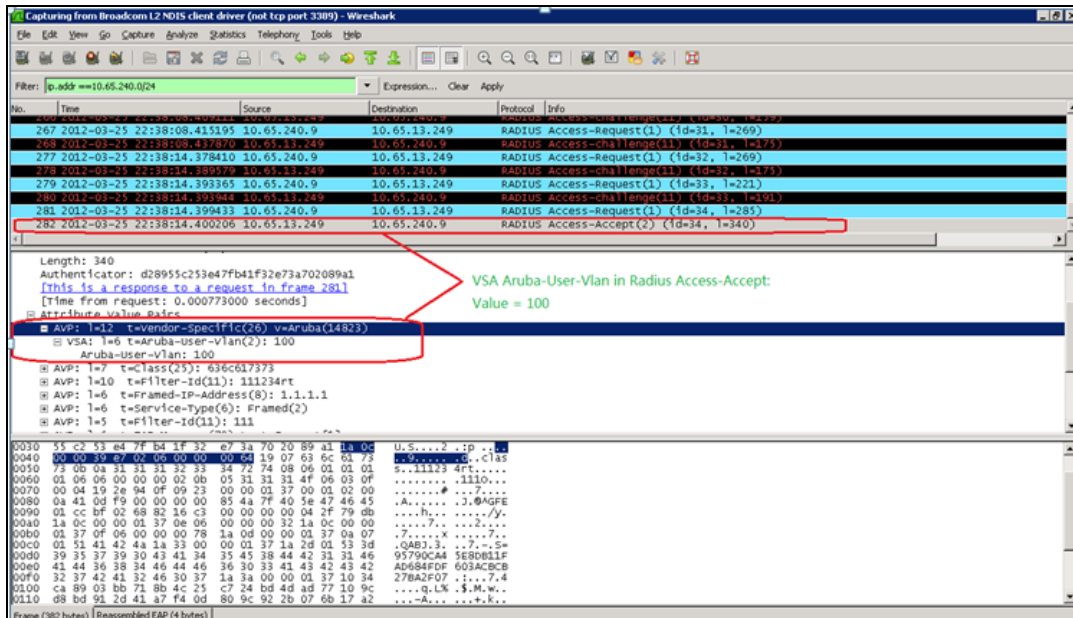
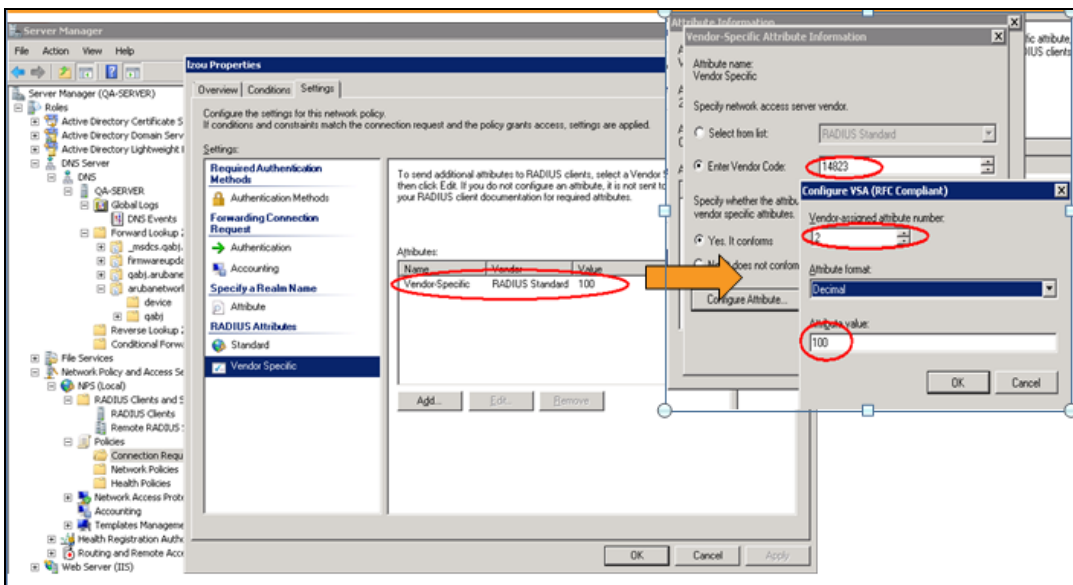


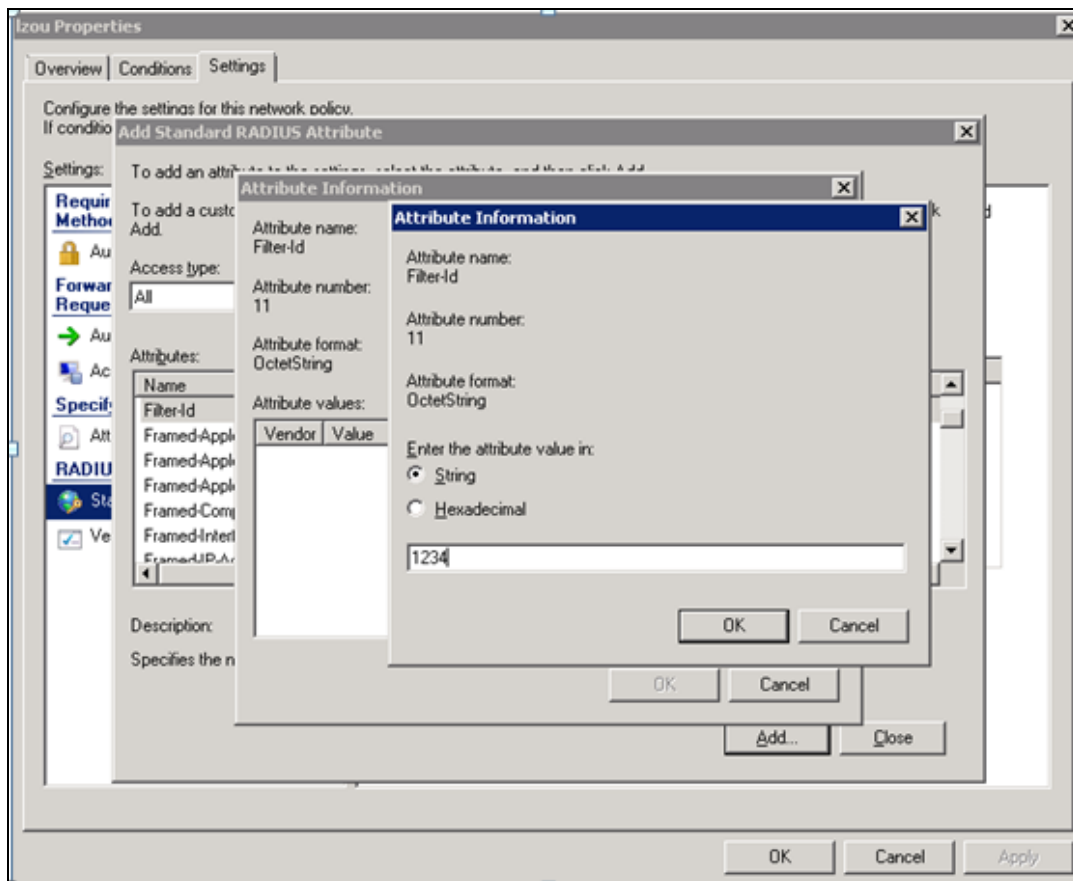
Figure 46 Configure VSA on a RADIUS Server



VLAN Assignment Based on Derivation Rules

When an external RADIUS server is used for authentication, the RADIUS server may return a reply message for authentication. If the RADIUS server supports return attributes, and sets an attribute value to the reply message, the OAW-IAP can analyze the return message and match attributes with a user pre-defined VLAN derivation rule. If the rule is matched, the VLAN value defined by the rule is assigned to the user. For a complete list of RADIUS server attributes, see [RADIUS Server Authentication with VSA on page 149](#).

Figure 47 Configuring RADIUS Attributes on the RADIUS Server



User Role

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

VLANs Created for an SSID

If the VSA and VLAN derivation rules are not matching, and the User Role does not contain a VLAN, the user VLAN can be derived by VLANs configured for an SSID or an Ethernet port profile.

Configuring VLAN Derivation Rules

The VLAN derivation rules allow administrators to assign a VLAN to the OAW-IAP clients based on the attributes returned by the RADIUS server.

You can configure VLAN derivation rules for an SSID profile by using the AOS-W Instant UI or the CLI.

In the AOS-W Instant UI

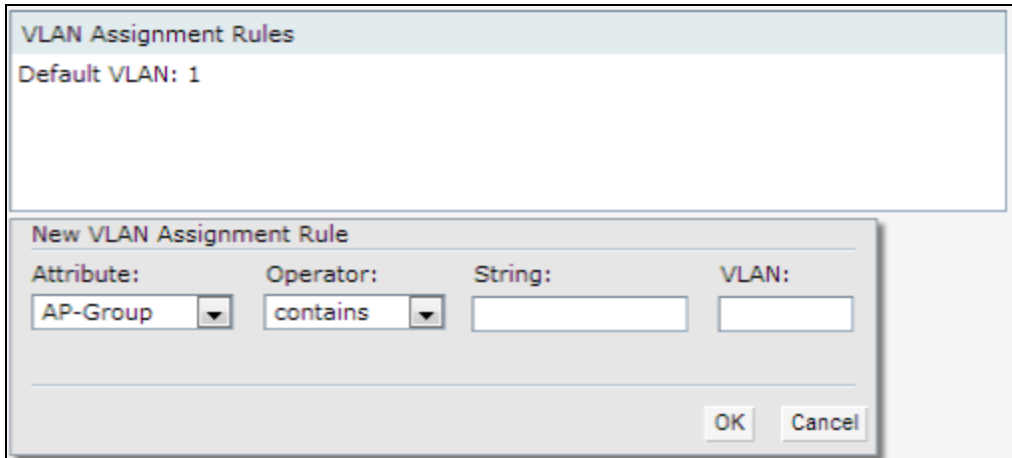
To configure VLAN derivation rules:

1. Perform the following steps:

- To configure VLAN derivation rule for a WLAN SSID profile, navigate to **Network > New > New WLAN > VLAN** or **Network > edit > Edit <WLAN-profile> > VLAN**. Select the **Dynamic** option under the **Client VLAN assignment**.
- To configure VLAN derivation rule for a wired network profile, navigate to **Wired > New > New Wired Network > VLAN** or **Wired > Edit > Edit Wired Network > VLAN**. The **VLAN** tab contents are displayed.

- Click **New** to create a VLAN assignment rule. The **New VLAN Assignment Rule** window is displayed. In this window, you can define a match method by which the string in *Operand* is matched with the attribute values returned by the authentication server.

Figure 48 VLAN Assignment Rule Window



- Select the attribute from the **Attribute** drop-down list. The list of supported attributes includes RADIUS attributes, dhcp-option, dot1x-authentication-type, mac-address, and mac-address-and-dhcp-options. For information on a list of RADIUS attributes, see [RADIUS Server Authentication with VSA on page 149](#).
- Select the operator from the **Operator** drop-down list. The following types of operators are supported:
 - contains**—The rule is applied only if the attribute value contains the string specified in *Operand*.
 - Is the VLAN**—The rule is applied if the VLAN is the same as the one returned by the RADIUS attribute.
 - equals**—The rule is applied only if the attribute value is equal to the string specified in *Operand*.
 - not-equals**—The rule is applied only if the attribute value is not equal to the string specified in *Operand*.
 - starts-with**—The rule is applied only if the attribute value starts with the string specified in *Operand*.
 - ends-with**—The rule is applied only if the attribute value ends with the string specified in *Operand*.
- Enter the string to match the attribute in the **String** text box.
- Select the appropriate VLAN ID from the **VLAN** drop-down list.
- Click **OK**.
- Ensure that the required security and access parameters are configured.
- Click **Finish** to apply the changes.

In the CLI

To create a VLAN assignment rule for a WLAN SSID:

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

To configure a VLAN assignment rule for a wired profile:

```
(Instant AP) (config)# wired-port-profile <nname>
(Instant AP) (wired ap profile <name>)# set-vlan <attribute>{equals|not-equals|starts-
with|ends-with|contains}<operator><VLAN-ID>|value-of}
(Instant AP) (wired ap profile <name>)# end
(Instant AP)# commit apply
```

Example

```
(Instant AP) (config)# wlan ssid-profile Profile1
```

```
(Instant AP) (SSID Profile "Profile1") # set-vlan mac-address-and-dhcp-options matches-regular-expression ..link 100
(Instant AP) (SSID Profile "Profile1") # end
(Instant AP) # commit apply
```

Using Advanced Expressions in Role and VLAN Derivation Rules

For complex policies of role and VLAN derivation using device DHCP fingerprints, you can use a regular expression to match with the combined string of the MAC address and the DHCP options. The combined string is formed by concatenating the hexadecimal presentation of the MAC address and all of the DHCP options sent by a particular device. The regular expression is a powerful pattern description language that can be used to perform advanced pattern matching of the above string.

If the combined device fingerprint string matches the specified regular expression, the role or VLAN can be set to the WLAN client.

The following table lists some of the most commonly used regular expressions, which can be used in user role and user VLAN derivation rules:

Table 42: Regular Expressions

Operator	Description
.	Matches any character. For example, l..k matches lack, lark, link, lock, look, Lync, and so on.
\	Matches the character that follows the backslash. For example, \192.\.0\. matches IP address ranges that start with 192.0, such as 192.0.1.1. The expression looks up only for the single characters that match.
[]	Matches any one character listed between the brackets. For example, [bc]lock matches block and clock.
\b	Matches the words that begin and end with the given expression. For example, \bdown matches downlink, linkdown, shutdown.
\B	Matches the middle of a word. For example, \Bvice matches services, devices, serviceID, deviceID, and so on.
^	Matches the characters at starting position in a string. For example, ^bcd matches bcde or bcdf, but not abcd.
[^]	Matches any characters that are not listed between the brackets. For example, [^u]link matches downlink, link, but not uplink.
?	Matches any one occurrence of the pattern. For example, ?est matches best, nest, rest, test, and so on.
\$	Matches the end of an input string. For example, eth\$ matches Eth, but not Ethernet.
*	Matches the declared element multiple times if it exists. For example, eth* matches all occurrences of eth, such as Eth, Ethernet, Eth0, and so on.
+	Matches the declared element one or more times. For example, aa+ matches occurrences of aa and

Operator	Description
	aaa.
()	Matches nested characters. For example, (192)* matches any number of the character string 192.
	Matches the character patterns on either side of the vertical bar. You can use this expression to construct a series of options.
\<	Matches the beginning of the word. For example, \<wire matches wired, wireless, and so on.
\>	Matches the end of the word. For example, \>list matches blacklist, whitelist, and so on.
{n}	Where n is an integer. Matches the declared element exactly n times. For example, {2}link matches uplink, but not downlink.
{n,}	Where n is an integer. Matches the declared element at n times. For example, {2,}ink matches downlink, but not uplink.

For information on how to use regular expressions in role and VLAN derivation rules, see the following topics:

- [Creating a Role Derivation Rule on page 201](#)
- [Configuring VLAN Derivation Rules on page 204](#)

Configuring a User Role for VLAN Derivation

This section describes the following procedures:

- [Creating a User VLAN Role on page 207](#)
- [Assigning User VLAN Roles to a Network Profile on page 208](#)

Creating a User VLAN Role

You can create a user role for VLAN derivation using the AOS-W Instant UI or the CLI.

In the AOS-W Instant UI

To configure a user role for VLAN derivation:

1. Click the **Security** link located directly above the Search bar in the AOS-W Instant main window.
2. Click the **Roles** tab. The Roles tab contents are displayed.
3. Under **Roles**, click **New**.
4. Enter a name for the new role and click **OK**.
5. Under **Access rules**, click **New**.
6. Select the **Rule type** as **VLAN assignment**.
7. Enter the ID of the VLAN in the **VLAN ID** text box.
8. Click **OK**.

In the CLI

To create a VLAN role:

```
(Instant AP) (config)# wlan access-rule <rule-name>
(Instant AP) (Access Rule <rule-name>)# vlan 200
(Instant AP) (Access Rule <rule-name>)# end
(Instant AP)# commit apply
```

Assigning User VLAN Roles to a Network Profile

You can configure user VLAN roles for a network profile using AOS-W Instant UI or the CLI.

In the AOS-W Instant UI

To assign a user VLAN role:

1. Click **Network > New > New WLAN > Access** or click **Network > edit > Edit <WLAN-profile> > Access**.
2. On the **Access** tab, ensure that the slider is at the **Role-based** option.
3. Click **New** under the **New Role Assignment** and configure the following parameters:
 - a. Select the attribute from the **Attribute** drop-down list.
 - b. Select the operator to match attribute from the **Operator** drop-down list.
 - c. Enter the string to match in the **String** text box.
 - d. Select the role to be assigned from the **Role** text box.
4. Click **OK**.

In the CLI

To assign VLAN role to a WLAN profile:

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


This chapter provides the following information:

- [Configuring DHCP Scopes on page 209](#)
- [Configuring the Default DHCP Scope for Client IP Assignment on page 216](#)

Configuring DHCP Scopes

The VC supports different modes of Dynamic Host Configuration Protocol (DHCP) address assignment. With each DHCP address assignment mode, various client traffic forwarding modes are associated. For more information on client traffic forwarding modes for IAP-VPN, see [IAP-VPN Forwarding Modes on page 241](#).

When using a local DHCP scope in an OAW-IAP cluster, ensure that the VLANs configured for this DHCP scope is allowed in the uplink switch.



In a single OAW-IAP network, when using a client DHCP scope for wired clients, ensure that client VLAN is not added in the allowed VLAN list for the port to which the OAW-IAP E0 port is connected.

This section describes the following procedures:

- [Configuring Local DHCP Scopes on page 209](#)
- [Configuring Distributed DHCP Scopes on page 211](#)
- [Configuring Centralized DHCP Scopes on page 214](#)

Configuring Local DHCP Scopes

You can configure Local; Local, L2; and Local, L3 DHCP scopes through the AOS-W Instant UI or the CLI.

- **Local**—In this mode, the VC acts as both the DHCP server and the default gateway. The configured subnet and the corresponding DHCP scope are independent of the subnets configured in other OAW-IAP clusters. The VC assigns an IP address from a local subnet and forwards traffic to both **corporate** and **non-corporate** destinations. The network address is translated appropriately and the packet is forwarded through the IPsec tunnel or through the uplink. This DHCP assignment mode is used in the Networks Address Translation (NAT) forwarding mode.
- **Local, L2**—In this mode, the VC acts as a DHCP server and the gateway located outside the OAW-IAP.
- **Local, L3**—This DHCP assignment mode is used with the L3 forwarding mode. In this mode, the VC acts as a DHCP server and the gateway, and assigns an IP address from the local subnet. The OAW-IAP routes the packets sent by clients on its uplink. The Local, L3 subnets can access corporate network through the IPsec tunnel. The network address for all client traffic, which is generated in the Local, L3 subnets and destined to the corporate network, is translated at the source with the tunnel inner IP. However, if corporate access to Local, L3 is not required, you can configure ACL rules to deny access.

In the AOS-W Instant UI

To configure a Local or a Local, L3 DHCP scope:

1. Click **More > DHCP Server**. The **DHCP Server** window is displayed.
2. To configure a **Local**; **Local, L2**; or **Local, L3** DHCP scopes, click **New** under **Local DHCP Scopes**. The **New DHCP Scope** window is displayed.
3. Based on the type of DHCP scope selected, configure the following parameters:

Table 43: Local DHCP Mode Configuration Parameters

Parameter	Description
Name	Enter a name for the DHCP scope.
Type	Select any of the following options: <ul style="list-style-type: none"> • Local—On selecting Local, the DHCP server for local branch network is used for keeping the scope of the subnet local to the OAW-IAP. In the NAT mode, the traffic is forwarded through the IPsec tunnel or the uplink. • Local, L2—On selecting Local, L2, the VC acts as a DHCP server and a default gateway in the local network that is used. • Local, L3—On selecting Local, L3, the VC acts as a DHCP server and a gateway. In this mode, the network address for traffic destined to the corporate network is translated at the source with the inner IP of the IPsec tunnel and is forwarded through the IPsec tunnel. The traffic destined to the non-corporate network is routed.
VLAN	Specify a VLAN ID. To use this subnet, ensure that the VLAN ID specified here is assigned to an SSID profile. For more information on SSID profile configuration, see Configuring VLAN Settings for a WLAN SSID Profile on page 85 and Configuring VLAN for a Wired Profile on page 107 .
Network	Specify the network to use.
Netmask	If Local ; Local, L2 ; or Local, L3 is selected, specify the subnet mask. The subnet mask and the network determine the size of the subnet.
Excluded address	Specify a range of IP addresses to exclude. You can add up to two exclusion ranges. Based on the size of the subnet and the value configured for Excluded address , the IP addresses either before or after the defined range are excluded.
Default Router	If Local, L2 is selected for type of DHCP scope, specify the IP address of the default router.
DNS Server	If required, specify the IP address of a DNS server for the Local ; Local, L2 ; and Local, L3 scopes.
Domain Name	If required, specify the domain name for the Local ; Local, L2 ; and Local, L3 scopes.
Lease Time	Specify a lease time for the client in minutes within a range of 2-1440 minutes. The default value is 720 minutes.
Option	Specify the type and a value for the DHCP option. You can configure the organization-specific DHCP options supported by the DHCP server. For example, 176, 242, and 161. To add multiple DHCP options, click the + icon.

4. Click **OK**.

In the CLI

To configure a Local DHCP scope:

```
(Instant AP) (config)# ip dhcp <profile-name>
(Instant AP) (DHCP Profile <profile-name>)# server-type <local>
(Instant AP) (DHCP Profile <profile-name>)# server-vlan <vlan-ID>
```

```
(Instant AP) (DHCP Profile <profile-name>)# subnet <IP-address>
(Instant AP) (DHCP Profile <profile-name>)# subnet-mask <subnet-mask>
(Instant AP) (DHCP Profile <profile-name>)# dns-server <name>
(Instant AP) (DHCP Profile <profile-name>)# domain-name <domain-name>
(Instant AP) (DHCP Profile <profile-name>)# lease-time <seconds>
(Instant AP) (DHCP Profile <profile-name>)# option <type> <value>
(Instant AP) (DHCP Profile <profile-name>)# end
(Instant AP)# commit apply
```

To configure a Local, L2 DHCP scope:

```
(Instant AP) (config)# ip dhcp <profile-name>
(Instant AP) (DHCP Profile <profile-name>)# server-type <local,l2>
(Instant AP) (DHCP Profile <profile-name>)# server-vlan <vlan-ID>
(Instant AP) (DHCP Profile <profile-name>)# subnet <IP-address>
(Instant AP) (DHCP Profile <profile-name>)# subnet-mask <subnet-mask>
(Instant AP) (DHCP Profile <profile-name>)# exclude-address <IP-address>
(Instant AP) (DHCP Profile <profile-name>)# default-router
(Instant AP) (DHCP Profile <profile-name>)# dns-server <name>
(Instant AP) (DHCP Profile <profile-name>)# domain-name <domain-name>
(Instant AP) (DHCP Profile <profile-name>)# lease-time <seconds>
(Instant AP) (DHCP Profile <profile-name>)# option <type> <value>
(Instant AP) (DHCP Profile <profile-name>)# end
(Instant AP)# commit apply
```

To configure a Local, L3 DHCP scope:

```
(Instant AP) (config)# ip dhcp <profile-name>
(Instant AP) (DHCP Profile <profile-name>)# server-type <local,l3>
(Instant AP) (DHCP Profile <profile-name>)# server-vlan <vlan-ID>
(Instant AP) (DHCP Profile <profile-name>)# subnet <IP-address>
(Instant AP) (DHCP Profile <profile-name>)# subnet-mask <subnet-mask>
(Instant AP) (DHCP Profile <profile-name>)# exclude-address <IP-address>
(Instant AP) (DHCP Profile <profile-name>)# dns-server <name>
(Instant AP) (DHCP Profile <profile-name>)# domain-name <domain-name>
(Instant AP) (DHCP Profile <profile-name>)# lease-time <seconds>
(Instant AP) (DHCP Profile <profile-name>)# option <type> <value>
(Instant AP) (DHCP Profile <profile-name>)# end
(Instant AP)# commit apply
```

Configuring Distributed DHCP Scopes

AOS-W Instant allows you to configure the DHCP address assignment for the branches connected to the corporate network through Virtual Private Network (VPN). You can configure the range of DHCP IP addresses used in the branches and the number of client addresses allowed per branch. You can also specify the IP addresses that must be excluded from those assigned to clients, so that they are assigned statically.

AOS-W Instant supports the following distributed DHCP scopes:

- **Distributed, L2**—In this mode, the VC acts as the DHCP server, but the default gateway is in the data center. Based on the number of clients specified for each branch, the range of IP addresses is divided. Based on the IP address range and client count configuration, the DHCP server in the VC controls a scope that is a subset of the complete IP address range for the subnet distributed across all the branches. This DHCP assignment mode is used with the L2 forwarding mode.
- **Distributed, L3**—In this mode, the VC acts as the DHCP server and the default gateway. Based on the number of clients specified for each branch, the range of IP addresses is divided. Based on the IP address range and client count configuration, the DHCP server in the VC is configured with a unique subnet and a corresponding scope.

You can configure distributed DHCP scopes such as Distributed, L2 or Distributed, L3 by using the AOS-W Instant UI or the CLI.

In the AOS-W Instant UI

To configure distributed DHCP scopes such as Distributed, L2 or Distributed, L3:

1. Click **More > DHCP Server**. The **DHCP Server** window is displayed.
2. To configure a distributed DHCP mode, click **New** under **Distributed DHCP Scopes**. The **New DHCP Scope** window is displayed. The following figure shows the contents of the **New DHCP Scope** window.

Figure 49 *New DHCP Scope: Distributed DHCP Mode*

3. Based on the type of distributed DHCP scope, configure the following parameters:

Table 44: *Distributed DHCP Mode Configuration Parameters*

Parameter	Description
Name	Enter a name for the DHCP scope.
Type	Select any of the following options: <ul style="list-style-type: none"> ● Distributed, L2—On selecting Distributed, L2, the VC acts as the DHCP server but the default gateway is in the data center. Traffic is bridged into VPN tunnel. ● Distributed, L3—On selecting Distributed, L3, the VC acts as both DHCP server and default gateway. Traffic is routed into the VPN tunnel.
VLAN	Specify a VLAN ID. To use this subnet, ensure that the VLAN ID specified here is assigned to an SSID profile. For more information on SSID profile configuration, see Configuring VLAN Settings for a WLAN SSID Profile on page 85 and Configuring VLAN for a Wired Profile on page 107 .
Netmask	If Distributed, L2 is selected for the type of DHCP scope, specify the subnet mask. The subnet mask and the network determine the size of subnet.

Table 44: Distributed DHCP Mode Configuration Parameters

Parameter	Description
Default router	If Distributed, L2 is selected for the type of DHCP scope, specify the IP address of the default router.
DNS server	If required, specify the IP address of a DNS server.
Domain name	If required, specify the domain name.
Lease time	Specify a lease time for the client in minutes within a range of 2–1440 minutes. The default value is 720 minutes.
Dynamic DNS	Select the Dynamic DNS check box to enable dynamic DNS on the Distributed, L3 client. Key —Enter the TSIG shared secret key.
IP Address Range	Specify a range of IP addresses to use. To add another range, click the + icon. You can specify up to four different ranges of IP addresses. <ul style="list-style-type: none">For the Distributed, L2 mode, ensure that all IP ranges are in the same subnet as the default router. On specifying the IP address ranges, a subnet validation is performed to ensure that the specified ranges of IP address are in the same subnet as the default router and subnet mask. The configured IP range is divided into blocks based on the configured client count.For the Distributed, L3 mode, you can configure any discontinuous IP ranges. The configured IP range is divided into multiple IP subnets that are sufficient to accommodate the configured client count. NOTE: You can allocate multiple branch IDs (BID) per subnet. The OAW-IAP generates a subnet name from the DHCP IP configuration, which the switch can use as a subnet identifier. If static subnets are configured in each branch, all of them are assigned the with BID 0, which is mapped directly to the configured static subnet.
Option	Specify the type and a value for the DHCP option. You can configure the organization-specific DHCP options supported by the DHCP server. For example, 176, 242, 161, and so on. To add multiple DHCP options, click the + icon. You can add up to eight DHCP options.

4. Click **Next**.
5. Specify the number of clients to use per branch. The client count configured for a branch determines the use of IP addresses from the IP address range defined for a DHCP scope. For example, if 20 IP addresses are available in an IP address range configured for a DHCP scope and a client count of 9 is configured, only a few IP addresses (in this example, 9) from this range will be used and allocated to a branch. The OAW-IAP does not allow the administrators to assign the remaining IP addresses to another branch, although a lower value is configured for the client count.
6. Click **Next**. The **Static IP** tab is displayed.
7. Specify the number of first and last IP addresses to reserve in the subnet.
8. Click **Finish**.

In the CLI

To configure a Distributed, L2 DHCP scope:

```
(Instant AP) (config)# ip dhcp <profile-name>
(Instant AP) (DHCP Profile <profile-name>)# ip dhcp server-type <Distributed,L2>
(Instant AP) (DHCP Profile <profile-name>)# server-vlan <vlan-ID>
(Instant AP) (DHCP Profile <profile-name>)# subnet-mask <subnet-mask>
(Instant AP) (DHCP Profile <profile-name>)# default-router <IP-address>
(Instant AP) (DHCP Profile <profile-name>)# client-count <number>
(Instant AP) (DHCP Profile <profile-name>)# dns-server <name>
(Instant AP) (DHCP Profile <profile-name>)# domain-name <domain-name>
(Instant AP) (DHCP Profile <profile-name>)# lease-time <seconds>
(Instant AP) (DHCP Profile <profile-name>)# ip-range <start-IP> <end-IP>
(Instant AP) (DHCP Profile <profile-name>)# reserve {first|last} <count>
(Instant AP) (DHCP Profile <profile-name>)# option <type> <value>
(Instant AP) (DHCP Profile <profile-name>)# end
(Instant AP)# commit apply
```

To configure a Distributed, L3 DHCP scope:

```
(Instant AP) (config)# ip dhcp <profile-name>
(Instant AP) (DHCP Profile <profile-name>)# ip dhcp server-type <Distributed,L3>
(Instant AP) (DHCP Profile <profile-name>)# server-vlan <vlan-ID>
(Instant AP) (DHCP Profile <profile-name>)# client-count <number>
(Instant AP) (DHCP Profile <profile-name>)# dns-server <name>
(Instant AP) (DHCP Profile <profile-name>)# domain-name <domain-name>
(Instant AP) (DHCP Profile <profile-name>)# lease-time <seconds>
(Instant AP) (DHCP Profile <profile-name>)# dynamic-dns [key <TSIG KEY>]
(Instant AP) (DHCP Profile <profile-name>)# ip-range <start-IP> <end-IP>
(Instant AP) (DHCP Profile <profile-name>)# reserve {first|last} <count>
(Instant AP) (DHCP Profile <profile-name>)# option <type> <value>
(Instant AP) (DHCP Profile <profile-name>)# end
(Instant AP)# commit apply
```

Configuring Centralized DHCP Scopes

When a centralized DHCP scope is configured, the following points are to be noted:

- The VC does not assign an IP address to the client and the DHCP traffic is directly forwarded to the DHCP server.
- For Centralized, L2 clients, the VC bridges the DHCP traffic to the switch over the VPN/GRE tunnel. The IP address is obtained from the DHCP server behind the switch serving the VLAN/GRE of the client. This DHCP assignment mode also allows you to add the DHCP option 82 to the DHCP traffic forwarded to the switch.
- For Centralized, L3 clients, the VC acts as a DHCP relay agent that forwards the DHCP traffic to the DHCP server located either in the corporate or local network. The Centralized, L3 VLAN IP is used as the source IP. The IP address is obtained from the DHCP server.

You can configure a centralized DHCP scope through the AOS-W Instant UI or the CLI.

In the AOS-W Instant UI

To configure a centralized DHCP scope:

1. Click **More > DHCP Server**. The **DHCP Server** window is displayed.
2. To configure a centralized DHCP scope, click **New** under **Centralized DHCP Scopes**. The **New DHCP Scope** window is displayed.
3. To configure a centralized profile, select the profile type as **Centralized, L2** or **Centralized, L3** and configure the following parameters.

Table 45: Centralized DHCP Mode Configuration Parameters

Parameter	Description
Name	Enter a name for the DHCP scope.
Type	Set the type as follows: <ul style="list-style-type: none"> ● Centralized, L2 for the Centralized, L2 profile ● Centralized, L3 for the Centralized, L3 profile
VLAN	Specify a VLAN ID. To use this subnet, ensure that the VLAN ID specified here is assigned to an SSID profile. For more information on SSID profile configuration, see Configuring VLAN Settings for a WLAN SSID Profile on page 85 and Configuring VLAN for a Wired Profile on page 107 .
Split tunnel	Set this to Enabled or Disabled for split tunnel functionality for the Centralized, L2 subnet. Enabling split tunnel allows a VPN user to access a public network and a local LAN or WAN network at the same time through the same physical network connection. For example, a user can use a remote access VPN software client connecting to a corporate network using a home wireless network. The user with split tunneling enabled is able to connect to file servers, database servers, mail servers, and other servers on the corporate network through the VPN connection. When the user connects to Internet resources (websites, FTP sites, and so on), the connection request goes directly to the gateway provided by the home network. The split-DNS functionality intercepts DNS requests from clients for non-corporate domains (as configured in Enterprise Domains list) and forwards to the OAW-IAP's own DNS server. When split-tunnel is disabled, all the traffic including the corporate and Internet traffic is tunneled irrespective of the routing profile specifications. If the GRE tunnel is down and when the corporate network is not reachable, the client traffic is dropped.
DHCP relay	If you are configuring a Centralized, L2 DHCP profile, you can select Enabled to allow the OAW-IAPs to intercept the broadcast packets and relay DHCP requests to the centralized DHCP server. NOTE: The DHCP relay option is not available for Centralized, L3 profile configuration.
Helper address	Specify the IP address of the DHCP server. NOTE: For Centralized, L2 DHCP profiles, the Helper address option is displayed only when DHCP relay is enabled.
VLAN IP	Specify the Centralized, L3 DHCP subnet gateway IP.
VLAN Mask	Specify the subnet mask of the Centralized, L3 DHCP subnet gateway IP.
Option82	Select Alcatel to enable DHCP Option 82 and allow clients to send DHCP packets with the Option 82 string. The Option 82 string is available only in the Alcatel (ALU) format. The ALU format for the Option 82 string consists of the following: <ul style="list-style-type: none"> ● Remote Circuit ID; X AP-MAC; SSID; SSID-Type ● Remote Agent; X IDUE-MAC NOTE: The Option 82 string is specific to Alcatel and is not configurable.

4. Click **OK**.

The following table describes the behavior of the DHCP Relay Agent and Option 82 in the OAW-IAP.

Table 46: DHCP Relay and Option 82

DHCP Relay	Option 82	Result
Enabled	Enabled	DHCP packet relayed with the ALU-specific Option 82 string
Enabled	Disabled	DHCP packet relayed without the ALU-specific Option 82 string
Disabled	Enabled	DHCP packet not relayed, but broadcast with the ALU-specific Option 82 string
Disabled	Disabled	DHCP packet not relayed, but broadcast without the ALU-specific Option 82 string

In the CLI

To configure a Centralized, L2 DHCP profile:

```
(Instant AP) (config)# ip dhcp <profile-name>
(Instant AP) (DHCP Profile <profile-name>)# server-type <centralized>
(Instant AP) (DHCP Profile <profile-name>)# server-vlan <vlan-ID>
(Instant AP) (DHCP Profile <profile-name>)# option82 alu
(Instant AP) (DHCP Profile <profile-name>)# disable-split-tunnel
(Instant AP) (DHCP Profile <profile-name>)# end
(Instant AP)# commit apply
```

To configure a Centralized, L3 DHCP profile:

```
(Instant AP) (config)# ip dhcp <profile-name>
(Instant AP) (DHCP Profile <profile-name>)# server-type <centralized>
(Instant AP) (DHCP Profile <profile-name>)# server-vlan <vlan-ID>
(Instant AP) (DHCP Profile <profile-name>)# dhcp-relay
(Instant AP) (DHCP Profile <profile-name>)# dhcp-server <DHCP-relay-server>
(Instant AP) (DHCP Profile <profile-name>)# vlan-ip <DHCP IP address> mask <VLAN mask>
(Instant AP) (DHCP Profile <profile-name>)# end
(Instant AP)# commit apply
```

Configuring the Default DHCP Scope for Client IP Assignment

The DHCP server is a built-in server, used for networks in which clients are assigned IP address by the VC. You can customize the DHCP pool subnet and address range to provide simultaneous access to more number of clients. The largest address pool supported is 2048. The default size of the IP address pool is 512.

When a DHCP server is configured and if the **Client IP assignment** parameter for an SSID profile is set to **Virtual Controller Assigned**, the VC assigns the IP addresses to the WLAN or the wired clients. By default, the OAW-IAP automatically determines a suitable DHCP pool for **Virtual Controller Assigned** networks. OAW-IAPs typically select the 172.31.98.0/23 subnet. If the IP address of the OAW-IAP is within the 172.31.98.0/23 subnet, the OAW-IAP selects the 10.254.98.0/23 subnet. However, this mechanism does not guarantee that it would avoid all possible conflicts with the wired network. If your wired network uses either 172.31.98.0/23 or 10.254.98.0/23, and you experience problems with the **Virtual Controller Assigned** networks after upgrading to AOS-W Instant 6.2.1.0-3.4.0.0 or later, manually configure the DHCP pool by following the steps described in this section.



You can configure a domain name, DNS server, and DHCP server for client IP assignment using the AOS-W Instant UI or the CLI.

In the AOS-W Instant UI

To configure a DHCP pool:

1. Navigate to **More > DHCP Server**. The **DHCP Server** tab contents are displayed.

Figure 50 *DHCP Servers Window*

The screenshot shows the 'DHCP Servers' configuration window. At the top, it says 'Virtual Controller Assigned Networks - Default DHCP Scope'. Below this are several input fields: 'Domain name:', 'DNS Server(s):', 'Network:', and 'Mask:'. There is also a 'Lease time:' field with a dropdown menu currently set to 'Minutes'. Below these fields are three sections for 'Distributed DHCP Scopes', 'Centralized DHCP Scopes', and 'Local DHCP Scopes'. Each section contains a table with columns for 'Name', 'Type', 'VLAN', and 'Branch Subnet' (for Distributed), or 'Name', 'Type', and 'VLAN' (for Centralized and Local). Each table has 'New', 'Edit', and 'Delete' buttons below it. At the bottom right of the window are 'OK' and 'Cancel' buttons.

2. Enter the domain name of the client in the **Domain name** text box.
3. Enter the IP addresses of the DNS servers separated by a comma (,) in the **DNS server(s)** text box.
4. Enter the duration of the DHCP lease in the **Lease time** text box. Select any of the following values from the drop-down list next to **Lease time**:
 - **Minutes**—For minutes, specify a value between 2 and 59.
 - **Hours**—For hours, specify a value between 1 and 23.
 - **Days**—For days, specify a value between 1 and 30.The default lease time is 0.
5. Enter the network range for the client IP addresses in the **Network** text box. The system generates a network range automatically that is sufficient for 254 addresses. If you want to provide simultaneous access to more number of clients, specify a larger range.
6. Specify the subnet mask details for the network range in the **Mask** text box.
7. Click **OK** to apply the changes.

In the CLI

To configure a DHCP pool:

```
(Instant AP) (config)# ip dhcp pool
(Instant AP) (DHCP)# domain-name <domain>
(Instant AP) (DHCP)# dns-server <DNS-IP-address>
(Instant AP) (DHCP)# lease-time <minutes>
(Instant AP) (DHCP)# subnet <IP-address>
(Instant AP) (DHCP)# subnet-mask <subnet-mask>
(Instant AP) (DHCP)# end
(Instant AP)# commit apply
```

To view the DHCP database:

```
(Instant AP)# show ip dhcp database
```

```
DHCP Subnet          :192.0.2.0
```

```
DHCP Netmask      :255.255.255.0
DHCP Lease Time (m) :20
DHCP Domain Name  :example.com
DHCP DNS Server   :192.0.2.1
```

This chapter describes time range profiles and the procedure for configuring time-based services. It includes the following topics:

- [Time Range Profiles on page 219](#)
- [Configuring a Time Range Profile on page 219](#)
- [Applying a Time Range Profile to a WLAN SSID on page 220](#)
- [Verifying the Configuration on page 221](#)

Time Range Profiles

Starting from AOS-W Instant 6.4.3.4-4.2.1.0, OAW-IAPs allow you to enable or disable an SSID for users at a particular time of the day. You can now create a time range profile and assign it to a WLAN SSID, so that user access to the Internet or network is restricted during a specific time period.

OAW-IAPs support the configuration of both absolute and periodic time range profiles. You can configure an absolute time range profile to execute during a specific timeframe or create a periodic profile to execute at regular intervals based on the periodicity specified in the configuration.

The following configuration conditions apply to the time-based services:

- Time-based services require an active NTP server connection. OAW-IAPs use the default NTP server for time synchronization. However, the administrators can also configure an NTP server on the OAW-IAP. To verify the time synchronization between the NTP server and the OAW-IAP, execute the **show time-range** command and check if the time on the NTP server is in synchronization with the local time. For more information on NTP server configuration, see [NTP Server](#).
- For a time range profile configured to **enable** the SSID on the OAW-IAP:
 - When the timer starts, if the current time is greater than the start time and lesser than the end time, the SSID will be brought UP. If the SSID is already UP, then there is no effect on the SSID.
 - When the timer ends, if the current time is greater than the end time, the SSID is brought DOWN. If the SSID is already DOWN, then there is no effect on the SSID.
- For a time range profile configured to **disable** the SSID on the OAW-IAP:
 - When the timer starts, if the current time is greater than the start time and lesser than the end time, the SSID will be brought DOWN. If the SSID is already DOWN, then there is no effect on the SSID.
 - When the timer ends, if the current time is greater than the end time, the SSID is brought UP. If the SSID is already UP, then there is no effect on the SSID.

Configuring a Time Range Profile

You can create time range profiles using the AOS-W Instant UI or the CLI.

In the AOS-W Instant UI

To create a time range profile:

1. Navigate to **System > Show advanced options > Time Based Services**.
2. Click **New** under **Time Range Profiles**. The **New Profile** window for creating time range profiles is displayed.
3. Configure the parameters listed in the following table:

Table 47: Time Range Profile Configuration Parameters

Parameter	Description
Name	Specify a name for the time range profile.
Type	Select the type of time range profile. Periodic —When configured, the state of the OAW-IAP changes based on the time range configured in the profile. Absolute —When configured, the state of the OAW-IAP changes during a specific date / day and time.
Period Type	For periodic time range profiles, specify a periodic interval (day/weekday/weekend/daily) at which the time range profile must be applied.
Start Day and End Day	For absolute time range profiles, specify the start day and the end day to configure a specific time period during which the time range profile is applied. NOTE: The year selected for Start Day and End Day cannot exceed the year 2037.
Start Time	Select the start time for the time range profile in the hh:mm format.
End Time	Select the end time for the time range profile in hh:mm format.

4. Click **OK**.

In the CLI:

To create an absolute time range profile:

```
(Instant AP) (config)# time-range <name> absolute start <startday> <starttime> end <endday>
<endtime>
(Instant AP) (config)# end
(Instant AP)# commit apply
```

To configure a periodic time range profile:

```
(Instant AP) (config)# time-range <name> periodic {<startday>|daily|weekday|weekend}
<starttime> to <endtime>
(Instant AP) (config)# end
(Instant AP)# commit apply
```

Applying a Time Range Profile to a WLAN SSID

To apply a time range profile to a WLAN SSID using the AOS-W Instant UI:

- Navigate to the WLAN SSID profile configuration wizard
 - Click **Network > New** or
 - Select an existing WLAN SSID and click **edit**.
- Click **Show advanced options**.
- Click **Edit**, select a time range profile from the list, then select a value from the **Status** drop-down list, and then click **OK**.
 - When a time range profile is enabled on an SSID, the SSID is made available to the users for the configured time range. For example, if the specified time range is 12:00–13:00, the SSID becomes available only between 12 PM and 1 PM on a given day.

- If a time range is disabled, the SSID becomes unavailable for the configured time range. For example, if the configured time range is 14:00–17:00, the SSID is made unavailable from 2 PM to 5 PM on a given day.

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



If the SSID has two time range profiles enabled with an overlapping duration, the time range profile will be executed as per the configuration conditions described earlier in this chapter. For example, if profile1 has 9AM-12PM as the duration and profile2 has 10AM-11AM as the duration and both are enabled on the SSID, the SSID becomes available only in the time range 9AM-11AM.

In the CLI

To enable a time range profile on an SSID:

```
(Instant AP) (config)# wlan ssid-profile <name>
(Instant AP) (SSID Profile "<name>")# time-range <name> enable
(Instant AP) (SSID Profile "<name>")# end
(Instant AP)# commit apply
```

To disable a time range profile on an SSID:

```
(Instant AP) (config)# wlan ssid-profile <name>
(Instant AP) (SSID Profile "<name>")# time-range <name> disable
(Instant AP) (SSID Profile "<name>")# end
(Instant AP)# commit apply
```

Verifying the Configuration

To view the time range profiles created on an OAW-IAP:

```
(Instant AP) # show time-range
Time Range Summary
-----
Profile Name  Type      Start Day  Start Time  End Day    End Time   Valid
-----
test          Periodic  daily      13:00       -          14:00     No
test1         Absolute  11/17/2015 10:00       11/24/2015 17:00     No
Lunchbreak    Periodic  weekday    12:00       -          13:00     No
Lunchbreak1   Periodic  daily      12:00       -          13:00     No
```

To verify if the time range profile is enabled on an SSID:

```
(Instant AP)# show time-profile
Time Range SSID Profile
-----
Time Profile Name  SSID profile Name  Enable/Disable
-----
Lunch Break        Test123             Enable
```

Example

The following command creates an absolute time range profile :

```
(Instant AP) (config)# time-range timep1 absolute start 10/20/2013 10:40 end 10/20/2015 10:50
```

The following command creates a periodic time range profile that executes on the specified day of the week:

```
(Instant AP) (config)# time-range timep2 periodic monday 10:40 to tuesday 10:50
```

The following command creates a periodic time range profile that executes daily:

```
(Instant AP) (config)# time-range testshs12 periodic daily 10:20 to 10:35
```

The following command creates a periodic time range profile that executes during the weekday:

```
(Instant AP) (config)# time-range timep3 periodic weekday 10:20 to 10:35
```

The following command creates a periodic time range profile that executes during the weekend:

```
(Instant AP) (config)# time-range timep4 periodic weekend 10:20 to 10:30
```

The following command removes the time range configuration:

```
(Instant AP) (config)# no time-range testshs12
```

This chapter describes the procedure for configuring Dynamic DNS (DDNS) on OAW-IAPs and their clients. It includes the following topics:

- [Enabling Dynamic DNS on page 223](#)
- [Configuring Dynamic DNS Updates for Clients on page 224](#)
- [Verifying the Configuration on page 225](#)

Enabling Dynamic DNS

Starting from AOS-W Instant 6.4.4.4-2.3.0, OAW-IAPs support the dynamic DNS feature which enables updating the DNS records of the OAW-IAP and the clients connected to it. In a scenario where the public IP address is dynamically handed to the OAW-IAP by the ISP, there are instances when the client loses remote connectivity to the OAW-IAP when there is a change in the IP address. Similarly, in case of OAW-IAP clients, where the OAW-IAP acts as a DHCP server, the host becomes unreachable when the dynamically assigned IP address is changed. The dynamic DNS feature eliminates these issues by configuring a domain name, thus providing a uniform approach to access the OAW-IAP or the clients. The IP address of the dynamic DNS client is mapped to the domain name and this gets automatically updated each time the IP address is changed.

You can enable Dynamic DNS using the AOS-W Instant UI or the CLI.

In the AOS-W Instant UI

To enable dynamic DNS:

1. Navigate to **Services > Dynamic DNS**.
2. Select the **Enable Dynamic DNS** check box.

Table 48: Dynamic DNS Configuration Parameters

Parameter	Description	Example
Key	Configures a Transaction Signature (TSIG) shared secret key to secure the dynamic updates. The following algorithm names are supported: <ul style="list-style-type: none"> • hmac-md5 (used by default if algo-name is not specified) • hmac-sha1 • hmac-sha256 NOTE: When a key is configured, the update is successful only if OAW-IAP and DNS server clocks are in sync.	hmac-sha1:arubaddns: 16YuLPdH21rQ6PuK9udsVLtJw3Y=
Server IP	Enter the server IP address of the DNS server to which the client updates are sent.	10.17.132.85
Interval	Specify the time interval (in secs) at which the DNS updates are to be synced to the server. The default time interval is 12 hours, minimum time interval is 15 minutes, and maximum time interval is 100 days.	900

3. Click **OK**.

In the CLI:

To enable dynamic DNS on an OAW-IAP

```
(Instant AP) (config)# dynamic-dns-ap
(Instant AP) (config)# end
(Instant AP) # commit apply
```

To configure a TSIG key and server IP address:

```
(Instant AP) (config)# dynamic-dns-ap key <algo-name:keyname:keystring>
(Instant AP) (config)# dynamic-dns-ap server <ddns_server>
(Instant AP) (config)# end
(Instant AP) # commit apply
```

To configure a time interval:

```
(Instant AP) (config)# dynamic-dns-interval <ddns_interval>
(Instant AP) (config)# end
(Instant AP) # commit apply
```

Configuring Dynamic DNS Updates for Clients

You can enable DDNS updates when creating or editing a DHCP scope for **Distributed, L3** clients. When enabled, the DDNS updates of the clients are periodically sent during the specified time to the DNS server that is configured in the DHCP profile. If there is no DNS server configured in the DHCP profile, the client DNS updates will be dropped. The DDNS updates are secured by using TSIG shared secret keys, when communicating between the client and the server. For more information, see [Configuring Distributed DHCP Scopes on page 211](#).

In the AOS-W Instant UI

To enable DDNS for clients:

1. Navigate to **More > DHCP Servers**, select the **Distributed, L3** DHCP Scope under **Distributed DHCP Scopes** and click **Edit**.
2. Select the **Dynamic DNS** check box.
3. Enter the TSIG shared secret **key**.
4. Click **Next** and then click **Finish**.

In the CLI

To enable DDNS for OAW-IAP clients:

```
(Instant AP) (config)# ip dhcp <profile name>
(Instant AP) (DHCP profile "<name>")# dynamic-dns
(Instant AP) (DHCP profile "<name>")# dynamic-dns key <algo-name:keyname:keystring>
(Instant AP) (DHCP Profile "<name>")# end
(Instant AP)# commit apply
```

Verifying the Configuration

To view the DDNS status on an OAW-IAP:

```
(Instant AP)# show ddns
DDNS Enabled      :Enabled
DDNS Server       :10.1.1.23
DDNS Key          :dynamic-dns delete 10.17.132.7 test.ddns host-anand 10.17.132.85 key hmac-
sha1:arubaddns:16YuLPdH21rQ6PuK9udsVltJw3Y=
DDNS Interval    :900
```

To view the list of DDNS clients:

```
(Instant AP)# show ddns clients
DDNS Client List
```

Host Name	Domain Name	IP Address	DHCP profile name	Success Count	Failure Count
iap1-ddns-home	test.ddns	192.192.192.17	None	16	22
132-13-Auto-PC	test.ddns	192.168.99.18	DistL3	9	3
132-14-Auto-PC	test.ddns	192.168.99.4	DistL3	2	0

```
Last updated      Last update status
```

```
-----
7 seconds ago    Success
7 seconds ago    Success
7 seconds ago    Success
```

DHCP profile name is None for the Master OAW-IAP update sent.

The **show running-config** command displays the **Key** in the encrypted format.

You can also configure dynamic DNS on an OAW-IAP or clients using the privileged execution mode in the CLI. For more information, refer to the **show ddns clients** command in the *AOS-W Instant 6.4.4.4-4.2.3.0 CLI Reference Guide*.



This chapter describes the following VPN configuration procedures:

- [Understanding VPN Features on page 226](#)
- [Configuring a Tunnel from an OAW-IAP to a Mobility Controller on page 227](#)
- [Configuring Routing Profiles on page 238](#)

Understanding VPN Features

As OAW-IAPs use a VC architecture, the OAW-IAP network does not require a physical switch to provide the configured WLAN services. However, a physical switch is required for terminating Virtual Private Networks (VPN) tunnels from the OAW-IAP networks at branch locations to datacenters, where the Alcatel-Lucent switch acts as a VPN concentrator.

When a VPN is configured, the OAW-IAP acting as the VC creates a VPN tunnel to an OmniAccess WLAN Switch in your corporate office. The switch acts as a VPN endpoint and does not supply the OAW-IAP with any configuration.

The VPN features are recommended for the following setups:

- Enterprises with many branches that do not have a dedicated VPN connection to the corporate office.
- Branch offices that require multiple OAW-IAPs.
- Individuals working from home and, connecting to the VPN.

The survivability feature of OAW-IAPs with the VPN connectivity of OAW-IAPs allows you to provide corporate connectivity on non-corporate networks.

Supported VPN Protocols

AOS-W Instant supports the following VPN protocols for remote access:

Table 49: *VPN Protocols*

VPN Protocol	Description
Alcatel-Lucent IPsec	<p>IPsec is a protocol suite that secures IP communications by authenticating and encrypting each IP packet of a communication session.</p> <p>You can configure an IPsec tunnel to ensure that the data flow between the networks is encrypted. However, you can configure a split-tunnel to encrypt only the corporate traffic.</p> <p>When IPsec is configured, ensure that you add the OAW-IAP MAC addresses to the whitelist database stored on the switch or an external server. IPsec supports Local, L2, and L3 modes of IAP-VPN operations.</p> <p>NOTE: The OAW-IAPs support IPsec only with Alcatel-Lucent switches.</p>
Layer-2 (L2) GRE	<p>Generic Routing Encapsulation (GRE) is a tunnel protocol for encapsulating multicast, broadcast, and L2 packets between a GRE-capable device and an endpoint. OAW-IAPs support the configuration of L2 GRE (Ethernet over GRE) tunnel with an Alcatel-Lucent switch to encapsulate the packets sent and received by the OAW-IAP.</p> <p>You can use the GRE configuration for L2 deployments when there is no encryption requirement between the OAW-IAP and switch for client traffic.</p> <p>OAW-IAPs support two types of GRE configuration:</p> <ul style="list-style-type: none">• Manual GRE—The manual GRE configuration sends unencrypted client traffic with an additional GRE header and does not support failover. When manual GRE is configured on the OAW-IAP, ensure that the GRE tunnel settings are enabled on the switch.• Aruba GRE—With Aruba GRE, no configuration on the switch is required except for adding the OAW-IAP MAC addresses to the whitelist database stored on the switch or an external server. Aruba GRE reduces manual configuration when Per-AP tunnel configuration is required and supports failover between two GRE endpoints. <p>NOTE: OAW-IAPs support manual and Aruba GRE configuration only for L2 mode of operations. Aruba GRE configuration is supported only on Alcatel-Lucent switches.</p>
L2TPv3	<p>The Layer 2 Tunneling Protocol version 3 (L2TPv3) feature allows the OAW-IAP to act as an L2TP Access Concentrator (LAC) and tunnel all wireless client's L2 traffic from the OAW-IAP to L2TP Network Server (LNS). In a Centralized, L2 model, the VLAN on the corporate side is extended to remote branch sites. Wireless clients associated with an OAW-IAP gets the IP address from the DHCP server running on LNS. For this, the OAW-IAP has to transparently allow DHCP transactions through the L2TPv3 tunnel.</p>

Configuring a Tunnel from an OAW-IAP to a Mobility Controller

OAW-IAP supports the configuration of tunneling protocols such as Generic Routing Encapsulation (GRE), IPsec, and L2TPv3. This section describes the procedure for configuring VPN host settings on an OAW-IAP to enable communication with a switch in a remote location:

- [Configuring an IPsec Tunnel on page 228](#)
- [Configuring an L2-GRE Tunnel on page 229](#)
- [Configuring an L2TPv3 Tunnel on page 232](#)

Configuring an IPsec Tunnel

An IPsec tunnel is configured to ensure that the data flow between the networks is encrypted. When configured, the IPsec tunnel to the switch secures corporate data.

You can configure an IPsec tunnel from the VC using the AOS-W Instant UI or the CLI.

In the AOS-W Instant UI

To configure a tunnel for IPsec protocol:

1. Click the **More > VPN** link in the AOS-W Instant UI. The **Tunneling** window is displayed.
2. Select **Aruba IPsec** from the **Protocol** drop-down list.
3. Enter the IP address or fully qualified domain name (FQDN) for the primary VPN/IPsec endpoint in the **Primary host** text box.
4. Enter the IP address or FQDN for the backup VPN/IPsec endpoint in the **Backup host** text box. This entry is optional. When you specify the primary and backup host details, the other details are displayed.
5. Specify the following parameters. A sample configuration is shown in [Figure 51](#).
 - a. To allow the VPN tunnel to switch back to the primary host when it becomes available again, select **Enabled** from the **Preemption** drop-down list. This step is optional.
 - b. If **Preemption** is enabled, specify a value in seconds for **Hold time**. When preemption is enabled and the primary host comes up, the VPN tunnel switches back to the primary host after the specified hold-time. The default value for **Hold time** is 600 seconds.
 - c. To allow the OAW-IAP to create a backup VPN tunnel to the switch along with the primary tunnel, and maintain both the primary and backup tunnels separately, select **Enabled** from the **Fast failover** drop-down list. When fast failover is enabled and if the primary tunnel fails, the OAW-IAP can switch the data stream to the backup tunnel. This reduces the total failover time to less than one minute.
 - d. To disconnect all wired and wireless users when the system switches during VPN tunnel transition from primary to backup and backup to primary, set **Reconnect User On Failover** to **Enabled**.
 - e. To configure an interval during which the wired and wireless users are disconnected during a VPN tunnel switch, specify a value in seconds for **Reconnect Time On Failover** within a range of 30–900 seconds. By default, the reconnection duration is set to 60 seconds.
 - f. Specify a value in seconds for **Secs between test packets**. Based on the configured frequency, the OAW-IAP can verify if an active VPN connection is available. The default value is 5 seconds, which means that the OAW-IAP sends one packet to the switch every 5 seconds.
 - g. Enter a value for **Max allowed test packet loss** to define a number for lost packets, exceeding which the OAW-IAP can determine that the VPN connection is unavailable. The default value is 2.

Figure 51 IPsec Configuration

The screenshot shows the 'Tunneling' configuration window with the 'Controller' tab active. The configuration parameters are as follows:

Parameter	Value
Protocol	Aruba IPsec
Primary host	10.0.0.1
Backup host	10.0.0.2
Preemption	Enabled
Hold time	600 sec.
Fast failover	Enabled
Reconnect User On Failover	Enabled
Reconnect Time On Failover	60 sec.
Secs between test packets	5
Max allowed test packet loss	2

- Click **Next** to create routing profiles. When the IPsec tunnel configuration is completed, the packets that are sent from and received by an OAW-IAP are encrypted.

In the CLI

To configure an IPsec VPN tunnel:

```
(Instant AP) (config)# vpn primary <name>
(Instant AP) (config)# vpn backup <name>
(Instant AP) (config)# vpn fast-failover
(Instant AP) (config)# vpn hold-time <seconds>
(Instant AP) (config)# vpn preemption
(Instant AP) (config)# vpn monitor-pkt-send-freq <frequency>
(Instant AP) (config)# vpn monitor-pkt-lost-cnt <count>
(Instant AP) (config)# vpn reconnect-user-on-failover
(Instant AP) (config)# vpn reconnect-time-on-failover <down_time>
(Instant AP) (config)# end
(Instant AP)# commit apply
```

Example

```
(Instant AP) (config)# vpn primary 192.0.2.18
(Instant AP) (config)# vpn backup 192.0.2.20
(Instant AP) (config)# vpn fast-failover
(Instant AP) (config)# vpn preemption

(Instant AP) (config)# ip dhcp distl2
(Instant AP) (DHCP Profile "distL2")# server-type Distributed,L2
(Instant AP) (DHCP Profile "distL2")# server-vlan 2
(Instant AP) (DHCP Profile "distL2")# ip-range 10.15.205.0 10.15.205.255
(Instant AP) (DHCP Profile "distL2")# subnet-mask 255.255.255.0
(Instant AP) (DHCP Profile "distL2")# lease-time 86400
(Instant AP) (DHCP Profile "distL2")# default-router 10.15.205.254
(Instant AP) (DHCP Profile "distL2")# dns-server 10.13.6.110,10.1.1.50
(Instant AP) (DHCP Profile "distL2")# domain-name alcatel-lucent.com
(Instant AP) (DHCP Profile "distL2")# client-count 5

(Instant AP) (config)# ip dhcp local
(Instant AP) (DHCP Profile "local")# server-type Local
(Instant AP) (DHCP Profile "local")# server-vlan 200
(Instant AP) (DHCP Profile "local")# subnet 172.16.200.1
(Instant AP) (DHCP Profile "local")# subnet-mask 255.255.255.0
(Instant AP) (DHCP Profile "local")# lease-time 86400
(Instant AP) (DHCP Profile "local")# dns-server 10.13.6.110,10.1.1.50
(Instant AP) (DHCP Profile "local")# domain-name alcatel-lucent.com
```

To view the VPN configuration:

```
(Instant AP)# show vpn config
```

Configuring an L2-GRE Tunnel

This section describes the following procedures:

- [Configuring Manual GRE Parameters](#)
- [Configuring Aruba GRE Parameters](#)

Configuring Manual GRE Parameters

You can configure a GRE tunnel between the OAW-IAP and the switch using either the VC IP or the OAW-IAP IP, based on the following OAW-IAP settings:

- If a VC IP is configured and if **Per-AP tunnel** is disabled, use VC IP.
- If a VC IP is not configured or if **Per-AP tunnel** is enabled, use the OAW-IAP IP.

For information on the GRE tunnel configuration on the switch, refer to the *AOS-W Instant 6.5.x.x User Guide*.

In the AOS-W Instant UI

To configure a GRE tunnel:

1. Click the **More > VPN** link located directly above the Search bar in the AOS-W Instant UI. The **Tunneling** window is displayed.
2. Select **Manual GRE** from the **Protocol** drop-down list.
3. Specify the following parameters. A sample configuration is shown in [Figure 52](#).
 - a. Enter an IP address or an FQDN for the main VPN/GRE endpoint in the **Host** text box.
 - b. Enter a value in the **GRE type** text box.
 - c. Select **Enabled** or **Disabled** from the **Per-AP tunnel** drop-down list. Enable this option to create a GRE tunnel from each OAW-IAP to the VPN/GRE endpoint rather than the tunnels created just from the master OAW-IAP. When enabled, the traffic to the corporate network is sent through a Layer-2 GRE tunnel from the OAW-IAP itself and need not be forwarded through the master OAW-IAP.



By default, the **Per-AP tunnel** option is disabled.

Figure 52 Manual GRE Configuration

The screenshot shows a web-based configuration window titled "Tunneling" with a "Help" link in the top right corner. The window has two tabs: "1 Controller" (active) and "2 Routing". Under the "Controller" tab, there are four configuration fields: "Protocol" is a dropdown menu set to "Manual GRE"; "Host" is a text input field containing "192.0.2.15"; "GRE type" is a text input field containing "1"; and "Per-AP tunnel" is a dropdown menu set to "Enabled". At the bottom right of the window, there are "Next" and "Cancel" buttons.

4. Click **Next** to continue. When the GRE tunnel configuration is completed on both the OAW-IAP and the switch, the packets sent from and received by an OAW-IAP are encapsulated, but not encrypted.

In the CLI

To configure a manual GRE VPN tunnel:

```
(Instant AP) (config)# gre primary <name>
(Instant AP) (config)# gre type <type>
(Instant AP) (config)# gre per-ap-tunnel
(Instant AP) (config)# end
(Instant AP)# commit apply
```

To view VPN configuration details:

```
(Instant AP)# show vpn config
```

To configure GRE tunnel on the switch:

```
(Instant AP) (config)# interface tunnel <Number>
(Instant AP) (config-tunnel)# description <Description>
(Instant AP) (config-tunnel)# tunnel mode gre <ID>
```

```
(Instant AP) (config-tunnel)# tunnel source <controller-IP>
(Instant AP) (config-tunnel)# tunnel destination <AP-IP>
(Instant AP) (config-tunnel)# trusted
(Instant AP) (config-tunnel)# tunnel vlan <allowed-VLAN>
```

Configuring Aruba GRE Parameters

The Aruba GRE feature uses the IPsec connection between the OAW-IAP and the switch to send the control information for setting up a GRE tunnel. When Aruba GRE configuration is enabled, a single IPsec tunnel between the OAW-IAP cluster and the switch, and one or several GRE tunnels are created based on the Per-AP tunnel configuration on the OAW-IAP. For Aruba GRE, no manual configuration is required on the switch to create the GRE tunnel.



Aruba GRE is supported only on Aruba Switches running AOS-W Instant 6.4.x.x or later versions.

In the AOS-W Instant UI

To configure Aruba GRE:

1. Click the **More > VPN** link located directly above the Search bar in the AOS-W Instant UI. The **Tunneling** window is displayed.
2. Select **Aruba GRE** from the **Protocol** drop-down list.
3. Enter the IP address or the FQDN for the main VPN/IPsec endpoint in the **Primary host** text box.
4. Enter the IP address or the FQDN for the backup VPN/IPsec endpoint in the **Backup host** text box. This entry is optional. When you enter the primary host IP address and backup host IP address, other details are displayed.
5. Specify the following parameters. A sample configuration is shown in [Figure 52](#).
 - a. To allow the VPN tunnel to switch back to the primary host when it becomes available again, select **Enabled** from the **Preemption** drop-down list. This step is optional.
 - b. If **Preemption** is enabled, specify a value in seconds for **Hold time**. When preemption is enabled and the primary host comes up, the VPN tunnel switches to the primary host after the specified hold time. The default value for **Hold time** is 600 seconds.
 - c. To allow the OAW-IAP to create a backup VPN tunnel to the switch along with the primary tunnel, and maintain both the primary and backup tunnels separately, select **Enabled** from the **Fast failover** drop-down list. If this option is enabled, when the primary tunnel fails, the OAW-IAP can switch the data stream to the backup tunnel. This reduces the total failover time to less than one minute.
 - d. To disconnect all wired and wireless users when the system switches during VPN tunnel transition from primary to backup and backup to primary, set **Reconnect user on failover** to **Enabled**.
 - e. To configure an interval for which wired and wireless users are disconnected during a VPN tunnel switch, specify a value in seconds for **Reconnect time on failover** within the range of 30–900 seconds. By default, the reconnection duration is set to 60 seconds.
 - f. Specify a value in seconds for **Secs between test packets**. Based on the configured frequency, the OAW-IAP can verify if an active VPN connection is available. The default value is 5 seconds, which means that the OAW-IAP sends one packet to the switch every 5 seconds.
 - g. Enter a value for **Max allowed test packet loss** to define a number for lost packets, exceeding which the OAW-IAP can determine that the VPN connection is unavailable. The default value is 2.
 - h. Select **Enabled** or **Disabled** from the **Per-AP tunnel** drop-down list. The administrator can enable this option to create a GRE tunnel from each OAW-IAP to the VPN/GRE endpoint rather than the tunnels created just from the master OAW-IAP. When enabled, the traffic to the corporate network is sent through a Layer-2 GRE tunnel from the OAW-IAP itself and need not be forwarded through the master OAW-IAP.

Figure 53 Aruba GRE Configuration

The screenshot shows a web-based configuration interface for Aruba GRE. The main title is 'Tunneling' with a 'Help' link. There are two tabs: '1 Controller' (highlighted in green) and '2 Routing'. The 'Controller' section is active and contains the following fields:

- Protocol: Aruba GRE (dropdown)
- Primary host: 192.0.2.2 (text input)
- Backup host: 192.0.2.4 (text input)
- Preemption: Enabled (dropdown)
- Hold time: 600 sec. (text input)
- Fast failover: Enabled (dropdown)
- Reconnect user on failover: Enabled (dropdown)
- Reconnect time on failover: 60 sec. (text input)
- Secs between test packets: 5 (text input)
- Max allowed test packet loss: 2 (text input)
- Per-AP tunnel: Enabled (dropdown)

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

6. Click **Next** to continue.

In the CLI

To enable Aruba GRE tunnel:

```
(Instant AP) (config) # vpn gre-outside
(Instant AP) (config) # vpn primary <name/IP-address>
(Instant AP) (config) # vpn backup <<name/IP-address>>
(Instant AP) (config) # vpn fast-failover
(Instant AP) (config) # vpn hold-time <seconds>
(Instant AP) (config) # vpn preemption
(Instant AP) (config) # vpn monitor-pkt-send-freq <frequency>
(Instant AP) (config) # vpn monitor-pkt-lost-cnt <count>
(Instant AP) (config) # vpn reconnect-user-on-failover
(Instant AP) (config) # vpn reconnect-time-on-failover <down_time>
(Instant AP) (config) # end
(Instant AP) # commit apply
```

To view VPN configuration details:

```
(Instant AP) # show vpn config
```

Configuring an L2TPv3 Tunnel

Some important points to note about L2TPv3 in the OAW-IAP context are as follows::

- AOS-W Instant supports tunnel and session configuration, and uses Control Message Authentication (RFC 3931) for tunnel and session establishment. Each L2TPv3 tunnel supports one data connection and this connection is termed as an L2TPv3 session.
- Each OAW-IAP supports tunneling over User Datagram Protocol (UDP) only.

- If the primary LNS is down, it fails over to the backup LNS. L2TPv3 has one tunnel profile, and under this a primary peer and a backup peer are configured. If the primary tunnel creation fails or if the primary tunnel gets deleted, the backup starts. The following two failover modes are supported:
 - Preemptive: In this mode, if the primary comes up when the backup is active, the backup tunnel is deleted and the primary tunnel resumes as an active tunnel. If you configure the tunnel to be preemptive, and when the primary tunnel goes down, it starts the persistence timer which tries to bring up the primary tunnel.
 - Non-Preemptive: In this mode, when the backup tunnel is established after the primary tunnel goes down, it does not make the primary tunnel active again.



L2TPv3 is not supported on OAW-IAP205 devices.

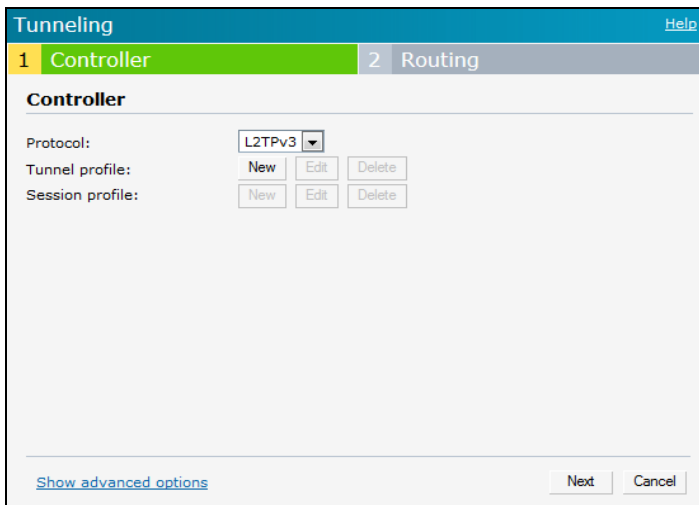
You can configure an L2TPv3 tunnel and session profiles through the AOS-W Instant UI or the CLI.

In the AOS-W Instant UI

To configure an L2TPv3 tunnel and session profile:

1. Click the **More > VPN** link located directly above the Search bar in the AOS-W Instant UI. The **Tunneling** window is displayed.

Figure 54 L2TPv3 Tunneling



2. Select **L2TPv3** from the **Protocol** drop-down list.
3. To configure the tunnel profile:
 - a. Click the **New** button.
 - b. Enter the tunnel name to be used for tunnel creation.

Figure 55 Tunnel Configuration

Tunnel Configuration

Primary Peer address: 10.0.0.63

Backup Peer address: 10.0.0.65

Peer UDP port: 3000

Local UDP port: 1701

Hello interval: 150 sec.

Message digest type: MD5

Shared key:

Checksum: Disabled

Failover mode: non-Preemptive

Failover retry interval: 80 sec.

Failover retry count: 5

MTU: 1570

OK Cancel

- c. Enter the primary server IP address in the **Primary Peer address** text box.
 - d. Enter the remote end backup tunnel IP address in the **Backup Peer address** text box. This is an optional text box entry and is required only when backup server is configured.
 - e. Enter a port number in the **Peer UDP port** text box.
 - f. Enter the remote end UDP port number in the **Local UDP port** text box. The default value is 1701.
 - g. Enter the interval at which the hello packets are sent through the tunnel in the **Hello interval** text box. The default value is 60 seconds.
 - h. Select the message digest as MD5 or SHA to be used for message authentication from the Message digest type drop-down list.
 - i. Select **Disabled** from the **Checksum** drop-down list.
 - j. Enter a shared key for the message digest in the **Shared Key** text box. This key should match with the tunnel endpoint shared key.
 - k. If required, select the failover mode as Primary or Backup (when the backup server is available).
 - l. Specify a value for the tunnel MTU value if required. The default value is 1460.
 - m. Click **OK**.
4. Configure the session profile:
- a. Enter the session name to be used for session creation.

Figure 56 Session Configuration

Session Configuration

Profile name:

Tunnel profile name: test

Tunnel IP address:

Tunnel Netmask:

Tunnel VLAN:

Cookie Len: 0

Cookie:

Remote end ID:

Default I2 specific sublayer:

OK Cancel

- b. Enter the tunnel profile name where the session will be associated.
 - c. Configure the tunnel IP address with the corresponding network mask and VLAN ID. This is required to reach an OAW-IAP from a corporate network. For example, SNMP polling.
 - d. Select the cookie length and enter a cookie value corresponding to the length. By default, the cookie length is not set.
 - e. Specify the remote end ID.
 - f. If required, enable default I2 specific sublayer in the L2TPv3 session.
 - g. Click **OK**.
5. Click **Next** to continue.

In the CLI

To configure an L2TPv3 VPN tunnel profile:

```
(Instant AP) (config)# l2tpv3 tunnel <l2tpv3_tunnel_profile>
(Instant AP) (L2TPv3 Tunnel Profile <l2tpv3_tunnel_profile>)# primary peer-address <peer_ip_
addr_tunnel>
(Instant AP) (L2TPv3 Tunnel Profile <l2tpv3_tunnel_profile>)# backup peer-address <peer_ip_
addr_tunnel>
(Instant AP) (L2TPv3 Tunnel Profile <l2tpv3_tunnel_profile>)# checksum
(Instant AP) (L2TPv3 Tunnel Profile <l2tpv3_tunnel_profile>)# failover-mode <mode>
(Instant AP) (L2TPv3 Tunnel Profile <l2tpv3_tunnel_profile>)# failover-retry-count <retry_
count>
(Instant AP) (L2TPv3 Tunnel Profile <l2tpv3_tunnel_profile>)# failover-retry-interval
<interval_in_sec>
(Instant AP) (L2TPv3 Tunnel Profile <l2tpv3_tunnel_profile>)# hello-timeout <interval_in_sec>
(Instant AP) (L2TPv3 Tunnel Profile <l2tpv3_tunnel_profile>)# local-port <local_udp_port>
(Instant AP) (L2TPv3 Tunnel Profile <l2tpv3_tunnel_profile>)# peer-port <peer_udp_port>
(Instant AP) (L2TPv3 Tunnel Profile <l2tpv3_tunnel_profile>)# message-digest-type <digest_algo>
(Instant AP) (L2TPv3 Tunnel Profile <l2tpv3_tunnel_profile>)# secret-key <key>
(Instant AP) (L2TPv3 Tunnel Profile <l2tpv3_tunnel_profile>)# mtu <tunnel_MTU>
(Instant AP) (L2TPv3 Tunnel Profile <l2tpv3_tunnel_profile>)# end
(Instant AP)# commit apply
```

To configure an L2TPv3 session profile:

```
(Instant AP) (config)# l2tpv3 session <l2tpv3_session_profile>
(Instant AP) (L2TPv3 Tunnel Profile <l2tpv3_session_profile>)# cookie len <len_of_cookie> value
<cookie_val>
(Instant AP) (L2TPv3 Tunnel Profile <l2tpv3_session_profile>)# l2tpv3 tunnel <l2tpv3_tunnel_
name_to_associate>
(Instant AP) (L2TPv3 Tunnel Profile <l2tpv3_session_profile>)# tunnel-ip <local_ip_addr_tunnel>
mask <tunnel_mask> vlan <tunnel_mgmt_vlan>
(Instant AP) (L2TPv3 Tunnel Profile <l2tpv3_session_profile>)# default-l2-specific-sublayer
(Instant AP) (L2TPv3 Tunnel Profile <l2tpv3_session_profile>)# end
(Instant AP)# commit apply
```

Example

```
(Instant AP) (config)# l2tpv3 tunnel test_tunnel
(Instant AP) (L2TPv3 Tunnel Profile "test_tunnel")# primary peer-address 10.0.0.65
(Instant AP) (L2TPv3 Tunnel Profile "test_tunnel")# backup peer-address 10.0.0.63
(Instant AP) (L2TPv3 Tunnel Profile "test_tunnel")# no checksum
(Instant AP) (L2TPv3 Tunnel Profile "test_tunnel")# failover-mode non-preemptive
(Instant AP) (L2TPv3 Tunnel Profile "test_tunnel")# failover-retry-count 5
(Instant AP) (L2TPv3 Tunnel Profile "test_tunnel")# failover-retry-interval 80
(Instant AP) (L2TPv3 Tunnel Profile "test_tunnel")# hello-timeout 150
(Instant AP) (L2TPv3 Tunnel Profile "test_tunnel")# mtu 1570
(Instant AP) (L2TPv3 Tunnel Profile "test_tunnel")# peer-port 3000
(Instant AP) (L2TPv3 Tunnel Profile "test_tunnel")# secret-key test123
(Instant AP) (L2TPv3 Tunnel Profile "test_tunnel")# end
```

```
(Instant AP)# commit apply

(Instant AP)(config) # l2tpv3 session test_session
(Instant AP)(L2TPv3 Session Profile "test_session")# cookie len 4 value 12345678
(Instant AP)(L2TPv3 Session Profile "test_session")# l2tpv3 tunnel test_tunnel
(Instant AP)(L2TPv3 Session Profile "test_session")# tunnel-ip 1.1.1.1 mask 255.255.255.0 vlan
5
(Instant AP)(L2TPv3 Tunnel Profile "test_tunnel")# end
(Instant AP)# commit apply
```

To view L2TPv3 configuration:

```
(Instant AP)# show l2tpv3 config
L2TPV3 Tunnel configuration
-----
Tunnel Profile   Primary Peer   Backup Peer   Peer UDP Port   Local UDP Port   Hello Interval
Host Name        MTU           Message Digest Type   secret Key                               Failover Mode
Failover Retry Count  Retry Interval  Checksum
-----
-----
test_tunnel      10.0.0.63     10.0.0.65     3000            1701             150
Instant-C4:42:98 1570         MD5            625beed39fa4ff3424edb3082ede48fa non-
preemptive 5           80            Disabled
L2TPV3 Session configuration
-----
Session Name     Tunnel Name   Local tunnel IP   Tunnel Mask     Tunnel Vlan     Session Cookie Length
Session Cookie   Session Remote End ID
-----
-----
test_session     0             1.1.1.1           255.255.255.0  5               0
0
```

To view L2TPv3 global configuration:

```
(Instant AP)# show l2tpv3 global parameter

L2TPV3 Global configuration
-----
Host Name
-----
Instant-C4:42:98
```

To view L2TPV3 session status:

```
(Instant AP)# show l2tpv3 session status
Session 1821009927 on tunnel 858508253:-
type: LAC Incoming Call, state: ESTABLISHED
created at: Jul 2 04:58:45 2013
administrative name: 'test_session' (primary)
created by admin: YES, peer session id: 12382
session profile name: test_session_primary
data sequencing required: OFF
use data sequence numbers: OFF
Peer configuration data:-
data sequencing required: OFF
framing types:
data rx packets: 16, rx bytes: 1560, rx errors: 0 rx cookie error 0
data tx packets: 6, tx bytes: 588, tx errors: 0
```

To view L2TPV3 tunnel status:

```
(Instant AP)# show l2tpv3 tunnel status
```

```
Tunnel 858508253, from 10.13.11.29 to 10.13.11.157:-
state: ESTABLISHED
created at: Jul 2 04:58:25 2013
administrative name: 'test_tunnel' (primary)
created by admin: YES, tunnel mode: LAC, persist: YES
local host name: Instant-C4:42:98
peer tunnel id: 1842732147, host name: aruba1600pop636635.hsbtst2.aus
UDP ports: local 1701, peer 3000
session limit: 0, session count: 1
tunnel profile: test_tunnel_primary, peer profile: default
session profile: default
hello timeout: 150, retry timeout: 80, idle timeout: 0
rx window size: 10, tx window size: 10, max retries: 5
use udp checksums: OFF
do pmtu discovery: OFF, mtu: 1460
trace flags: PROTOCOL FSM API AVPDATA FUNC XPRT DATA SYSTEM CLI
peer vendor name: Katalix Systems Ltd. Linux-2.6.32-358.2.1.el6.x86_64 (x86_64)
peer protocol version: 1.0, firmware 0
peer rx window size: 10
Transport status:-
ns/nr: 98/97, peer 98/96
cwnd: 10, ssthresh: 10, congpkt_acc: 9
Transport statistics:-
out-of-sequence control/data discards: 0/0
ACKs tx/txfail/rx: 0/0/96
retransmits: 0, duplicate pkt discards: 0, data pkt discards: 0
hellos tx/txfail/rx: 94/0/95
control rx packets: 193, rx bytes: 8506
control tx packets: 195, tx bytes: 8625
data rx packets: 0, rx bytes: 0, rx errors: 0
data tx packets: 6, tx bytes: 588, tx errors: 0
establish retries: 0
```

To view L2TPv3 tunnel config:

```
(Instant AP)# show l2tpv3 tunnel config
Tunnel profile test_tunnel_primary
l2tp host name: Instant-C4:42:98
local UDP port: 1701
peer IP address: 10.0.0.65
peer UDP port: 3000
hello timeout 150, retry timeout 80, idle timeout 0
rx window size 10, tx window size 10, max retries 5
use UDP checksums: OFF
do pmtu discovery: OFF, mtu: 1570
framing capability: SYNC ASYNC
bearer capability: DIGITAL ANALOG
use tiebreaker: OFF
peer profile: NOT SET
session profile: NOT SET
trace flags: PROTOCOL FSM API AVPDATA FUNC XPRT DATA SYSTEM CLI

Tunnel profile test_tunnel_backup
l2tp host name: aruba1600pop658509.hsb-dev4.aus
local UDP port: 1701
peer IP address: 10.13.11.157
peer UDP port: 1701
hello timeout 60, retry timeout 1, idle timeout 0
rx window size 10, tx window size 10, max retries 5
use UDP checksums: OFF
do pmtu discovery: OFF, mtu: 1460
framing capability: SYNC ASYNC
bearer capability: DIGITAL ANALOG
```

```
use tiebreaker: OFF
peer profile: NOT SET
session profile: NOT SET
trace flags: PROTOCOL FSM API AVPDATA FUNC XPRT DATA SYSTEM CLI
```

To view L2TPv3 system statistics:

```
(Instant AP)# show l2tpv3 system statistics
L2TP counters:-
Total messages sent: 99, received: 194, retransmitted: 0
illegal: 0, unsupported: 0, ignored AVPs: 0, vendor AVPs: 0
Setup failures: tunnels: 0, sessions: 0
Resource failures: control frames: 0, peers: 0
tunnels: 0, sessions: 0
Limit exceeded errors: tunnels: 0, sessions: 0
Frame errors: short frames: 0, wrong version frames: 0
unexpected data frames: 0, bad frames: 0
Internal: authentication failures: 0, message encode failures: 0
no matching tunnel discards: 0, mismatched tunnel ids: 0
no matching session_discards: 0, mismatched session ids: 0
total control frame send failures: 0, event queue fulls: 0
Message counters:-
Message RX Good RX Bad TX
ILLEGAL 0 0 0
SCCRQ 0 0 1
SCCRP 1 0 0
SCCCN 0 0 1
STOPCCN 0 0 0
RESERVED1 0 0 0
HELLO 95 0 95
OCRQ 0 0 0
OCRP 0 0 0
OCCN 0 0 0
ICRQ 0 0 1
ICRP 1 0 0
ICCN 0 0 1
RESERVED2 0 0 0
CDN 0 0 0
WEN 0 0 0
SLI 0 0 0
```

Configuring Routing Profiles

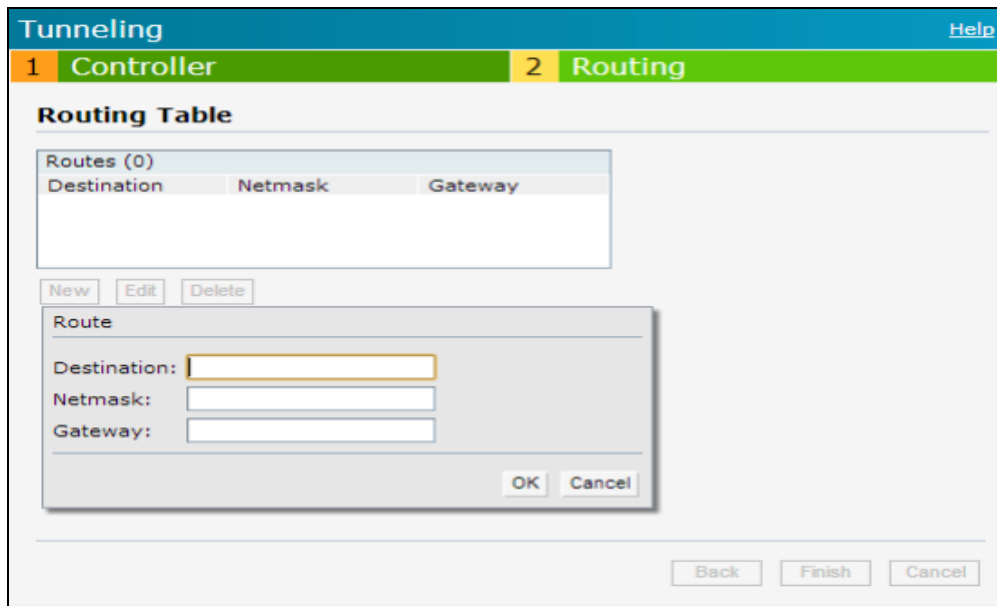
OAW-IAPs can terminate a single VPN connection on an OmniAccess WLAN Switch. The routing profile defines the corporate subnets which need to be tunneled through IPsec. You can configure routing profiles for policy based routing into the VPN tunnel using the AOS-W Instant UI or the CLI.

In the AOS-W Instant UI

To configure a routing profile:

1. Click **Routing** in the **Tunneling** window. The routing details are displayed.
2. Click **New**. The route parameters to configure are displayed.

Figure 57 Tunneling—Routing



3. Update the following parameters:
 - **Destination**— Specify the destination network that is reachable through the VPN tunnel. This defines the IP or subnet that must reach through the IPsec tunnel. Traffic to the IP or subnet defined here will be forwarded through the IPsec tunnel.
 - **Netmask**—Specify the subnet mask to the destination.
 - **Gateway**—Specify the gateway to which the traffic must be routed. This IP address must be the switch IP address on which the VPN connection is terminated. If you have a primary and backup host, configure two routes with the same destination and netmask, but ensure that the gateway is the primary switch IP for one route and the backup switch IP for the second route.
 - **Metric**—The default metric value is 15. Specify a metric value for the datapath route. When two routes or more routes with the same network destination are available for data forwarding, the route with the least metric value takes preference.
4. Repeat step 3 to create the required number of routing profiles.
5. Click **OK**.
6. Click **Finish**.

In the CLI

```
(Instant AP) (config)# routing-profile
(Instant AP) (Routing-profile)# route <destination> <mask> <gateway> {<metric>}
(Instant AP) (Routing-profile)# end
(Instant AP)# commit apply
```



Routing profile is primarily used for IAP-VPN scenarios, to control which traffic should flow between the master OAW-IAP and the VPN tunnel, and which traffic should flow outside of the tunnel.

This section provides the following information:

- [Understanding IAP-VPN Architecture on page 240](#)
- [Configuring OAW-IAP and Switch for IAP-VPN Operations on page 243](#)

Understanding IAP-VPN Architecture

The IAP-VPN architecture includes the following two components:

- OAW-IAPs at branch sites
- Switch at the datacenter

The master OAW-IAP at the branch site acts as the VPN endpoint and the switch at the datacenter acts as the VPN concentrator. When an OAW-IAP is set up for VPN, it forms an IPsec tunnel to the switch to secure sensitive corporate data. IPsec authentication and authorization between the switch and the OAW-IAPs are based on the RAP whitelist configured on the switch.



Only the master OAW-IAP in an OAW-IAP cluster forms the VPN tunnel.

From the switch perspective, the master OAW-IAPs that form the VPN tunnel are considered as VPN clients. The switch terminates VPN tunnels and routes or switches the VPN traffic. The OAW-IAP cluster creates an IPsec or GRE VPN tunnel from the VC to a OmniAccess WLAN Switch in a branch office. The switch only acts as an IPsec or GRE VPN endpoint and it does not configure the OAW-IAP.

IAP-VPN Scalability Limits

The switch scalability in IAP-VPN architecture depends on factors such as IPsec tunnel limit, Branch ID limit, and datapath route table limit. The following table provides the IAP-VPN scalability information for various switch platforms:

Table 50: IAP-VPN Scalability

Platforms	Branches	Routes	L3 Mode Users	NAT Users	Total L2 Users
3200	1000	1000	N/A	N/A	64,000
3400	2000	2000			64,000
3600	8000	8000			64,000
M3	8000	8000			64,000
7210	8000	8000			64,000
7220	16,000	16,000			128,000
7240	32,000	32,000			128,000

- **Branches**—The number of IAP-VPN branches that can be terminated on a given switch platform.
- **Routes**—The number of L3 routes supported on the switch.
- **L3 mode and NAT mode users**—The number of trusted users supported on the switch. There is no scale impact on the switch. They are limited only by the number of clients supported per OAW-IAP.
- **L2 mode users**—The number of L2 mode users are limited to 128,000 for 7220 or 7240 Switches and 64,000 across all platforms.

IAP-VPN Forwarding Modes

The forwarding modes determine whether the DHCP server and default gateway for clients reside in the branch or at the datacenter. These modes do not determine the firewall processing or traffic forwarding functionality. The VC enables different DHCP pools (various assignment modes) in addition to allocating IP subnets for each branch.

The VC allows different modes of forwarding traffic from the clients on a VLAN based on the DHCP scope configured on the OAW-IAP.

For the IAP-VPN deployments, the following forwarding modes are supported:

- Local mode
- L2 Switching mode
- L3 routing mode

The DHCP scopes associated with these forwarding modes are described in the following sections.



Ensure that VLAN 1 is not configured for any of the DHCP scopes as it is reserved for a different purpose.

Local Mode

In this mode, the OAW-IAP cluster at that branch has a local subnet and the master OAW-IAP of the cluster acts as the DHCP server and gateway for clients. The local mode provides access to the corporate network using the inner IP of the IPsec tunnel. The network address for traffic destined to the corporate network is translated at the source with the inner IP of the IPsec tunnel and is forwarded through the IPsec tunnel. The traffic destined to the non-corporate network is translated using the IP address of the OAW-IAP and is forwarded through the uplink.



When the local mode is used for forwarding client traffic, hosts on the corporate network cannot establish connections to the clients on the OAW-IAP, because the source addresses of the clients are translated.

Local, L2 Mode

In this mode, the OAW-IAP cluster at that branch has a local subnet and the master OAW-IAP of the cluster acts as the DHCP server. The default gateway is located outside the OAW-IAP and the network address for the client traffic is not translated at source. In the Local, L2 mode, access to the corporate network is supported only in a single OAW-IAP cluster. The traffic to the non-corporate network is locally bridged.

Local, L3 Mode

In this mode, the network address for traffic destined to the corporate network is translated at the source with the inner IP of the IPsec tunnel and is forwarded through the IPsec tunnel. The traffic destined to the non-corporate network is routed.

Distributed, L2 Mode

In this mode, the OAW-IAP assigns an IP address from the configured subnet and forwards traffic to both corporate and non-corporate destinations. Clients receive the corporate IP with VC as the DHCP server. The default gateway for the client still resides in the datacenter and hence this mode is an L2 extension of corporate VLAN to remote site. Either the switch or an upstream router can be the gateway for the clients. Client traffic destined to datacenter resources is forwarded by the master OAW-IAP (through the IPsec tunnel) to the client's default gateway in the datacenter.

When an OAW-IAP registers with the switch, the switch automatically adds the VPN tunnel associated to this OAW-IAP into the VLAN multicast table. This allows the clients connecting to the L2 mode VLAN to be part of the same L2 broadcast domain on the switch.

Distributed, L3 Mode

The Distributed, L3 mode contains all broadcast and multicast traffic to a branch. The Distributed, L3 mode reduces the cost and eliminates the complexity associated with the classic site-to-site VPN. However, this mode is very similar to a classic site-to-site IPsec VPN where two VPN endpoints connect individual networks together over a public network.

In Distributed, L3 mode, each branch location is assigned a dedicated subnet. The master OAW-IAP in the branch manages the dedicated subnet and acts as the DHCP server and gateway for clients. Client traffic destined to datacenter resources is routed to the switch through the IPsec tunnel, which then routes the traffic to the appropriate corporate destinations.

When an OAW-IAP registers with the switch, the switch adds a route to enable the routing of traffic from the corporate network to clients on this subnet in the branch.

Centralized, L2 Mode

The Centralized, L2 mode extends the corporate VLAN or broadcast domain to remote branches. The DHCP server and the gateway for the clients reside in the datacenter. Either the switch or an upstream router can be the gateway for the clients. For DHCP services in Centralized, L2 mode, Alcatel-Lucent recommends using an external DHCP server and not the DHCP server on the switch. Client traffic destined to datacenter resources is forwarded by the master OAW-IAP (through the IPsec tunnel) to the client's default gateway in the datacenter.

Centralized, L3 Mode

For Centralized, L3 clients, the VC acts as a DHCP relay agent that forwards the DHCP traffic to the DHCP server located behind the switch in the corporate network and reachable through the IPsec tunnel. The Centralized, L3 VLAN IP is used as the source IP. The IP address is obtained from the DHCP server.

DHCP Scope and VPN Forwarding Modes Mapping

The following table provides a summary of the DHCP scope and VPN forwarding modes mapping:

Table 51: DHCP Scope and VPN Forwarding Modes Matrix

Options	Local	Local, L2	Local, L3	Centralized, L2	Centralized, L3	Distributed, L2	Distributed, L3
DHCP server	VC	VC	VC	DHCP Server in the Datacenter	DHCP Server in the Datacenter and VC acts as a relay agent	VC	VC
Default Gateway for clients	VC	Default Gateway in the local network	VC	Controller or a router in the Datacenter	VC	Controller or a router in the Datacenter	VC
Corporate Traffic	Source-NAT is performed with inner IP of the IPsec tunnel	Not applicable	Source-NAT is performed with inner IP of the IPsec tunnel	L2 reachable	Routed	L2 reachable	Routed
Internet Traffic	Source-NAT is performed with local IP of the VC	Locally bridged	Routed	Source-NAT is performed with local IP of the VC	Source-NAT is performed with local IP of the VC	Source-NAT is performed with local IP of the VC	Source-NAT is performed with local IP of the VC
Branch access from datacenter	No	No	No	Yes	Yes	Yes	Yes

Configuring OAW-IAP and Switch for IAP-VPN Operations

This section describes the configuration procedures for the OAW-IAP and the switch to realize generic use cases. For information on specific deployment scenarios, see [IAP-VPN Deployment Scenarios on page 395](#).



This section describes the configuration procedures to perform on the OAW-IAP for generic use cases. For information on specific deployment scenarios, see [IAP-VPN Deployment Scenarios on page 395](#).

Configuring an OAW-IAP Network for IAP-VPN Operations

An OAW-IAP network requires the following configurations for IAP-VPN operations.

1. [Defining the VPN Host Settings](#)

2. [Configuring Routing Profiles](#)
3. [Configuring DHCP Profiles](#)
4. [Configuring an SSID or Wired Port](#)
5. [Enabling Dynamic RADIUS Proxy](#)
6. [Configuring Enterprise Domains](#)

Defining the VPN Host Settings

The VPN endpoint on which a master OAW-IAP terminates its VPN tunnel is considered as the host. A master OAW-IAP in an OAW-IAP network can be configured with a primary and backup host to provide VPN redundancy. You can define VPN host settings through **More > VPN > Controller** in the UI.

You can configure the following VPN profiles for the IAP-VPN operations. For more information, see [Configuring a Tunnel from an OAW-IAP to a Mobility Controller on page 227](#).

- [IPsec](#)
- [L2TPv3](#)
- [Manual GRE](#)
- [Aruba GRE](#)

Configuring Routing Profiles

The routing profile on the OAW-IAP determines whether the traffic destined to a subnet must be tunneled through IPsec or bridged locally. If the routing profile is empty, the client traffic will always be bridged locally. For example, if the routing profile is configured to tunnel 10.0.0.0 /8, the traffic destined to 10.0.0.0 /8 will be forwarded through the IPsec tunnel and the traffic to all other destinations is bridged locally.

You can also configure a routing profile with 0.0.0.0 as gateway to allow both the client and OAW-IAP traffic to be routed through a non-tunnel route. If the gateway is in the same subnet as uplink IP address, it is used as a static gateway entry. A static route can be added to all master and slave OAW-IAPs for these destinations. The VPN traffic from the local subnet of OAW-IAP or the VC IP address in the local subnet is not routed to tunnel, but will be switched to the relevant VLAN. For example, when a 0.0.0.0/0.0.0.0 routing profile is defined, to bypass certain IPs, you can add a route to the IP by defining 0.0.0.0 as the destination, thereby forcing the traffic to be routed through the default gateway of the OAW-IAP.

You can configure routing profiles through **More > VPN > Controller** UI. For step-by-step procedural information on configuring routing profile, see [Configuring Routing Profiles on page 238](#).



The OAW-IAP network has only one active tunnel even when fast failover is enabled. At any given time, traffic can be tunneled only to one VPN host.

Configuring DHCP Profiles

You can create DHCP profiles to determine the IAP-VPN mode of operation. An OAW-IAP network can have multiple DHCP profiles configured for different modes of IAP-VPN. You can configure up to eight DHCP profiles. For more information on the IAP-VPN modes of operation, see [IAP-VPN Forwarding Modes on page 241](#).

You can create any of the following types of DHCP profiles for the IAP-VPN operations:

- Local
- Local, L2
- Local, L3
- Distributed, L2
- Distributed, L3

- Centralized, L2
- Centralized, L3

For more information on configuring DHCP profiles, see [Configuring DHCP Scopes on page 209](#).



A Centralized, L2 or Distributed, L2 VLAN or subnet cannot be used to serve OAW-IAPs in a hierarchical mode of deployment. Ensure that the physical IP of the OAW-IAPs connecting to the master OAW-IAP in hierarchical mode of deployment is not on a VLAN or subnet that is in Centralized, L2 or Distributed, L2 mode of operation. For information on hierarchical mode of deployment, see [Understanding Hierarchical Deployment on page 113](#).

Configuring an SSID or Wired Port

For a client to connect to the IAP-VPN network, an SSID or wired port profile on an OAW-IAP must be configured with appropriate IAP-VPN mode of operation. The VLAN configuration in an SSID or wired port profile determines whether an SSID or wired port is configured for the IAP-VPN operations.

To configure an SSID or wired port for a specific IAP-VPN mode, the VLAN ID defined in the SSID or wired port profile must match the VLAN ID defined in the DHCP profile configuration. If the VLAN assignment for an SSID or wired port profile is set to VC assigned, custom, or a static VLAN ID that does not match the VLAN ID configured in the DHCP profiles, the IAP-VPN operations are affected. For example, if a local DHCP profile is configured with a VLAN ID of 200, the VLAN configuration on the SSID must be set to a static VLAN ID 200.



Ensure that the VLAN assignment for an SSID or wired port profile is not set to default as the VPN tunnel is not supported on the default VLAN.

For information on how to configure an SSID or wired port profile, see [Wireless Network Profiles on page 79](#) and [Configuring a Wired Profile on page 106](#), respectively.

Enabling Dynamic RADIUS Proxy

The RADIUS server can be deployed at different locations and VLANs. In most cases, a centralized RADIUS or local server is used to authenticate users. However, some user networks can use a local RADIUS server for employee authentication and a centralized RADIUS-based captive portal server for guest authentication. To ensure that the RADIUS traffic is routed to the required RADIUS server, the dynamic RADIUS proxy feature must be enabled. When enabled, dynamic RADIUS proxy ensures that all the RADIUS traffic is sourced from the VC IP or inner IP of the OAW-IAP IPsec tunnel depending on the RADIUS server IP and routing profile.



Ensure that a static VC IP is configured before enabling dynamic RADIUS proxy in order to tunnel the RADIUS traffic to the central RADIUS server in the datacenter.

For information on enabling dynamic RADIUS proxy, see [Configuring Dynamic RADIUS Proxy Parameters on page 161](#).

Configuring Enterprise Domains

By default, all the DNS requests from a client are forwarded to the client's DNS server. In a typical OAW-IAP deployment without VPN configuration, client DNS requests are resolved by the DNS server of clients. For the IAP-VPN scenario, the enterprise domain settings on the OAW-IAP are used to determine how client DNS requests are routed. For information on how to configure enterprise domains, see [Configuring Enterprise Domains on page 194](#).

Configuring a Switch for IAP-VPN Operations

Alcatel-Lucent switches provide an ability to terminate the IPsec and GRE VPN tunnels from the OAW-IAP and provide corporate connectivity to the branch network.

For IAP-VPN operations, ensure that the following configuration and verification procedures are completed on the switch:

- [OSPF Configuration](#)
- [VPN Configuration](#)
- [Branch-ID Allocation](#)
- [Branch Status Verification](#)



This section describes the configuration procedures for the switch to realize generic use cases. For information on specific deployment scenarios, see [IAP-VPN Deployment Scenarios on page 395](#).



AOS-W Instant 6.3 or later version is recommended the switches with IAP-VPN configuration. The IAP-VPN configuration is not supported on OAW-4306 Series switches.

OSPF Configuration

Open Shortest Path First (OSPF) is a dynamic Interior Gateway routing Protocol (IGP) based on IETF RFC 2328. The premise of OSPF is that the shortest or fastest routing path is used. The implementation of OSPFv2 allows switches to deploy effectively in a Layer 3 topology. The switches can act as the default gateway for all clients and forward user packets to the upstream router.

Each IAP-VPN can be defined a separate subnet derived from the corporate intranet pool to allow IAP-VPN devices to work independently. For sample topology and configuration, refer to the *AOS-W Instant 6.5 User Guide*.

To redistribute IAP-VPN routes into the OSPF process:

```
(Instant AP) (config) # router ospf redistribute rapng-vpn
```

To verify if the redistribution of the IAP-VPN is enabled:

```
(host) #show ip ospf redistribute
```

To configure aggregate route for IAP-VPN routes:

```
(Instant AP) (config) # router ospf aggregate-route rapng-vpn
```

To view the aggregated routes for IAP-VPN routes:

```
(Instant AP) #show ip ospf rapng-vpn aggregate-routes  
RAPNG VPN aggregate routes
```

```
-----  
Prefix Mask Contributing routes Cost  
-----  
201.201.200.0 255.255.252.0 5 268779624  
100.100.2.0 255.255.255.0 1 10
```

To verify the details of a configured aggregated route:

```
(Instant AP) # show ip ospf rapng-vpn aggregated-routes <net> <mask>  
(Instant AP) # show ip ospf rapng-vpn aggregate-routes 100.100.2.0 255.255.255.0  
Contributing routes of RAPNG VPN aggregate route
```

```
-----  
Prefix Mask Next-Hop Cost  
-----  
100.100.2.64 255.255.255.224 5.5.0.10 10
```

To view all the redistributed routes:

```
(Instant AP) # show ip ospf database  
OSPF Database Table
```

```
-----  
Area ID      LSA Type      Link ID      Adv Router    Age    Seq#          Checksum  
-----
```

0.0.0.15	ROUTER	9.9.9.9	9.9.9.9	159	0x80000016	0xee92
0.0.0.15	ROUTER	10.15.148.12	10.15.148.12	166	0x80000016	0x4c0d
0.0.0.15	NETWORK	10.15.148.12	10.15.148.12	167	0x80000001	0x9674
0.0.0.15	NSSA	12.12.2.0	9.9.9.9	29	0x80000003	0x7b54
0.0.0.15	NSSA	12.12.12.0	9.9.9.9	164	0x80000008	0x63a
0.0.0.15	NSSA	12.12.12.32	9.9.9.9	164	0x80000008	0x7b8
0.0.0.15	NSSA	50.40.40.0	9.9.9.9	164	0x80000007	0x8ed4
0.0.0.15	NSSA	51.41.41.128	9.9.9.9	164	0x80000007	0x68f6
0.0.0.15	NSSA	53.43.43.32	9.9.9.9	164	0x80000007	0x2633
0.0.0.15	NSSA	54.44.44.16	9.9.9.9	164	0x80000007	0x353
N/A	AS_EXTERNAL	12.12.2.0	9.9.9.9	29	0x80000003	0x8c06
N/A	AS_EXTERNAL	12.12.12.0	9.9.9.9	169	0x80000001	0x25e4
N/A	AS_EXTERNAL	12.12.12.32	9.9.9.9	169	0x80000001	0x2663
N/A	AS_EXTERNAL	50.40.40.0	9.9.9.9	169	0x80000001	0xab80
N/A	AS_EXTERNAL	51.41.41.128	9.9.9.9	169	0x80000001	0x85a2
N/A	AS_EXTERNAL	53.43.43.32	9.9.9.9	169	0x80000001	0x43de
N/A	AS_EXTERNAL	54.44.44.16	9.9.9.9	169	0x80000001	0x20fe

To verify if the redistributed routes are installed or not:

```
(Instant AP)# show ip route
Codes: C - connected, O - OSPF, R - RIP, S - static
M - mgmt, U - route usable, * - candidate default, V - RAPNG VPN
Gateway of last resort is Imported from DHCP to network 0.0.0.0 at cost 10
Gateway of last resort is Imported from CELL to network 0.0.0.0 at cost 10
Gateway of last resort is Imported from PPPOE to network 0.0.0.0 at cost 10
Gateway of last resort is 10.15.148.254 to network 0.0.0.0 at cost 1
S* 0.0.0.0/0 [1/0] via 10.15.148.254*
V 12.12.2.0/24 [10/0] ipsec map
V 12.12.12.0/25 [10/0] ipsec map
V 12.12.12.32/27 [10/0] ipsec map
V 50.40.40.0/24 [10/0] ipsec map
V 51.41.41.128/25 [10/0] ipsec map
V 53.43.43.32/27 [10/0] ipsec map
V 54.44.44.16/28 [10/0] ipsec map
C 9.9.9.0/24 is directly connected, VLAN9
C 10.15.148.0/24 is directly connected, VLAN1
C 43.43.43.0/24 is directly connected, VLAN132
C 42.42.42.0/24 is directly connected, VLAN123
C 44.44.44.0/24 is directly connected, VLAN125
C 182.82.82.12/32 is an ipsec map 10.15.149.69-182.82.82.12
C 182.82.82.14/32 is an ipsec map 10.17.87.126-182.82.82.14
```

VPN Configuration

The following VPN configuration steps on the switch enable the OAW-IAPs to terminate their VPN connection on the switch:

Whitelist Database Configuration

The whitelist database is a list of the MAC addresses of the OAW-IAPs that are allowed to establish VPN connections with the switch. This list can be either stored in the switch database or on an external server.

You can use the following CLI command to configure the whitelist database entries if the switch is acting as the whitelist database:

```
(host)# whitelist-db rap add mac-address 00:11:22:33:44:55 ap-group test
```

The **ap-group** parameter is not used for any configuration, but needs to be configured. The parameter can be any valid string.

If an external server is used as the location for the whitelist database, add the MAC addresses of the valid OAW-IAPs in the external database or external directory server and then configure a RADIUS server to authenticate the OAW-IAPs using the entries in the external database or external directory server.

If you are using the Windows 2003 server, perform the following steps to configure the external whitelist database on it. There are equivalent steps available for the Windows Server 2008 and other RADIUS servers.

1. Add the MAC addresses of all the OAW-IAPs in the Active Directory of the RADIUS server:
 - a. Open the **Active Directory and Computers** window, add a new user and specify the MAC address (without the colon delimiter) of the OAW-IAP for the username and password, respectively.
 - b. Right-click the user that you have just created and click **Properties**.
 - c. On the **Dial-in** tab, select **Allow access** in the **Remote Access Permission** section and click **OK**.
 - d. Repeat Step a through Step c for all OAW-IAPs.
2. Define the remote access policy in the Internet Authentication Service:
 - a. In the **Internet Authentication Service** window, select **Remote Access Policies**.
 - b. Launch the wizard to configure a new remote access policy.
 - c. Define filters and select **grant remote access permission** in the **Permissions** window.
 - d. Right-click the policy that you have just created and select **Properties**.
 - e. In the **Settings** tab, select the policy condition, and click **Edit Profile...**
 - f. In the **Advanced** tab, select **Vendor Specific**, and click **Add** to add new vendor-specific attributes.
 - g. Add new vendor-specific attributes and click **OK**.
 - h. In the **IP** tab, provide the IP address of the OAW-IAP and click **OK**.

VPN Local Pool Configuration

The VPN local pool is used to assign an IP address to the OAW-IAP after successful XAUTH VPN.

```
(Instant AP) # ip local pool "rapngpool" <startip> <endip>
```

Role Assignment for the Authenticated OAW-IAPs

Define a role that includes an Source-NAT rule to allow connections to the RADIUS server and for the Dynamic RADIUS Proxy in the OAW-IAP to work. This role is assigned to OAW-IAPs after successful authentication.

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

VPN Profile Configuration

The VPN profile configuration defines the server used to authenticate the OAW-IAP (internal or an external server) and the role assigned to the OAW-IAP after successful authentication.

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

Branch-ID Allocation

For branches deployed in Distributed, L3 and Distributed, L2 modes, the master OAW-IAP in the branch and the switch should agree upon a subnet/IP addresses to be used for DHCP services in the branch. The process or protocol used by the master OAW-IAP and the switch to determine the subnet/IP addresses used in a branch is called BID allocation. The BID allocation process is not essential for branches deployed in local or Centralized, L2 mode. The following are some of the key functions of the BID allocation process:

- Determines the IP addresses used in a branch for Distributed, L2 mode
- Determines the subnet used in a branch for Distributed, L3 mode
- Avoids IP address or subnet overlap (that is, avoids IP conflict)

- Ensures that a branch is allocated the same subnet or range of IP addresses irrespective of which OAW-IAP in the branch becomes the master in the OAW-IAP cluster

Branch Status Verification

To view the details of the branch information connected to the switch, execute the **show iap table** command.

Example

This example shows the details of the branches connected to the switch:

```
(host) #show iap table long
```

```
IAP Branch Table
```

```
-----
Name          VC MAC Address      Status  Inner IP      Assigned Subnet  Assigned Vlan
-----
Tokyo-CB:D3:16 6c:f3:7f:cc:42:f8  DOWN   0.0.0.0
Paris-CB:D3:16 6c:f3:7f:cc:3d:04  UP     10.15.207.140  10.15.206.99/29  2
LA             6c:f3:7f:cc:42:25  UP     10.15.207.111  10.15.206.24/29  2
Munich        d8:c7:c8:cb:d3:16  DOWN   0.0.0.0
London-c0:e1  6c:f3:7f:c0:e1:b1  UP     10.15.207.120  10.15.206.64/29  2
Instant-CB:D3 6c:f3:7f:cc:42:1e  DOWN   0.0.0.0
Delhi         6c:f3:7f:cc:42:ca  DOWN   0.0.0.0
Singapore     6c:f3:7f:cc:42:cb  UP     10.15.207.122  10.15.206.120/29  2
```

```
Key          Bid(Subnet Name)
---
```

```
b3c65c...
b3c65c...
b3c65c... 2(10.15.205.0-10.15.205.250,5),1(10.15.206.1-10.15.206.252,5)
a2a65c... 0
b3c65c... 7(10.15.205.0-10.15.205.250,5),8(10.15.206.1-10.15.206.252,5)
b3c65c...
b3c65c... 1(10.15.205.0-10.15.205.250,5),2(10.15.206.1-10.15.206.252,5)
b3c65c... 14(10.15.205.0-10.15.205.250,5),15(10.15.206.1-10.15.206.252,5)
```

The output of this command provides the following information:

Table 52: Branch Details

Parameter	Description
Name	Displays the name of the branch.
VC MAC Address	Displays the MAC address of the VC of the branch.
Status	Displays the current status of the branch (UP/DOWN).
Inner IP	Displays the internal VPN IP of the branch.
Assigned Subnet	Displays the subnet mask assigned to the branch.

Table 52: Branch Details

Parameter	Description
Assigned Vlan	Displays the VLAN ID assigned to the branch.
Key	Displays the key for the branch, which is unique to each branch.
Bid (Subnet Name)	<p>Displays the Branch ID (BID) of the subnet.</p> <p>In the example above, the switch displays bid-per-subnet-per-branch i.e., for "LA" branch, BID "2" for the ip-range "10.15.205.0-10.15.205.250" with client count per branch "5"). If a branch has multiple subnets, it can have multiple BIDs.</p> <p>If a branch is in UP state and does not have a Bid(Subnet Name), it means that the OAW-IAP is connected to a switch, which did not assign any BID for any subnet. In the above example, "Paris-CB:D3:16" branch is UP and does not have a Bid(Subnet Name). This means that either the OAW-IAP is connected to a backup switch or it is connected to a primary switch without any Distributed, L2 or Distributed, L3 subnets.</p>



The **show iap table** command output does not display the **Key** and **Bid(Subnet Name)** details.

This chapter provides the following information:

- [ARM Overview on page 251](#)
- [Configuring ARM Features on an OAW-IAP on page 252](#)
- [Configuring Radio Settings on page 258](#)

ARM Overview

Adaptive Radio Management (ARM) is a radio frequency management technology that optimizes WLAN performance even in networks with the 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 a fair distribution of the 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 802.11 a, b, g, n, and ac client types to interoperate at the highest performance levels.

Channel or Power Assignment

The channel or power assignment 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 the ongoing operations when RF conditions change.

Voice Aware Scanning

The Voice Aware scanning feature prevents an OAW-IAP supporting an active voice call from scanning for other channels in the RF spectrum and allows the OAW-IAP to resume scanning when there are no active voice calls. This significantly improves the voice quality when a call is in progress and simultaneously delivers the automated RF management functions. By default, this feature is enabled.

Load Aware Scanning

The Load Aware Scanning feature dynamically adjusts scanning function 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. By default, this feature is enabled.

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 sends reports to a VC on network (WLAN) coverage, interference, and intrusion detection.

ARM Metrics

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

Configuring ARM Features on an OAW-IAP

This section describes the following procedures for configuring ARM features:

- [Band Steering on page 252](#)
- [Airtime Fairness Mode on page 253](#)
- [Client Match on page 253](#)
- [Access Point Control on page 255](#)

Band Steering

The band steering feature assigns the dual-band capable clients to 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 that on the 2.4 GHz band. You can configure band steering parameters through the AOS-W Instant UI or the CLI.

In the AOS-W Instant UI

To configure band steering:

1. In the **RF > ARM > Show advanced options** tab view, configure the following parameters:

Table 53: *Band Steering Mode—Configuration Parameters*

Parameter	Description
Prefer 5 GHz	Select this option to use band steering in the 5 GHz mode. On selecting this, the OAW-IAP steers the client to the 5 GHz band (if the client is 5 GHz-capable), but allows the client connection on the 2.4 GHz band if the client persistently attempts for 2.4 GHz association.
Force 5 GHz	Select this option to enforce 5 GHz band steering mode on the OAW-IAPs.
Balance Bands	Select this option to allow the OAW-IAP to balance the clients across the two radios to best utilize the available 2.4 GHz bandwidth. This feature takes into account the fact that the 5 GHz band has more channels than the 2.4 GHz band, and that the 5 GHz channels operate in 40 MHz, while the 2.4 GHz band operates in 20 MHz.
Disabled	Select this option if you want to allow the clients to select the band to use.

2. Click **OK**.

In the CLI

To configure band steering:

```
(Instant AP) (config)# arm
(Instant AP) (ARM)# band-steering-mode {<Prefer 5 GHz>| <Force 5 GHz>|<Balance
Bands>|<Disabled>}
(Instant AP) (ARM)# end
(Instant AP)# commit apply
```

Airtime Fairness Mode

The airtime fairness feature provides equal access to all clients on the wireless medium, regardless of client type, capability, or operating system, thus delivering uniform performance to all clients. This feature prevents the clients from monopolizing resources. You can configure airtime fairness mode parameters through the AOS-W Instant UI or the CLI.

In the AOS-W Instant UI

1. For **Airtime fairness mode** configuration, specify any of the following values under the **RF > ARM > Show advanced options** tab:

Table 54: Airtime Fairness Mode—Configuration Parameters

Parameter	Description
Default Access	Select this option to provide access based on client requests. When Air Time Fairness is set to default access, per-user and per-SSID bandwidth limits are not enforced.
Fair Access	Select this option to allocate Airtime evenly across all the clients.
Preferred Access	Select this option to set a preference where 802.11n clients are assigned more airtime than 802.11a/11g. The 802.11a/11g clients get more airtime than 802.11b. The ratio is 16:4:1.

2. Click **OK**.

In the CLI

```
(Instant AP) (config) # arm
(Instant AP) (ARM) # air-time-fairness-mode {<Default Access>| <Fair Access> | <Preferred
Access>
(Instant AP) (ARM) # end
(Instant AP) # commit apply
```

Client Match

The ARM client match feature continually monitors a client's RF neighborhood to provide ongoing client band steering and load balancing, and enhanced OAW-IAP reassignment for roaming mobile clients. This feature supersedes the legacy band steering and spectrum load balancing features, which unlike client match, do not trigger OAW-IAP changes for clients already associated to an OAW-IAP. In addition to this, the Client Match feature provides the smartphone handoff assist function which helps smartphones to switch between 3G and 4G networks when the Wi-Fi connectivity is poor. The OAW-IAP monitors the Received Signal Strength Indicator (RSSI) of the smartphone and checks if it remains under the threshold connectivity strength for a certain duration and deauthenticates the client.

Legacy 802.11 a/b/g access points do not support the client match feature. When client match is enabled on 802.11 n-capable access points, the client match feature overrides any settings configured for the legacy band steering, station handoff assist, or load balancing feature. 802.11 ac-capable access points do not support the legacy band steering, station handoff assist, or load balancing settings; so these access points must be managed using client match.



When the client match feature is enabled on an OAW-IAP, the OAW-IAP measures the RF health of its associated clients. In the current release, the client match feature is supported only within an OAW-IAP cluster. If any of the following trigger conditions is met, clients are moved from one OAW-IAP to another for better performance and client experience:

- **Dynamic Load Balancing**—Client match balances clients across OAW-IAPs on different channels, based on the client load on the OAW-IAPs and the signal to noise ratio (SNR) levels the client detects from an underutilized OAW-IAP. If an OAW-IAP radio can support additional clients, the OAW-IAP will participate in client match load balancing and clients can be directed to that OAW-IAP radio, subject to the predefined SNR thresholds. For better load balancing, clients are steered from busy channels to idle channels.
- **Sticky Clients**—The client match feature also helps mobile clients that tend to stay associated to an OAW-IAP despite low signal levels. OAW-IAPs using client match continually monitor the client's RSSI as the client roams between OAW-IAPs, and move the client to an OAW-IAP when a better radio match can be found. This prevents mobile clients from remaining associated to the OAW-IAPs with less than ideal RSSI, which can cause poor connectivity and reduce performance for other clients associated with that OAW-IAP.
- **Band Steering**—OAW-IAPs using the client match feature monitor the RSSI for clients that advertise a dual-band capability. If a client is currently associated to a 2.4 GHz radio and the OAW-IAP detects that the client has a good RSSI from the 5 GHz radio, the OAW-IAP steers the client to the 5 GHz radio, as long as the 5 GHz RSSI is not significantly worse than the 2.4 GHz RSSI, and the OAW-IAP retains a suitable distribution of clients on each of its radios.
- **Channel Utilization**—Based on the percentage of channel utilization, clients are steered from a busy channel to an idle channel.
- **Client Capability Match**—Based on the client capability match, clients are steered to appropriate channel, for example, HT20, HT40, or VHT80.



Starting from the Instant 6.3.1.1-4.0 release, spectrum load balancing is integrated with the client match feature. Client match allows the OAW-IAPs in a cluster to be divided into several logical OAW-IAP RF neighborhood called domains, which share the same clients. The VC determines the distribution of clients and balances client load across channels, regardless of whether the OAW-IAP is responding to the probe requests of wireless clients.

You can configure client match parameters in the AOS-W Instant UI or the CLI. When client match is enabled, the dashboard in the main window displays the **Client Match** link on selecting an OAW-IAP in the **Access Points** tab or a client in the **Clients** tab. Clicking this link provides a graphical representation of radio map view of an OAW-IAP and the client distribution on an OAW-IAP radio. For more information, see [Client Match on page 49](#).

In the AOS-W Instant UI

1. For client match configuration, specify the following parameters in the **RF > ARM > Show advanced options** tab:

Table 55: Client Match Configuration Parameters

Parameter	Description
Client match	Select Enabled to enable the Client match feature on OAW-IAPs. When enabled, client count will be balanced among all the channels in the same band. For more information, see ARM Overview on page 251 . By default, the client match feature is disabled. NOTE: When client match is enabled, ensure that Scanning is enabled.
CM calculating interval	Specify a value for calculating the interval of Client match. The value specified for CM calculating interval determines the interval at which client match is calculated. The interval is specified in seconds and the default value is 30 seconds. You can specify a value within the range of 10–600.
CM neighbor matching %	Specify a value for CM neighbor matching % . This number takes into account the least similarity percentage to be considered as in the same virtual RF neighborhood of client match. You can specify a percentage value within the range of 20–100. The default value is 75%.
CM threshold	Specify a value for CM threshold . This number takes acceptance client count difference among all the channels of client match into account. When the client load on an OAW-IAP reaches or exceeds the threshold, client match is enabled on that OAW-IAP. You can specify a value within range of 1–255. The default value is 2.
SLB mode	Select a mode from the SLB mode drop-down list. The SLB mode determines the balancing strategy for client match. The following options are available: <ul style="list-style-type: none"> • Channel • Radio • Channel + Radio

2. Click **OK**.

In the CLI

```
(Instant AP) (config)# arm
(Instant AP) (ARM) # client-match calc-interval <seconds>
(Instant AP) (ARM) # client-match calc-threshold <threshold>
(Instant AP) (ARM) # client-match nb-matching <percentage>
(Instant AP) (ARM) # client-match slb-mode 1
(Instant AP) (ARM) # end
(Instant AP) # commit apply
```

Access Point Control

You can configure access point control parameters through the AOS-W Instant UI or the CLI.

In the AOS-W Instant UI

1. For **Access Point Control**, specify the following parameters in the **RF > ARM > Show advanced options** tab:

Table 56: Access Point Control—Configuration Parameters

Parameter	Description
Customize Valid Channels	Select this check box to customize valid channels for 2.4 GHz and 5 GHz. By default, the OAW-IAP uses valid channels as defined by the Country Code (regulatory domain). On selecting the Customize Valid Channels check box, a list of valid channels for both 2.4 GHz and 5 GHz are displayed. The valid channel customization feature is disabled by default.
Minimum Transmit Power	Specify the minimum transmission power. The value specified for Minimum Transmit Power indicates the minimum Effective Isotropic Radiated Power (EIRP) that can range from 3 dBm to 33 dBm in 3 dBm increments. If the minimum transmission EIRP setting configured on an OAW-IAP is not supported by the OAW-IAP model, this value is reduced to the highest supported power setting. The default value for minimum transmit power is 18 dBm.
Maximum Transmit Power	Specify the maximum transmission power. The value specified for Maximum Transmit Power indicates the maximum Effective Isotropic Radiated Power (EIRP) that can range from 3 dBm to 33 dBm in 3 dBm increments. If the maximum transmission EIRP configured on an OAW-IAP is not supported by the OAW-IAP model, the value is reduced to the highest supported power setting. The default value for maximum transmit power is 127 dBm.
Client aware	When Enabled , ARM does not change channels for the OAW-IAPs with active clients, except for high-priority events such as RADAR or excessive noise. This feature must be enabled in most deployments for a stable WLAN. If the Client Aware mode is Disabled , the OAW-IAP may change to a more optimal channel, that may disrupt the current client traffic for a while. The Client aware option is Enabled by default. NOTE: When Client aware is disabled, channels can be changed even when the clients are active on a BSSID.
Scanning	Select Enabled so that the OAW-IAP dynamically scans all 802.11 channels within its 802.11 regulatory domain at regular intervals and reports to the OAW-IAP. This scanning report includes WLAN coverage, interference, and intrusion detection data. NOTE: For client match configuration, ensure that scanning is enabled.
Wide Channel Bands	Select a band to allow the OAW-IAPs to be placed in 40 MHz (wide band) channels. The Wide Channel Bands allows administrators to configure 40 MHz channels in the 2.4 GHz and 5 GHz bands. 40 MHz channels are two 20 MHz adjacent channels that are bonded together. A 40 MHz channel effectively doubles the frequency bandwidth available for data transmission.
80 MHz Support	Enables or disables the use of 80 MHz channels on OAW-IAPs. This feature allows ARM to assign 80 MHz channels on OAW-IAPs with 5 GHz radios, which support a very high throughput. This setting is enabled by default. NOTE: Only the OAW-IAPs that support 802.11ac can be configured with 80 MHz channels.

2. Reboot the OAW-IAP.

3. Click **OK**.

In the CLI

To configure access point control parameters:

```
(Instant AP) (config) # arm
(Instant AP) (ARM) # a-channels <5GHz-channels>
(Instant AP) (ARM) # min-tx-power <power>
(Instant AP) (ARM) # max-tx-power <power>
(Instant AP) (ARM) # client-aware
(Instant AP) (ARM) # wide-bands {<5GHz>|<2GHz>|<All>|<None>}
(Instant AP) (ARM) # scanning
(Instant AP) (ARM) # 80mhz-support
(Instant AP) (ARM) # end
(Instant AP) # commit apply
```

Verifying ARM Configuration

To view ARM configuration:

```
(Instant AP) # show arm config

Minimum Transmit Power      :18
Maximum Transmit Power     :127
Band Steering Mode         :prefer-5ghz
Client Aware               :enable
Scanning                   :enable
Wide Channel Bands         :5ghz
80Mhz Support              :enable
Air Time Fairness Mode    :fair-access
Client Match               :disable
CM NB Matching Percent     :75
CM Calculating Interval   :30
CM SLB Threshold           :2
CM SLB Balancing Mode     :channel based
CM max client match req   :5
CM max adoption           :5
Custom Channels            :No
2.4 GHz Channels
-----
Channel  Status
-----  -
1        enable
2        disable
3        disable
4        disable
5        disable
6        enable
7        disable
8        disable
9        disable
10       disable
11       enable
12       disable
13       disable
1+       enable
2+       disable
3+       disable
4+       disable
5+       disable
6+       disable
7+       enable
```

5.0 GHz Channels

Channel	Status
36	enable
40	enable
44	enable
48	enable
52	enable
56	enable
60	enable
64	enable
149	enable
153	enable
157	enable
161	enable
165	enable
36+	enable
44+	enable
52+	disable
60+	disable
149+	enable
157+	enable
36E	enable
52E	enable
149E	enable

Client Match for Access Points in a Zone

When Client match is enabled, the decision to move a client from the home OAW-IAP to a target OAW-IAP is made at the radio level. However, this proves inefficient when client match is enabled on an OAW-IAP or SSID operating in a specific zone, it could result in the client being moved to a target OAW-IAP that does not have the same zone specific SSID as the home OAW-IAP.

Starting from AOS-W Instant 6.5.1.0-4.3.1.0, the decision to move a client from a home OAW-IAP to a target OAW-IAP will be made at the SSID level instead of the radio level, by adding the SSID name to the client match radio database. Client Match will check if the same SSID (zone specific SSID on Home OAW-IAP) is available on the target OAW-IAP before it moves the client. This ensures that client match works as expected when zone settings are configured on the OAW-IAP.

Additionally, the maximum clients threshold and the current associated client number of the SSID is added to the client match radio database to prevent the clients from being moved to an SSID whose associated client number is already reached its limit.

You can use the following commands to view the SSID details stored in client match:

The **show ap client-match-ssid-table** command displays the client match SSID table for the current OAW-IAP and its neighboring OAW-IAPs.

The **show ap client-match-ssid-table radio-mac <mac>** command displays the client match SSID table for a specific OAW-IAP denoted by its mac address.

Configuring Radio Settings

You can configure 2.4 GHz and 5 GHz radio settings for an OAW-IAP either using the AOS-W Instant UI or the CLI.

In the AOS-W Instant UI

To configure radio settings:

1. Click the **RF** link located directly above the Search bar of the AOS-W Instant main window.
2. Click **Show advanced options**. The advanced options are displayed.
3. Click the **Radio** tab.
4. Under the channel 2.4.GHz or 5 GHz, or both, configure the following parameters.

Table 57: Radio Configuration Parameters

Parameter	Description
Legacy only	Select Enabled to run the radio in non-802.11n mode. This option is set to Disabled by default.
802.11d / 802.11h	Select Enabled to allow the radio to advertise its 802.11d (Country Information) and 802.11h (Transmit Power Control) capabilities. This option is set to Disabled by default.
Beacon interval	Enter the Beacon period for the OAW-IAP in milliseconds. This indicates how often the 802.11 beacon management frames are transmitted by the access point. You can specify a value within the range of 60-500. The default value is 100 milliseconds.
Interference immunity level	<p>Select to increase the immunity level to improve performance in high-interference environments.</p> <p>The default immunity level is 2.</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 2.4 GHz appliances such as cordless phones. • Level 4—Level 3 settings, and FIR immunity. At this level, the OAW-IAP adjusts its sensitivity to in-band power, which can improve performance in environments with high and constant levels of noise interference. • Level 5—The OAW-IAP completely disables PHY error reporting, improving performance by eliminating the time the OAW-IAP would spend on PHY processing. <p>NOTE: Increasing the immunity level makes the OAW-IAP to lose a small amount of range.</p>
Channel switch announcement count.	Specify the count to indicate the number of channel switching announcements that must be sent before switching to a new channel. This allows associated clients to recover gracefully from a channel change.

Table 57: Radio Configuration Parameters

Parameter	Description
Background spectrum monitoring	Select Enabled to allow the OAW-IAPs in access mode to continue with normal access service to clients, while performing additional function of monitoring RF interference (from both neighboring OAW-IAPs and non Wi-Fi sources such as, microwaves and cordless phones) on the channel they are currently serving clients.
Customize ARM power range	Select the check box and select a minimum (Min Power) and maximum (Max Power) power range value for the 2.4 GHz and 5 GHz band frequencies. The default value is 3 dBm. Unlike the configuration in the ARM profile, the transmit power of all radios in the Radio profile do not share the same configuration.
Very high throughput	Ensure that this check box is selected to enable very high throughput (VHT) on 802.11ac devices with 5 GHz radio. If VHT is enabled for the 5 GHz radio profile on an OAW-IAP, it is automatically enabled for all SSIDs configured on an OAW-IAP. By default, VHT is enabled on all SSIDs. If you want the 802.11ac OAW-IAPs to function as 802.11n OAW-IAPs, clear the check box to disable VHT on these devices.

5. Click **OK**.

In the CLI

To configure 2.4 GHz radio settings:

```
(Instant AP) (config)# rf dot11g-radio-profile
(Instant AP) (RF dot11g Radio Profile)# beacon-interval <milliseconds>
(Instant AP) (RF dot11g Radio Profile)# legacy-mode
(Instant AP) (RF dot11g Radio Profile)# spectrum-monitor
(Instant AP) (RF dot11g Radio Profile)# dot11h
(Instant AP) (RF dot11g Radio Profile)# interference-immunity <level>
(Instant AP) (RF dot11g Radio Profile)# csa-count <count>
(Instant AP) (RF dot11g Radio Profile)# max-distance <count>
(Instant AP) (RF dot11g Radio Profile)# max-tx-power <db>
(Instant AP) (RF dot11g Radio Profile)# min-tx-power <db>
(Instant AP) (RF dot11g Radio Profile)# end
(Instant AP)# commit apply
```

To configure 5 GHz radio settings:

```
(Instant AP) (config)# rf dot11a-radio-profile
(Instant AP) (RF dot11a Radio Profile)# beacon-interval <milliseconds>
(Instant AP) (RF dot11a Radio Profile)# legacy-mode
(Instant AP) (RF dot11a Radio Profile)# spectrum-monitor
(Instant AP) (RF dot11a Radio Profile)# spectrum-band <type>
(Instant AP) (RF dot11a Radio Profile)# dot11h
(Instant AP) (RF dot11a Radio Profile)# interference-immunity <level>
(Instant AP) (RF dot11a Radio Profile)# max-distance <count>
(Instant AP) (RF dot11a Radio Profile)# max-tx-power <db>
(Instant AP) (RF dot11a Radio Profile)# min-tx-power <db>
(Instant AP) (RF dot11a Radio Profile)# csa-count <count>
(Instant AP) (RF dot11a Radio Profile)# end
(Instant AP)# commit apply
```

To disable VHT on a 5 GHz radio profile:

```
(Instant AP) (config)# rf dot11a-radio-profile
(Instant AP) (RF dot11a Radio Profile)# very-high-throughput-disable
```

```
(Instant AP) (RF dot11a Radio Profile) # end
(Instant AP) # commit apply
```

To view the radio configuration:

```
(Instant AP) # show radio config
```

```
2.4 GHz:
Legacy Mode:enable
Beacon Interval:100
802.11d/802.11h:enable
Interference Immunity Level:2
Channel Switch Announcement Count:0
MAX Distance:600
Channel Reuse Type:disable
Channel Reuse Threshold:0
Background Spectrum Monitor:disable
```

```
5.0 GHz:
Legacy Mode:enable
Beacon Interval:100
802.11d/802.11h:enable
Interference Immunity Level:2
Channel Switch Announcement Count:2
MAX Distance:600
Channel Reuse Type:disable
Channel Reuse Threshold:0
Background Spectrum Monitor:disable
Standalone Spectrum Band:5ghz-upper
```

Configuring Cell Size Reduction using the CLI

The Cell Size Reduction feature allows you to manage dense deployments and to increase overall system performance and capacity by shrinking an OAW-IAPs receive coverage area, thereby minimizing co-channel interference and optimizing channel reuse.

The default 0 dB reduction allows the radio to retain its current default Rx sensitivity value.

Values from 1 dB–55 dB reduce the power level that the radio can hear by that amount. If you configure this feature to use a non-default value, you must also reduce the radio's transmission (Tx) power to match its new received (Rx) power level. Failure to match a device's Tx power level to its Rx power level can result in a configuration that allows the radio to send messages to a device that it cannot hear.

To configure Cell Size Reduction for 2.4 GHz radio profile in the CLI:

```
(Instant AP) (config) # rf dot11g-radio-profile
(Instant AP) (RF dot11g Radio Profile) # cell-size-reduction <reduction>
(Instant AP) (RF dot11g Radio Profile) # end
(Instant AP) # commit apply
```

To configure Cell Size Reduction for 5 GHz radio profile in the CLI:

```
(Instant AP) (config) # rf dot11a-radio-profile
(Instant AP) (RF dot11a Radio Profile) # cell-size-reduction <reduction>
(Instant AP) (RF dot11a Radio Profile) # end
(Instant AP) # commit apply
```

ARM Channel Selection using the CLI

Starting from AOS-W Instant 6.5.0.0-4.3.0.0, OAW-IAPs can search for a new environment in a short span of time, so that the ARM is triggered to perform frequent scanning and selection of a valid channel for transmission.

By default, the ARM is triggered to scan all the channels every 10 seconds, and select the best channel for transmission. But when the OAW-IAP is in a new environment, ARM is triggered to perform frequent scanning of the non-DFS channels every 200 milliseconds, and select the best available channel for transmission. The **ap-frequent-scan** command is introduced in the CLI to enable the OAW-IAPs to trigger frequent scanning of transmission signals on a radio profile.



Wireless connection is affected for a few seconds when the frequent scanning of non-DFS channels is ongoing. The connection is re-established after the ARM selects a valid channel. Typically, a frequent scanning session lasts for less than 10 seconds.

Perform the following checks before scanning:

- The DFS channels must be skipped (this is done to avoid delays in scanning).
- The OAW-IAP must be on stand-alone mode.
- The **client-aware** parameter must be disabled in the ARM profile.

In the CLI

The following example triggers ARM scanning on a 2.4 GHz frequency band radio profile:

```
(Instant AP)# ap-frequent-scan 2.4
```

To verify the status of ARM scanning:

```
(Instant AP)# show ap debug am-config
```

This chapter provides the following information:

- [Deep Packet Inspection on page 263](#)
- [Enabling Application Visibility on page 263](#)
- [Application Visibility on page 264](#)
- [Enabling URL Visibility on page 269](#)
- [Configuring ACL Rules for Application and Application Categories on page 269](#)
- [Configuring Web Policy Enforcement Service on page 272](#)

Deep Packet Inspection

AppRF is Alcatel-Lucent's custom-built Layer 7 firewall capability. It consists of an onboard deep packet inspection and a cloud-based Web Policy Enforcement (WPE) service that allows creating firewall policies based on types of application. The WPE capabilities require the OAW-IAP to have a WPE subscription. For more information on subscription, contact the Alcatel-Lucent Sales Team.

OAW-IAPs with DPI capability analyze data packets to identify applications in use and allow you to create access rules to determine client access to applications, application categories, web categories, and website URLs based on web reputation. You can also define traffic-shaping policies such as bandwidth control and QoS per application for client roles. For example, you can block bandwidth-monopolizing applications on a guest role within an enterprise.

The AppRF feature provides application visibility for analyzing client traffic flow. OAW-IAPs support the power of both in-device packet flow identification and dynamically updated cloud-based web categorization.

Enabling Application Visibility

Enabling AppRF visibility allows you to view the AppRF statistics for an OAW-IAP or the clients associated with an OAW-IAP. Full URL visibility for HTTP sessions fed to Analytics and Location Engine (ALE) is exposed as northbound APIs which can be consumed by URL analytical engines for advanced client URL data mining and analytics.

You can enable AppRF visibility by using the AOS-W Instant UI or the CLI.

In the AOS-W Instant UI

To enable AppRF:

1. Navigate to **System > General**.
2. Select **All** from the **AppRF visibility** drop-down list to view both application and web categories charts or either **App** or **WebCC** to view their DPI graphs separately.
3. Click **OK**.

In the CLI

To enable AppRF visibility:

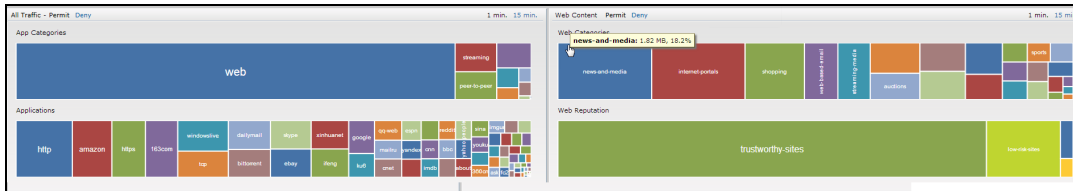
```
(Instant AP) (config)# dpi [app|webcc]
(Instant AP) (config)# end
(Instant AP)# commit apply
```

Application Visibility

The AppRF graphs are based on Deep Packet Inspection (DPI) application and Web Policy Enforcement (WPE) service, which provide application traffic summary for the client devices associated with an OAW-IAP. The **AppRF** link above the activity panel of the dashboard is displayed only if **AppRF visibility** is enabled in the **System** window.

The following figure provides a view of the AppRF dashboard:

Figure 58 AppRF Dashboard



The AppRF dashboard presents four different graph areas with data graphs on all client traffic and content filters based on App Category, Web Category, and Web Reputation. Click each category to view the real-time client traffic data or usage trend in the last 15 minutes or 1 minute.

The **permit** and **deny** monitoring tabs in the All Traffic and Web Content sections provide enforcement visibility support.

- **Permit** represents the allowed or permitted traffic on the OAW-IAP.
- **Deny** represents all the blocked URLs and traffic .

Application Categories Chart

The application categories chart displays details on the client traffic towards the application categories. By clicking the rectangle area, you can view the following graphs, and toggle between the chart and list views.

Figure 59 Application Categories Chart: Client View

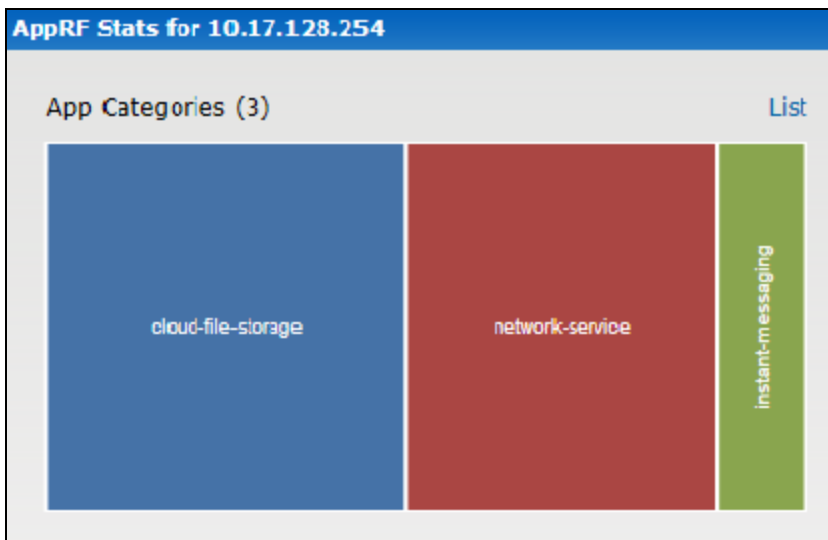


Figure 60 Application Categories List: Client View

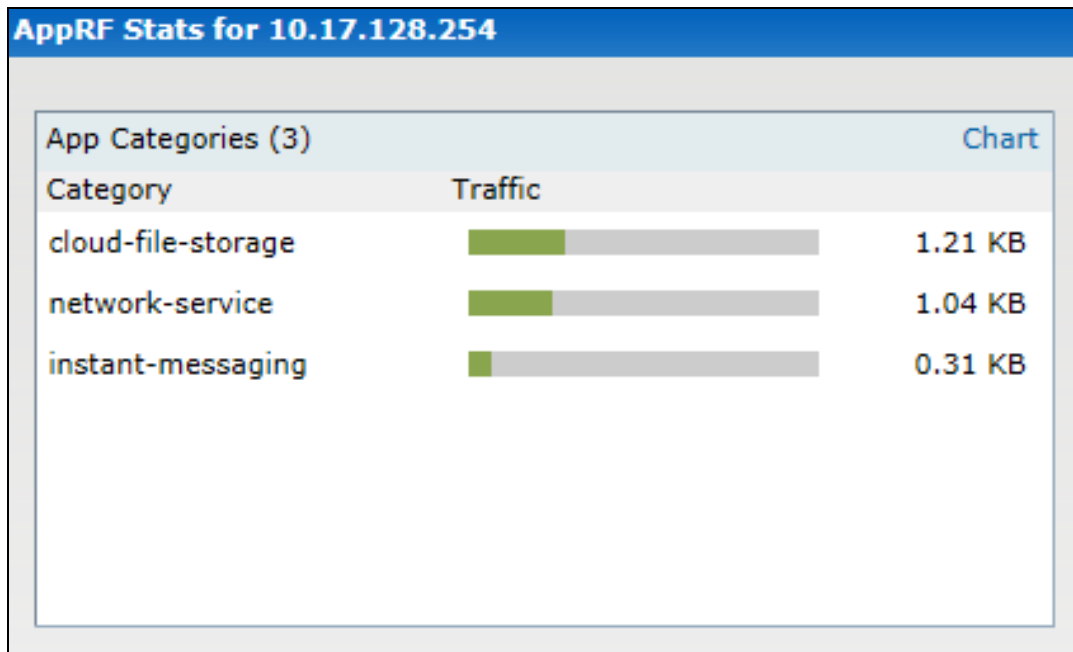
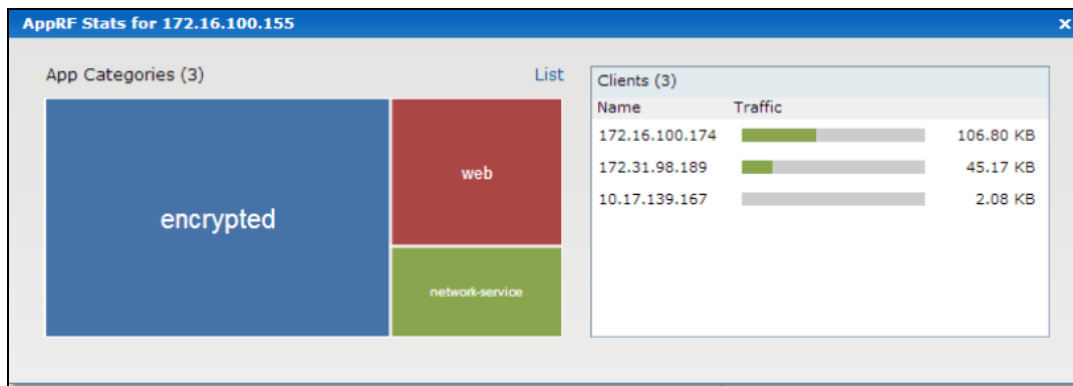


Figure 61 Application Categories Chart: OAW-IAP View



Applications Chart

The applications chart displays details on the client traffic towards the applications. By clicking the rectangular area, you can view the following graphs, and toggle between the chart and list views.

Figure 62 Applications Chart: Client View

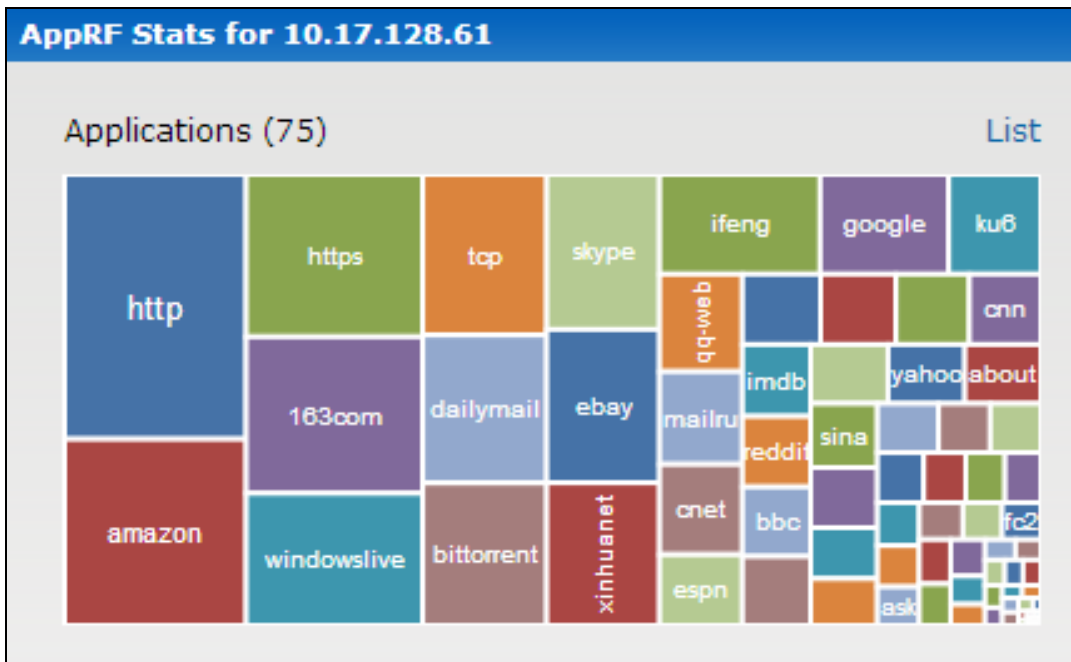
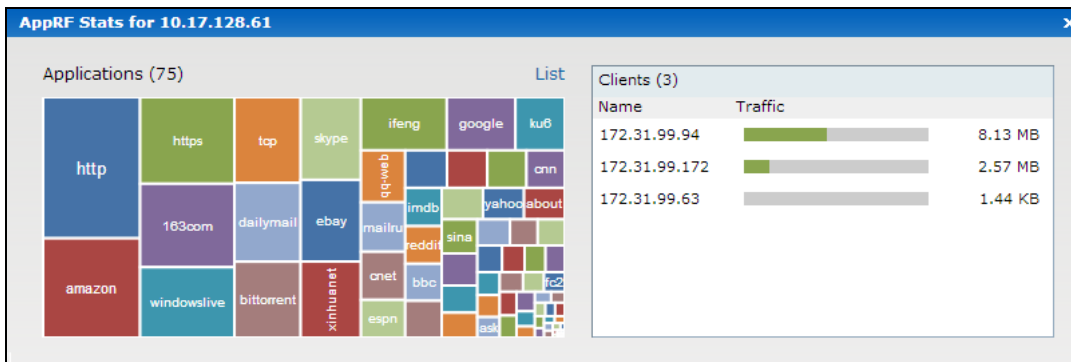


Figure 63 Applications List: Client View

The list shows traffic details for 72 applications. The top applications are https, windowslive, amazon, 163com, http, ebay, and people.

Application	Traffic
https	956.04 KB
windowslive	926.47 KB
amazon	870.90 KB
163com	849.57 KB
http	635.73 KB
ebay	506.51 KB
people	359.27 KB

Figure 64 Application Chart: Access Point View



Web Categories Charts

The web categories chart displays details about the client traffic to the web categories. By clicking the rectangle area, you can view the following graphs, and toggle between the chart and list views.

Figure 65 Web Categories Chart: Client View

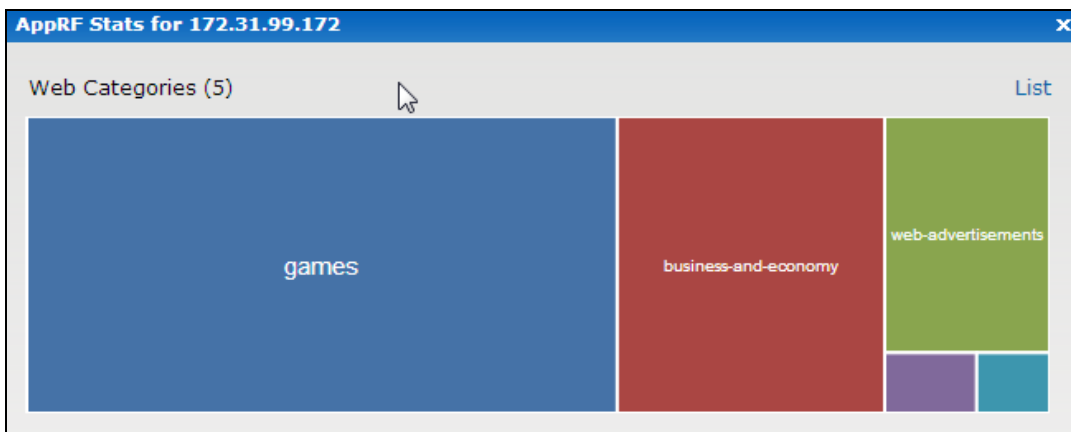


Figure 66 Web Categories List: Client View

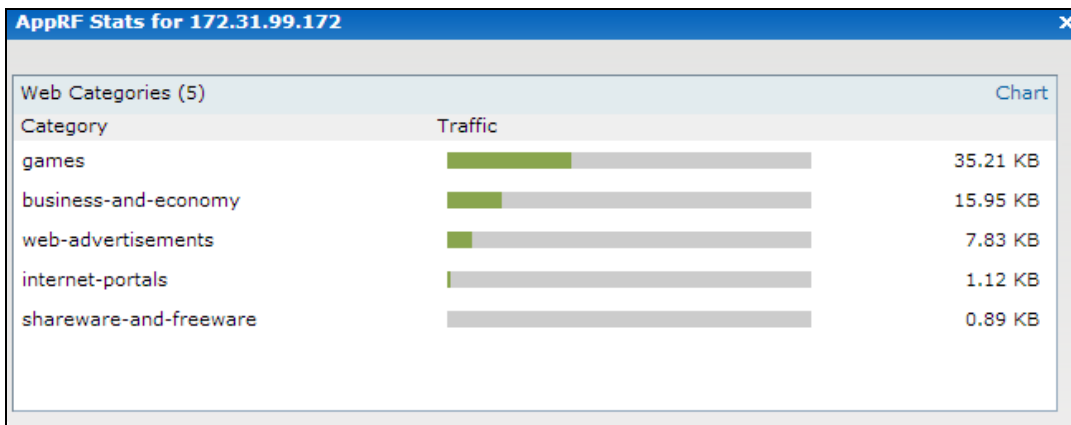
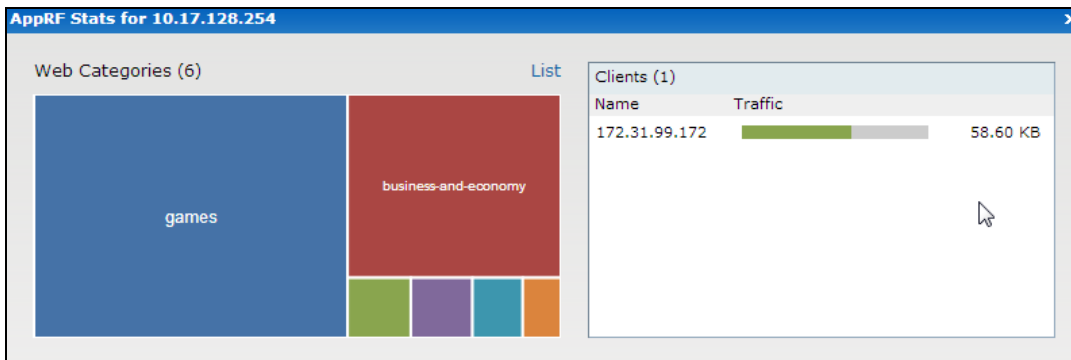


Figure 67 Web Categories Chart: Access Point View



Web Reputation Charts

The web reputation chart displays details about the client traffic to the URLs that are assigned security ratings. By clicking in the rectangle area, you can view the following graphs, and toggle between the chart and list views.

Figure 68 Web Reputation Chart: Client View

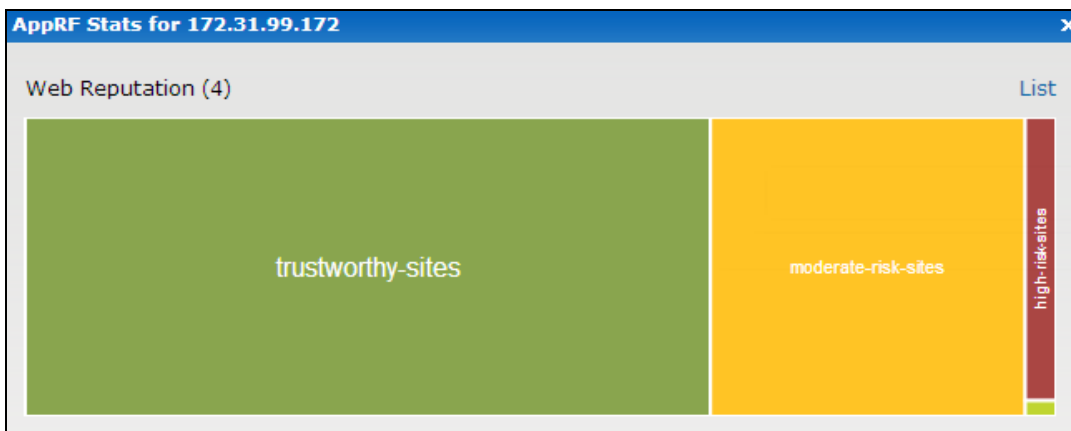


Figure 69 Web Reputation List: Client View

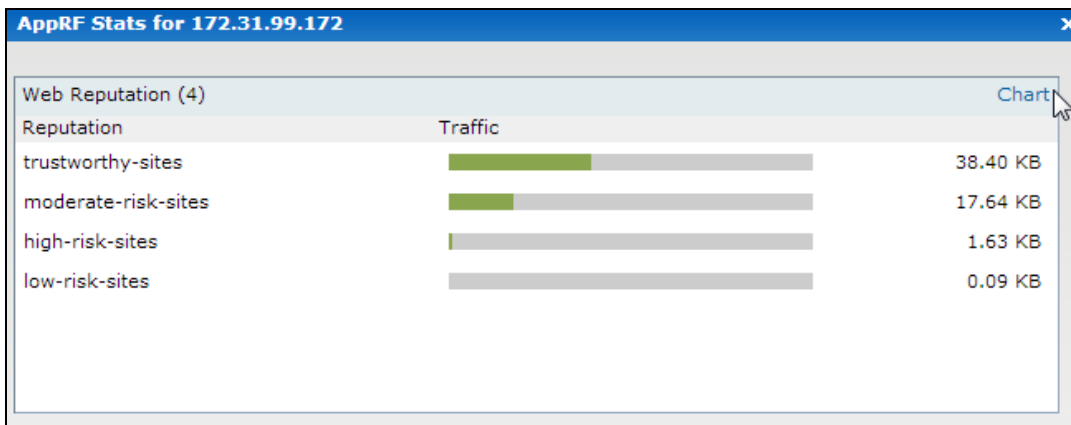
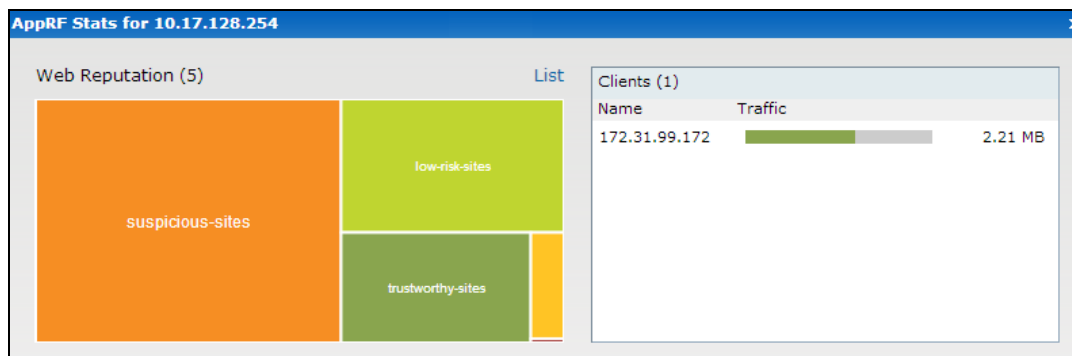


Figure 70 Web Reputation Chart: OAW-IAP View



Enabling URL Visibility

Enabling URL visibility allows the OAW-IAP to extract the full URL information of the HTTP and HTTPS sessions and periodically log them on the ALE server. Full URL visibility for HTTP sessions fed to ALE are exposed as Northbound APIs, and are used by URL analytical engines for advanced client URL data mining and analysis.

You can enable URL visibility by using the AOS-W Instant UI or the CLI:

In the AOS-W Instant UI

To enable URL visibility:

1. Navigate to **System > General**.
2. Select **Enabled** from the **URL visibility** drop-down list.
3. Click **OK**.

In the CLI

To enable URL visibility:

```
(Instant AP) (config)# url-visibility
(Instant AP) (config)# end
(Instant AP)# commit apply
```

Configuring ACL Rules for Application and Application Categories

This section describes the procedure for configuring access rules based on application and application categories. The Application and Application rules utilize the onboard DPI engine.

- For information on configuring access rules to control access to network services, see [Configuring ACL Rules for Network Services on page 180](#).
- For information on configuring access rules based on web categories and web reputation, see [Configuring Web Policy Enforcement Service on page 272](#).

In the AOS-W Instant UI

To configure ACL rules for a user role:

1. Navigate to the **Security > Roles** tab. The **Roles** tab contents are displayed.
You can also configure access rules for a wired or wireless client by using:
 - a. The WLAN wizard (**Network > WLAN SSID > Edit > Edit WLAN > Access**) or
 - b. The Wired profile (**More > Wired > Edit > Edit Wired Network > Access**) window.
2. Select the role for which you want to configure the access rules.

3. In the **Access rules** section, click **New** to add a new rule. The **New Rule** window is displayed.
4. Ensure that the rule type is set to **Access Control**.
5. To configure access to applications or application category, select a service category from the following list:
 - Application
 - Application category
6. Based on the selected service category, configure the following parameters:

Table 58: Access Rule Configuration Parameters

Service Category	Description
Application	Select the applications to which you want to allow or deny access.
Application category	<p>Select any of the following application categories to which you want to allow or deny access:</p> <ul style="list-style-type: none"> • antivirus • authentication • cloud-file-storage • collaboration • encrypted • enterprise-apps • gaming • im-file-transfer • instant-messaging • mail-protocols • mobile-app-store • network-service • peer-to-peer • social-networking • standard • streaming • thin-client • tunneling • unified-communications • web • Webmail
Application Throttling	<p>Application throttling allows you to set a bandwidth limit for an application, application category, web category, or for sites based on their web reputation. For example, you can limit the bandwidth rate for video streaming applications such as YouTube or Netflix, or assign a low bandwidth to high-risk sites. If your OAW-IAP model does not support configuring access rules based on application or application category, you can create a rule based on web category or website reputation and assign bandwidth rates.</p> <p>To specify a bandwidth limit:</p>

Table 58: Access Rule Configuration Parameters

Service Category	Description
	<ol style="list-style-type: none"> 1. Select the Application Throttling check box. 2. Specify the downstream and upstream rates in Kbps.
Action	<p>Select any of following actions:</p> <ul style="list-style-type: none"> • Select Allow to allow access to users based on the access rule. • Select Deny to deny access to users based on the access rule. • Select Destination-NAT to allow changes to destination IP address. • Select Source-NAT to allow changes to the source IP address. <p>The destination-NAT and source-NAT actions apply only to the network services rules.</p>
Destination	<p>Select a destination option for the access rules for network services, applications, and application categories. You can allow or deny access to any the following destinations based on your requirements.</p> <ul style="list-style-type: none"> • to all destinations—Access is allowed or denied to all destinations. • to a particular server—Access is allowed or denied to a particular server. After selecting this option, specify the IP address of the destination server. • except to a particular server—Access is allowed or denied to servers other than the specified server. After selecting this option, specify the IP address of the destination server. • to a network—Access is allowed or denied to a network. After selecting this option, specify the IP address and netmask for the destination network. • except to a network—Access is allowed or denied to networks other than the specified network. After selecting this option, specify the IP address and netmask of the destination network. • to domain name—Access is allowed or denied to the specified domains. After selecting this option, specify the domain name in the Domain Name text box. • to master IP—Access is allowed or denied to the master IP address.
Log	<p>Select this check box to create a log entry when this rule is triggered. AOS-W Instant supports firewall-based logging function. Firewall logs on the OAW-IAPs are generated as security logs.</p>
Blacklist	<p>Select the Blacklist check box to blacklist the client when this rule is triggered. The blacklisting lasts for the duration specified in Auth failure blacklist time on the Blacklisting tab of the Security window. For more information, see Blacklisting Clients on page 174.</p>

Table 58: Access Rule Configuration Parameters

Service Category	Description
Disable scanning	Select Disable scanning check box to disable ARM scanning when this rule is triggered. The selection of the Disable scanning applies only if ARM scanning is enabled. For more information, see Configuring Radio Settings on page 258 .
DSCP tag	Select the DSCP tag check box to specify a DSCP value to prioritize traffic when this rule is triggered. Specify a value within the range of 0–63. To assign a higher priority, specify a higher value.
802.1p priority	Select the 802.1p priority check box to specify an 802.1p priority. Specify a value between 0 and 7. To assign a higher priority, specify a higher value.

3. Click **OK** and then click **Finish**.

In the CLI

To configure access rules:

```
(Instant AP) (config)# wlan access-rule <access-rule-name>
(Instant AP) (Access Rule <Name>)#rule <dest> <mask> <match/invert> {app <app> {permit|deny}
|appcategory <appgrp>} [<option1...option9>]
(Instant AP) (Access Rule <Name>)# end
(Instant AP)# commit apply
```

Example

The following CLI example shows hoe to configure employee access rules:

```
(Instant AP) (config)# wlan access-rule employee
(Instant AP) (Access Rule "employee")# rule any any match app youtube permit throttle-
downstream 256 throttle-up 256
(Instant AP) (Access Rule "employee")# rule any any match appcategory collaboration permit
(Instant AP) (Access Rule "employee")# end
(Instant AP)# commit apply
```

Configuring Web Policy Enforcement Service

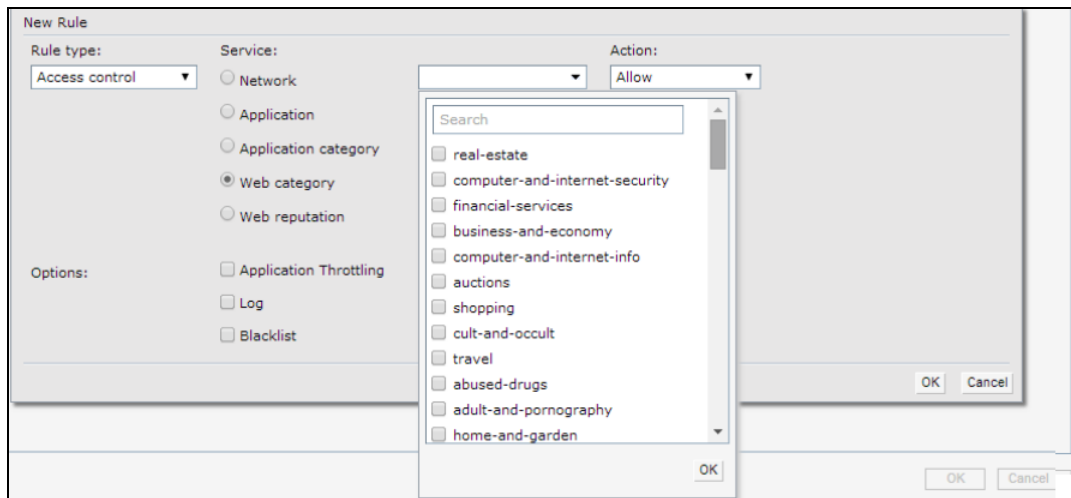
You can configure the WPE service on an OAW-IAP to block certain categories of websites based on your organization specifications by defining ACL rules by using the AOS-W Instant UI or the CLI.

In the AOS-W Instant UI

To configure WPE service:

1. Navigate to **Security > Roles**.
2. Select any WLAN SSID or wired profile role, and click **New** in the Access Rules section.
3. Select the rule type as **Access Control**.
4. To set an access policy based on the web category:
 - a. Under **Service**, select **Web category** and expand the **Web categories** drop-down list.

Figure 71 Web Policy Enforcement



- b. Select the categories to which you want to deny or allow access. You can also search for a web category and select the required option.
 - c. From the **Action** drop-down list, select **Allow** or **Deny** as required.
 - d. Click **OK**.
5. To filter access based on the security ratings of the website:
- a. Select **Web reputation** under **Service**.
 - b. Move the slider to the required security rating level. Move the slider to select a specific web reputation value to deny access to websites with a reputation value lower than or equal to the configured value or to permit access to websites with a reputation value higher than or equal to the configured value. The following options are available:
 - Trustworthy—These are well known sites with strong security practices and may not expose the user to security risks. There is a very low probability that the user will be exposed to malicious links or payloads.
 - Low risk—These are benign sites and may not expose the user to security risks. There is a low probability that the user will be exposed to malicious links or payloads.
 - Moderate risk—These are generally benign sites, but may pose a security risk. There is some probability that the user will be exposed to malicious links or payloads.
 - Suspicious—These are suspicious sites. There is a higher than average probability that the user will be exposed to malicious links or payloads.
 - High risk—These are high-risk sites. There is a high probability that the user will be exposed to malicious links or payloads.
 - c. From the **Action** drop-down list, select **Allow** or **Deny** as required.



For a complete list of categories and information about each of these categories, visit the BrightCloud® Security Services web page at <http://www.brightcloud.com/tools/change-request-url-ip.php>.

6. To set a bandwidth limit based on web category or web reputation score, select **Application Throttling** check box and specify the downstream and upstream rates in Kbps. For example, you can set a higher bandwidth for trusted sites and a low bandwidth rate for high-risk sites.
7. If required, select the following check boxes :
 - Log
 - Blacklist
 - Disable scanning

- DSCP tag
- 802.1p priority

8. Click **OK** on the **Roles** tab to save the changes to the role for which you defined ACL rules.

In the CLI

To control access based on web categories and security ratings:

```
(Instant AP) (config)# wlan access-rule <access_rule>
(Instant AP) (Access Rule "<access-rule>")# rule <dest> <mask> <match> webcategory <webgrp>
{permit | deny}[<option1...option9>]
(Instant AP) (Access Rule "<access-rule>")# rule <dest> <mask> <match> webreputation <webrep>
{permit | deny}[<option1...option9>]
(Instant AP) (Access Rule "<access-rule>")# end
(Instant AP)# commit apply
```

Example

The following CLI example shows how to set access rules based on the web category and the web reputation:

```
(Instant AP) (config)# wlan access-rule URLFilter
(Instant AP) (Access Rule "URLFilter")# rule any any match webcategory gambling deny
(Instant AP) (Access Rule "URLFilter")# rule any any match webcategory training-and-tools
permit
(Instant AP) (Access Rule "URLFilter")# rule any any match webreputation suspicious-sites deny
(Instant AP) (Access Rule "URLFilter")# end
(Instant AP)# commit apply
```

This chapter explains the steps required to configure voice and video services on an OAW-IAP for Voice over IP (VoIP) devices, Session Initiation Protocol (SIP), Spectralink Voice Priority (SVP), H323, SCCP, Vocera, and Alcatel NOE phones, clients running Microsoft OCS, and Apple devices running the Facetime application.

This section includes the following topics:

- [Wi-Fi Multimedia Traffic Management on page 275](#)
- [Media Classification for Voice and Video Calls on page 278](#)
- [Enabling Enhanced Voice Call Tracking on page 279](#)

Wi-Fi Multimedia Traffic Management

Wi-Fi Multimedia (WMM) is a Wi-Fi Alliance specification based on the IEEE 802.11e wireless Quality of Service (QoS) standard. WMM works with 802.11a, 802.11b, 802.11g, and 802.11n physical layer standards.

WMM supports the following access categories (ACs):

- Voice
- Video
- Best effort
- Background

The following table shows the mapping of the WMM access categories to 802.1p priority values. The 802.1p priority value is contained in a two-byte QoS control field in the WMM data frame.

Table 59: *WMM AC to 802.1p Priority Mapping*

802.1p Priority	WMM Access Category
1	Background
2	
0	Best effort
3	
4	Video
5	
6	Voice
7	

In a non-WMM or hybrid environment, where some clients are not WMM-capable, you can configure an SSID with higher values for best effort and voice ACs, to allocate a higher bandwidth to clients transmitting best effort and voice traffic.

Configuring WMM for Wireless Clients

You can configure WMM for wireless clients by using the UI or the CLI.

In the AOS-W Instant UI

To configure the WMM for wireless clients:

1. Navigate to the WLAN wizard.
 - a. Click **Networks > New** or
 - b. Click **Networks**, and select the **WLAN SSID > edit**.
2. Click **Show advanced options** under **WLAN Settings**.
3. Specify a percentage value for the following WMM access categories in the corresponding **Share** text box. You can allocate a higher bandwidth for voice and video traffic than that for other types of traffic based on the network profile.
 - **Background WMM**—Allocates bandwidth for background traffic such as file downloads or print jobs.
 - **Best effort WMM**—Allocates bandwidth or best effort traffic such as traffic from legacy devices or traffic from applications or devices that do not support QoS.
 - **Video WMM**—Allocates bandwidth for video traffic generated from video streaming.
 - **Voice WMM**—Allocates bandwidth for voice traffic generated from the incoming and outgoing voice communication.
4. Click **Next** and complete the configuration as required.

In the CLI

Configuring WMM for wireless clients:

```
(Instant AP) (config)# wlan ssid-profile <name>
(Instant AP) (SSID Profile <name>)# wmm-background-share <share>
(Instant AP) (SSID Profile <name>)# wmm-best-effort-share <share>
(Instant AP) (SSID Profile <name>)# wmm-video-share <share>
(Instant AP) (SSID Profile <name>)# wmm-voice-share <share>
(Instant AP) (SSID Profile <name>)# end
(Instant AP)# commit apply
```

Mapping WMM ACs and DSCP Tags

The IEEE 802.11e standard defines the mapping between WMM ACs and Differentiated Services Code Point (DSCP) tags. You can customize the mapping values between WMM ACs and DSCP tags to prioritize various traffic types and apply these changes to a WMM-enabled SSID profile.

DSCP classifies packets based on network policies and rules. The following table shows the default WMM AC to DSCP mappings and the recommended WMM AC to DSCP mappings.

Table 60: WMM AC-DSCP Mapping

DSCP Value	WMM Access Category
8	Background
16	
0	Best effort
24	

Table 60: WMM AC-DSCP Mapping

DSCP Value	WMM Access Category
32	Video
40	
48	Voice
56	

By customizing WMM AC mappings, all packets received are matched against the entries in the mapping table and prioritized accordingly. The mapping table contains information for upstream (client to OAW-IAP) and downstream (OAW-IAP to client) traffic.

You can configure different WMM to DSCP mapping values for each WMM AC when configuring an SSID profile by using the AOS-W Instant UI or the CLI.

In the AOS-W Instant UI

To configure DSCP mapping values:

1. Navigate to the WLAN wizard.
 1. Click **Network > New** or
 2. Click **Network**, and select the **WLAN SSID > edit**.
2. Click **Show advanced options** under **WLAN Settings**.
3. Specify the appropriate DSCP mapping value within a range of 0–63 for the following access categories in the **DSCP mapping** text box:
 - **Background WMM**—DSCP mapping for the background traffic.
 - **Best effort WMM**—DSCP mapping for the best-effort traffic.
 - **Video WMM**—DSCP mapping for the video traffic.
 - **Voice WMM**—DSCP mapping for the voice traffic.
4. Click **Next** and complete the configuration as required.

In the CLI

Configuring DSCP settings on an SSID:

```
(Instant AP) (config)# wlan ssid-profile <name>
(Instant AP) (SSID Profile <name>)# wmm-background-dscp <dscp>
(Instant AP) (SSID Profile <name>)# wmm-best-effort-dscp <dscp>
(Instant AP) (SSID Profile <name>)# wmm-video-dscp <dscp>
(Instant AP) (SSID Profile <name>)# wmm-voice-dscp <dscp>
(Instant AP) (SSID Profile <name>)# end
(Instant AP)# commit apply
```

You can configure up to 8 DSCP mappings values within the range of 0-63. You can also configure a combination of multiple values separated by a comma, for example, **wmm-voice-dscp 46,44,42,41**.

Configuring WMM U-APSD

To extend the battery life and enable power saving on WLAN clients, OAW-IAPs support Unscheduled Automatic Power Save Delivery (U-APSD) for the clients that support WMM. The U-APSD or the WMM Power Save feature is enabled by default on all SSIDs. When configured, U-APSD enables a client station to retrieve the unicast QoS traffic buffered in the OAW-IAP by sending trigger frames. During the association or reassociation with the OAW-IAP, the station indicates the WMM Access Categories for which U-APSD is enabled. In the current release, OAW-IAPs support U-APSD on all WMM ACs.

To disable U-APSD on an SSID:

```
(Instant AP) (config)# wlan ssid-profile <ssid_profile>
(Instant AP) (SSID Profile "<ssid_profile>")# wmm-uapsd-disable
(Instant AP) (SSID Profile "<ssid_profile>")# end
(Instant AP)# commit apply
```

To re-enable U-APSD on an SSID:

```
(Instant AP) (config)# wlan ssid-profile <ssid_profile>
(Instant AP) (SSID Profile "<ssid_profile>")# no wmm-uapsd-disable
(Instant AP) (SSID Profile "<ssid_profile>")# end
(Instant AP)# commit apply
```

Media Classification for Voice and Video Calls

AOS-W Instant supports the following media classification types:

- [Classify Media Flag](#)
- [STUN Based Media Classification](#)

Classify Media Flag

Voice and video devices use a signaling protocol to establish, control, and terminate voice and video calls. These control or signaling sessions are usually permitted using predefined ACLs. If the control signaling packets are encrypted, the OAW-IAP cannot determine the dynamic ports that are used for voice or video traffic. In these cases, the OAW-IAP has to use an ACL with the classify-media option enabled to identify the voice or video flow based on a deep packet inspection and analysis of the actual traffic. AOS-W Instant identifies and prioritizes voice and video traffic from applications such as Skype for Business, Apple Facetime, and Jabber.

Skype for Business uses Session Initiation Protocol (SIP) over TLS or HTTPS to establish, control, and terminate voice and video calls. Apple Facetime uses Extensible Messaging and Presence Protocol (XMPP) over TLS or HTTPS for these functions.

The following CLI example shows the media classification for VoIP calls:

```
(Instant AP) (config)# wlan access-rule example_s4b_test
(Instant AP) (example_s4b_test)# rule alias <domain_name_for_S4B_server> match tcp 443 443
permit log classify-media
(Instant AP) (example_s4b_test)# rule any any match tcp 5060 5060 permit log classify-media
(Instant AP) (example_s4b_test)# rule any any match tcp 5061 5061 permit log classify-media
(Instant AP) (example_s4b_test)# rule any any match tcp 5223 5223 permit log classify-media
(Instant AP) (example_s4b_test)# rule any any match any any any permit
(Instant AP) (example_s4b_test)# end
(Instant AP)# commit apply
```

STUN Based Media Classification

STUN based media classification requires the ACLs permitting signaling sessions without the **classify-media** flag. However, it requires an implicit deny firewall rule for User Datagram Protocol (UDP) to be activated. All other traffic that should be allowed in the network must be explicitly configured using ACL rules. The OAW-IAP automatically allows firewall sessions for voice and video calls made from Skype for Business and Apple Facetime. For all other S4B and Facetime applications like desktop sharing and file transfer, the corresponding ports must be explicitly opened by using ACL rules.

Before media transmission, a VOIP client initiates a Session Traversal Utilities for NAT (STUN) connectivity check. Sessions created by STUN are subjected to media classification that classifies the media as Real-time Transport Protocol (RTP) or non-RTP. The firewall automatically allows the RTP session on the OAW-IAP and denies the non-RTP sessions.

The following CLI example shows the STUN based media classification for Skype for Business:

```
(Instant AP) (config)#wlan access-rule example_s4b_test
(Instant AP) (example_s4b_test)# rule alias <domain_name_for_S4B_server> match tcp 443 443
permit
(Instant AP) (example_s4b_test)# rule any any match tcp 5223 5223 permit
(Instant AP) (example_s4b_test)# rule any any match tcp 5061 5061 permit
(Instant AP) (example_s4b_test)# rule any any match any any any deny
(Instant AP) (example_s4b_test)# end
(Instant AP)# commit apply
```



The Type of Service (ToS) values for calls prioritized using the above mentioned media classification types will always carry a ToS of 40 for a voice session and 48 for a video session.

Enabling Enhanced Voice Call Tracking

AOS-W Instant provides seamless support for tracking VoIP calls in the network by using SNMP to send the location details of the caller to the third-party server. This feature is currently applied for tracking Emergency 911 (E911) VoIP calls.

The Master OAW-IAP identifies the location from where the VoIP call was placed and sends the details of the location to the third-party SNMP server. You must configure the third-party server as an SNMP host and enable SNMP traps to activate the voice call tracking feature on the OAW-IAP. For more information on configuring a third-party server as an SNMP host, see [Configuring SNMP on page 362](#).

The Master OAW-IAP will send the WLSXIAPVOICECLIENTLOCATIONUPDATE SNMP trap under the following scenarios:

- The VoIP call is successful.
- The VoIP client roams from one OAW-IAP to another during an active call, the Master OAW-IAP will identify the VoIP client and send out the WLSXIAPVOICECLIENTLOCATIONUPDATE trap to the emergency call server.



The trap sending feature is not supported for L3 mobility.

The WLSXIAPVOICECLIENTLOCATIONUPDATE trap contains the following information:

Table 61: *SNMP Trap Details for VoIP Calls*

Parameter	Description
<i>wlsxTrapVclpAddress</i>	IP address of the VoIP client.
<i>wlsxTrapVcMacAddress</i>	MAC address of the VoIP client.
<i>wlsxTrapAPMacAddress</i>	MAC address of the OAW-IAP which generated the trap.
<i>wlsxTrapAPName</i>	Name of the OAW-IAP which generated the trap.

SNMP GET

In order to find the location of a particular emergency caller, the third-party SNMP server sends a query to the Master OAW-IAP using SNMP GET. The Master OAW-IAP responds back to the SNMP server with the location (OAW-IAP Name) of the VoIP caller. Following are the key parameters in the response sent by the Master OAW-IAP:

- VoIP Client IP Address
- VoIP Client MAC Address
- OAW-IAP MAC Address
- OAW-IAP Name

This chapter provides information on how to configure the following services on an OAW-IAP:

- [Configuring AirGroup on page 281](#)
- [Configuring an OAW-IAP for RTLS Support on page 290](#)
- [Configuring an OAW-IAP for Analytics and Location Engine Support on page 291](#)
- [Managing BLE Beacons on page 292](#)
- [Clarity Live on page 293](#)
- [Cluster Security on page 306](#)
- [Configuring OpenDNS Credentials on page 295](#)
- [Integrating an OAW-IAP with Palo Alto Networks Firewall on page 295](#)
- [Integrating an OAW-IAP with an XML API Interface on page 297](#)
- [CALEA Integration and Lawful Intercept Compliance on page 300](#)

Configuring AirGroup

AirGroup provides a unique enterprise-class capability that leverages zero configuration networking to enable AirGroup services from mobile devices efficiently. Zero configuration networking enables service discovery, address assignment, and name resolution for desktop computers, mobile devices, and network services. It is designed for flat, single-subnet IP networks such as wireless networking at home. The users can register their personal devices and define a group of users who can share the registered devices. Administrators can register and manage an organization's shared devices such as printers and grant global access to each device, or restrict access according to the username, role, or user location.

In large universities and enterprise networks, it is common for devices to connect to the network across VLANs. As a result, user devices on a specific VLAN cannot discover a service that resides on another VLAN. As the addresses used by the protocol are link-scope multicast addresses, each query or advertisement can only be forwarded on its respective VLAN, but not across different VLANs. Broadcast and multicast traffic are usually filtered out from a wireless LAN network to preserve the airtime and battery life. This inhibits the performance of AirGroup services that rely on multicast traffic. Alcatel-Lucent addresses this challenge with AirGroup technology.

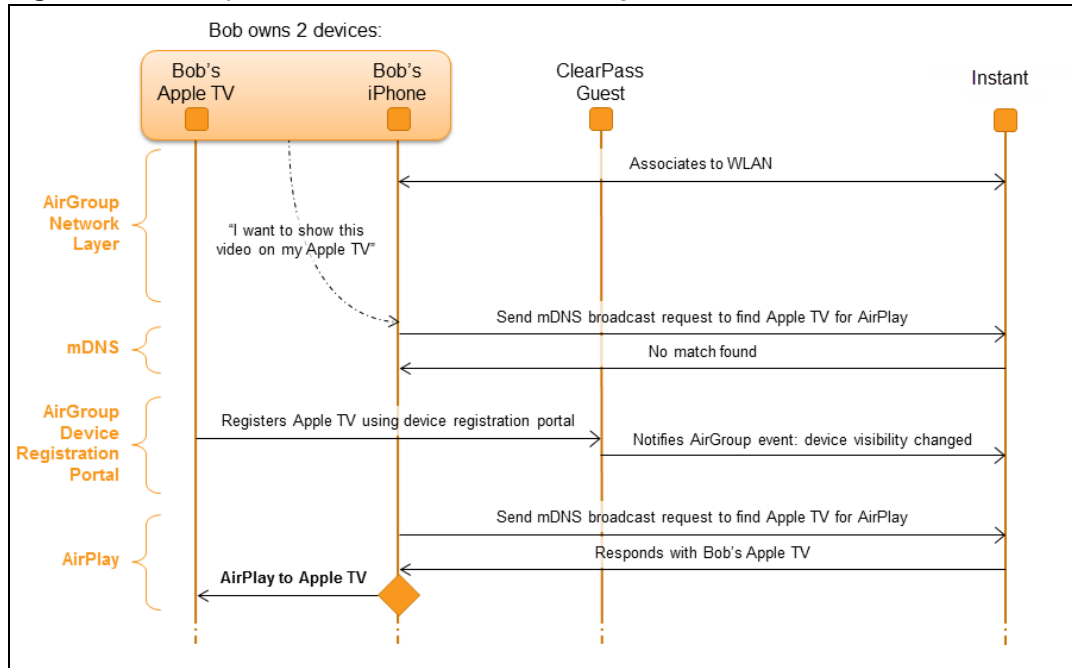
The distributed AirGroup architecture allows each OAW-IAP to handle multicast DNS (mDNS) and Digital Living Network Alliance (DLNA) queries and responses individually instead of overloading a VC with these tasks. This results in a scalable AirGroup solution.

The AirGroup solution supports both wired and wireless devices. An AirGroup device can be registered by an administrator or a guest user.

1. The AirGroup administrator gives an end user the AirGroup operator role, which authorizes the user to register the client devices on the ClearPass Policy Manager platform.
2. OAW-IAPs maintain information for all AirGroup services. OAW-IAP queries ClearPass Policy Manager to map each device's access privileges to the available services and responds to the query made by a device based on contextual data such as user role, username, and location.

The following figure illustrates how AirGroup enables personal sharing of Apple devices:

Figure 72 AirGroup Enables Personal Device Sharing



AirGroup is not supported on 3G and PPPoE uplinks.

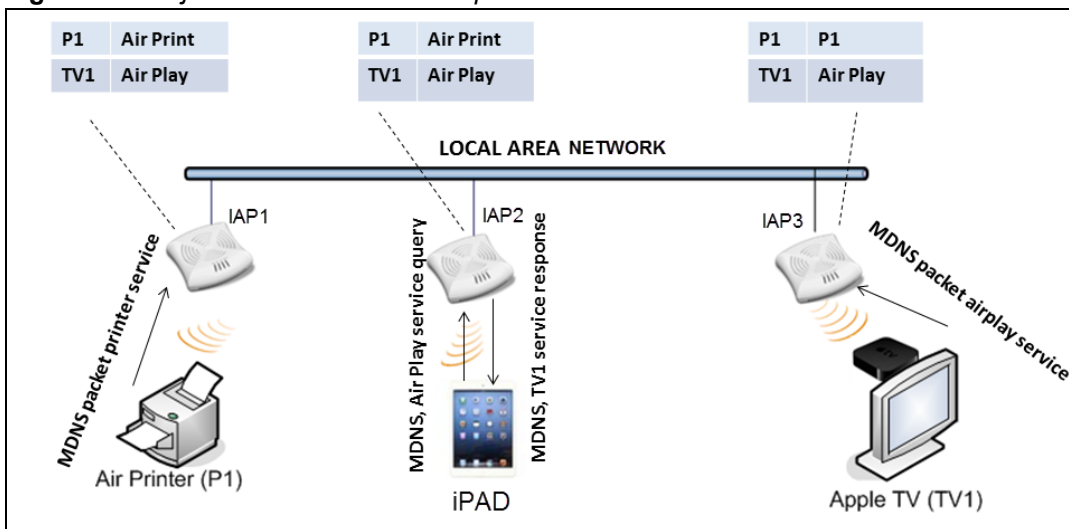
Multicast DNS and Bonjour® Services

Bonjour is the trade name for the zero configuration implementation introduced by Apple. It is supported by most of the Apple product lines, including the Mac OS X operating system, iPhone, iPod Touch, iPad, Apple TV, and AirPort Express. Apple AirPlay and AirPrint services are based on the Bonjour protocol and are essential services in campus Wi-Fi networks.

Bonjour can be installed on computers running Microsoft Windows® and is supported by the new network-capable printers. Bonjour is also included with popular software programs such as Apple iTunes, Safari, and iPhoto. Bonjour uses multicast DNS (mDNS) to locate devices and the services offered by these devices.

As shown in the following figure, the OAW-IAP1 discovers AirPrint (P1) and OAW-IAP3 discovers Apple TV (TV1). OAW-IAP1 advertises information about its connected P1 device to the other OAW-IAPs that is OAW-IAP2 and OAW-IAP3. Similarly, OAW-IAP3 advertises TV1 device to OAW-IAP1 and OAW-IAP2. This type of distributed architecture allows any OAW-IAP to respond to its connected devices locally. In this example, the iPad connected to OAW-IAP2 obtains direct response from the same OAW-IAP about the other Bonjour-enabled services in the network.

Figure 73 Bonjour Services and AirGroup Architecture



For a list of supported Bonjour services, see [AirGroup Services on page 285](#).

DLNA UPnP Support

In addition to the mDNS protocol, OAW-IAPs now support Universal Plug and Play (UPnP), and DLNA-enabled devices. DLNA is a network standard derived from UPnP, which enables devices to discover the services available in a network. DLNA also provides the ability to share data between the Windows or Android-based multimedia devices. All the features and policies applicable to mDNS are extended to DLNA to ensure full interoperability between compliant devices.

In a UPnP-based scenario, the following types of devices are available in a network:

- Controlled devices (servers)
- Control points (clients)

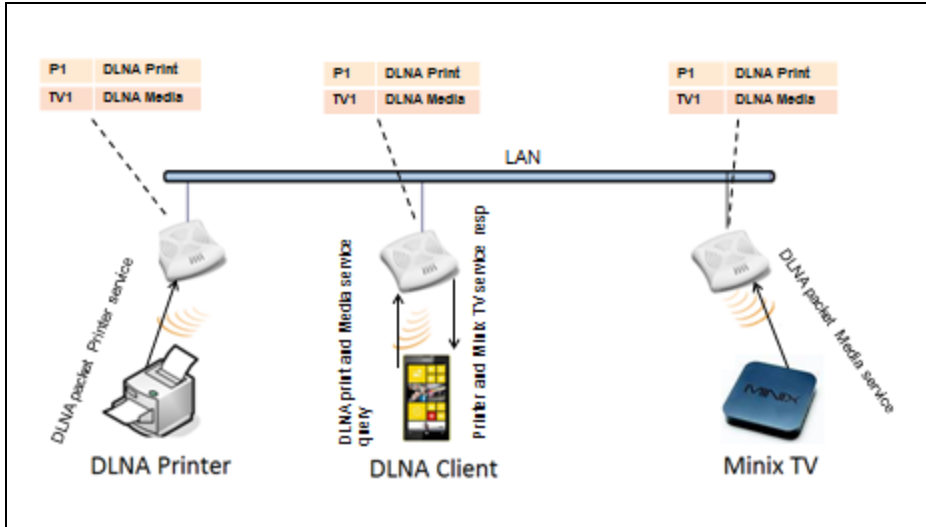
When a controlled device joins a network and acquires IP address, it multicasts a number of discovery messages for advertising itself, its embedded devices, and services. On the other hand, when a control point joins a network, it may multicast a search discovery message for finding interesting devices and services. The devices listening on the multicast address respond if they match the search criteria in the search message.

In a single OAW-IAP network, the OAW-IAP maintains a cache table containing the list of discovered services in the network. The OAW-IAP also enforces native policies such as disallowing roles and VLANs and the policies defined on ClearPass Policy Manager to determine the devices or services that are allowed and can be discovered in the network. Whenever a search request comes, the OAW-IAP looks up its cache table and filters the cached data, based on configured policies, then builds a search response, and unicasts it to the requesting device.

In an OAW-IAP cluster, the OAW-IAPs maintain a list of associated UPnP devices and allow the discovery of the associated devices.

The following figure illustrates DLNA UPnP Services and AirGroup Architecture.

Figure 74 DLNA UPnP Services and AirGroup Architecture



For a list of supported DLNA services, see [AirGroup Services](#) on page 285.

AirGroup Features

AirGroup supports the following features:

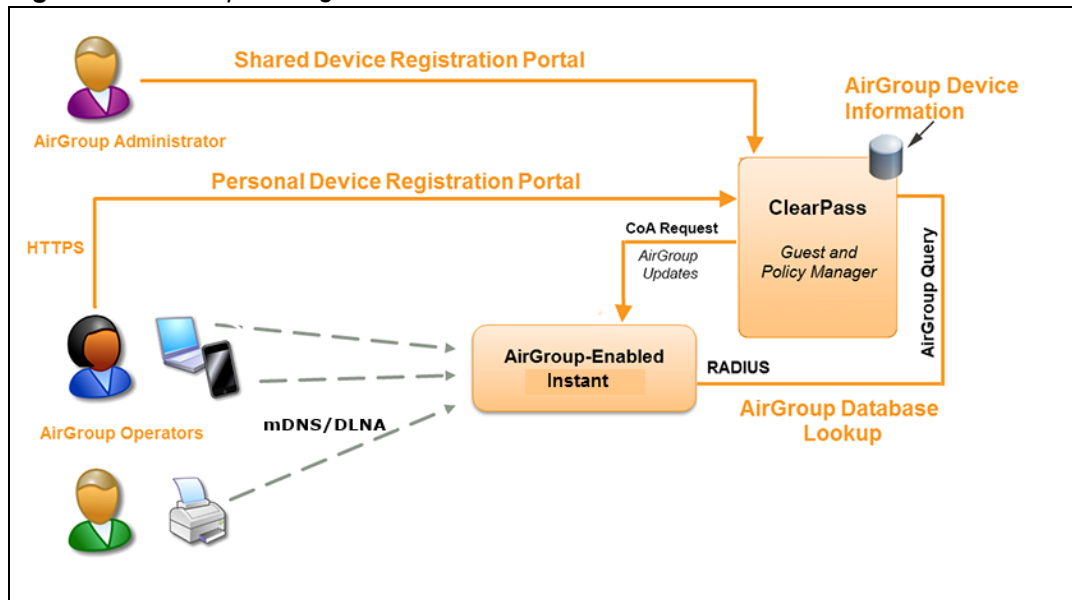
- Sends unicast responses to mDNS or DLNA queries and reduces the traffic footprint.
- Ensures cross-VLAN visibility and availability of AirGroup devices and services.
- Allows or blocks AirGroup services for all users.
- Allows or blocks AirGroup services based on user roles.
- Allows or blocks AirGroup services based on VLANs.
- Matches devices to their closest services such as printers.

AirGroup also enables context awareness for services across the network:

- AirGroup is aware of personal and shared devices. For example, an Apple TV in a dorm room can be associated with the student who owns it or an Apple TV in a meeting room or a printer in a supply room that is available to certain users, such as the marketing department.
- AirGroup is aware of the location of services when ClearPass Policy Manager support is enabled. For example, depending on the proximity, a user would be presented with the closest printer instead of all the printers in the building.
- When configured, AirGroup enables a client to perform a location-based discovery. For example, when a client roams from one AOS-W Instant cluster to another, it can discover devices available in the new cluster to which the client is currently connected.

The following figure shows an example of a higher-education environment with shared, local, and personal services available to mobile devices.

Figure 75 *AirGroup in a Higher-Education Environment*



When AirGroup discovers a new device, it interacts with ClearPass Policy Manager to obtain the shared attributes such as shared location and role. However, the current versions of OAW-IAPs do not support the enforcement of shared location policy.

AirGroup Services

AirGroup supports zero configuration services. The services are preconfigured and are available as part of the factory default configuration. The administrator can also enable or disable any or all services by using the AOS-W Instant UI or the CLI.

The following services are available for OAW-IAP clients:

- AirPlay™—Apple® AirPlay allows wireless streaming of music, video, and slide shows from your iOS device to Apple TV® and other devices that support the AirPlay feature.
- AirPrint™—Apple AirPrint allows you to print from an iPad®, iPhone®, or iPod® Touch directly to any AirPrint-compatible printers.
- iTunes—The iTunes service is used by iTunes Wi-Fi sync and iTunes home-sharing applications across all Apple devices.
- RemoteMgmt—The RemoteMgmt service allows remote login, remote management, and FTP utilities on Apple devices.
- Sharing—The Sharing service allows applications such as disk sharing and file sharing among Apple devices.
- Chat—The iChat® (Instant Messenger) application on Apple devices uses this service.
- ChromeCast—The ChromeCast service allows you to use a ChromeCast device to play audio or video content on a high-definition television by streaming content through Wi-Fi from the Internet or local network.
- DLNA Media—Applications such as Windows Media Player use this service to browse and play media content on a remote device.
- DLNA Print—This service is used by printers that support DLNA.



In the AOS-W Instant 6.4.0.2-4.1.0.0 release, it is recommended to have a maximum of upto 80 AirGroup servers in the network.

For more information on configuring AirGroup services, see [Configuring AirGroup and AirGroup Services on an OAW-IAP on page 287](#).

AirGroup Components

AirGroup leverages key elements of the Alcatel-Lucent solution portfolio including operating system software for AOS-W Instant, ClearPass Policy Manager, and the VLAN-based or role-based filtering options offered by the AirGroup services. The components that make up the AirGroup solution include the AOS-W Instant, ClearPass Policy Manager, and ClearPass Guest. The version requirements are described in the following table:

Table 62: AOS-W Instant, ClearPass Policy Manager, and ClearPass Guest Requirements

Component	Minimum Version for mDNS Services	Minimum Version for DLNA Services
AOS-W Instant	AOS-W Instant 6.2.0.0-3.2.0.0	AOS-W Instant 6.4.0.2-4.1.0.0
ClearPass Policy Manager software	ClearPass Policy Manager 5.2	ClearPass Policy Manager 6.2
ClearPass Guest Services plugin	ClearPass Guest 6.2.0	ClearPass Guest 6.3.0



Starting from ClearPass Policy Manager version 6.0, the ClearPass Guest and the AirGroup Services plug-in are integrated into a single platform.

AirGroup maintains seamless connectivity between clients and services across VLANs and SSIDs. The following table summarizes the filtering options supported by AOS-W Instant:

Table 63: AirGroup Filtering Options

Features	AOS-W Instant Deployment Models	
	Integrated with ClearPass Guest	Integrated with ClearPass Policy Manager
Allow mDNS and DLNA traffic to propagate across subnets/VLANs	Yes	Yes
Limit mDNS and DLNA traffic on the network	Yes	Yes
VLAN-based AirGroup service policy enforcement	Yes	Yes
User-role-based AirGroup service policy enforcement	Yes	Yes
Portal to self-register personal devices	No	Yes
Device-owner-based policy enforcement	No	Yes
Shared user-list-based policy enforcement	No	Yes
Shared role-list based-policy enforcement	No	Yes

ClearPass Policy Manager and ClearPass Guest Features

ClearPass Policy Manager and ClearPass Guest support the following features:

- Registration portal for WLAN users to register their personal devices.
- Registration portal for WLAN administrators to register shared devices.
- Operator-defined *personal* AirGroup to specify a list of other users who can share devices with the operator.
- Administrator-defined username, user role, and location attributes for shared devices.

Configuring AirGroup and AirGroup Services on an OAW-IAP

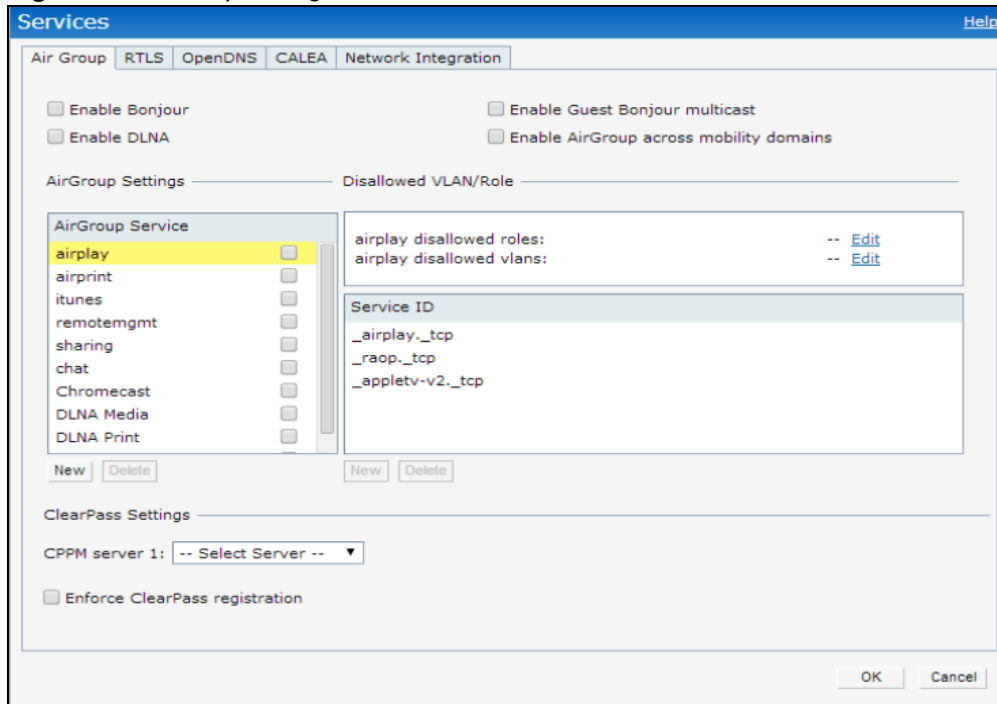
You can configure AirGroup services by using the AOS-W Instant UI or the CLI.

In the AOS-W Instant UI

To enable AirGroup and its services:

1. Click the **More > Services** link on the AOS-W Instant main window.
2. Click the **Air Group** tab.

Figure 76 AirGroup Configuration



3. To enable support for Bonjour services, select the **Enable Bonjour** check box and select the AirGroup services related to Bonjour as required.
4. To enable DLNA support, select the **Enable DLNA** check box and select the DLNA services.
5. To allow the users to use Bonjour services enabled in a guest VLAN, select **Enable Guest Bonjour multicast**. When this check box is enabled, the Bonjour devices are visible only in the guest VLAN and AirGroup will not discover or enforce policies in guest VLAN.
6. Select the **Enable Air Group across mobility domains** check box to enable inter-cluster mobility. When enabled, the OAW-IAP shares the mDNS database information with the other clusters. The DNS records in the VC can be shared with all the VC configured for L3 Mobility.

By default, this feature is disabled. To define clusters, go to the **System > L3 Mobility** tab.

7. Ensure that the required AirGroup services are selected. To add any service, click **New** and add. To allow all services, select **allowall**. If a custom service is added, you can add a corresponding service ID by clicking **New** under **Service ID**.



If an OAW-IAP is upgraded to the current release with the **Bonjour** check box enabled, ensure that the corresponding Bonjour services are selected.

AOS-W Instant supports the use of up to 6 custom services.

8. Based on the services configured, you can block any user roles from accessing an AirGroup service and restrict the AirGroup servers connected to a specific set of VLANs from being discovered. The user roles and VLANs marked as disallowed are prevented from accessing the corresponding AirGroup service. You can create a list of disallowed user roles and VLANs for all AirGroup services configured on the OAW-IAP. For example, if the AirPlay service is selected, the **edit** links for the **airplay disallowed roles** and **airplay disallowed vlans** are displayed. Similarly, if sharing service is selected, the **edit** links for the **sharing disallowed roles** and **sharing disallowed vlans** are displayed.
 - To block user roles from accessing an AirGroup service, click the corresponding **edit** link and select the user roles for which you want to restrict access. By default, an AirGroup service is accessible by all user roles configured in your OAW-IAP cluster.
 - To block VLANs from allowing access to an AirGroup service, click the corresponding **edit** link and select the VLANs to exclude. By default, the AirGroup services are accessible by users or devices in all VLANs configured in your OAW-IAP cluster.
9. **ClearPass Settings**—Use this section to configure the ClearPass Policy Manager server, CoA server, and enforce ClearPass registering.
 - **CPPM server 1**—Indicates the ClearPass Policy Manager server information for AirGroup policy.
 - **Enforce ClearPass registering**—When enabled, only devices registered with ClearPass Policy Manager will be discovered by Bonjour devices, based on the ClearPass Policy Manager policy.

In the CLI

To configure AirGroup:

```
(Instant AP) (config) # airgroup
(Instant AP) (airgroup) # enable [dlna-only | mdns-only]
(Instant AP) (airgroup) # cppm enforce-registration
(Instant AP) (airgroup) # cppm-server <server>
(Instant AP) (airgroup) # cppm-query-interval <interval>
(Instant AP) (airgroup) # disallow-vlan <vlan-ID>
(Instant AP) (airgroup) # enable-guest-multicast
(Instant AP) (airgroup) # multi-swarm
(Instant AP) (airgroup) # end
(Instant AP) # commit apply
```

To enable DLNA support:

```
(Instant AP) (config) # airgroup
(Instant AP) (airgroup) # enable dlna-only
(Instant AP) (airgroup) # end
(Instant AP) # commit apply
```

To enable support for Bonjour services:

```
(Instant AP) (config) # airgroup
(Instant AP) (config) # enable mdns-only
(Instant AP) (airgroup) # end
(Instant AP) # commit apply
```

To configure AirGroup services:

```
(Instant AP) (config) # airgroupservice <airgroup-service>
```



```
(Instant AP) (airgroup-service) # id <airgroupservice-ID>
(Instant AP) (airgroup-service) # description <text>
(Instant AP) (airgroup-service) # disallow-role <role>
(Instant AP) (airgroup-service) # disallow-vlan <vlan-ID>
(Instant AP) (airgroup-service) # end
(Instant AP) # commit apply
```

To verify the AirGroup configuration status:

```
(Instant AP) # show airgroup status
```

Configuring AirGroup and ClearPass Policy Manager Interface in AOS-W Instant

Configure the AOS-W Instant and ClearPass Policy Manager interface to allow an AirGroup OAW-IAP and ClearPass Policy Manager to exchange information regarding device sharing, and location. The configuration options define the RADIUS server that is used by the AirGroup RADIUS client.

The AirGroup configuration with ClearPass Policy Manager involves the following steps:

1. [Create a RADIUS Server](#)
2. [Assigning a Server to AirGroup](#)
3. [Configuring ClearPass Policy Manager to Enforce Registration](#)
4. [Configuring Change of Authorization \(CoA\)](#)

Creating a RADIUS Server

You can create a RADIUS server in the **Air Group** window. Navigate to **Services > AirGroup > Clear Pass Settings > CPPM server 1 >** and select **New** from the drop-down list.

You can configure an external RADIUS Security window. For more information on configuring ClearPass Policy Manager server, see [Configuring an External Server for Authentication on page 154](#).

Assigning a Server to AirGroup

To associate the ClearPass Policy Manager server with AirGroup, select the ClearPass Policy Manager server from the **CPPM Server 1** drop-down list.



If two ClearPass Policy Manager servers are configured, the CPPM server 1 acts as a primary server and the CPPM server 2 acts as a backup server.

After the configuration is complete, this particular server will be displayed in the CoA server option. To view this server go to **Services > AirGroup > ClearPass Settings > CoA server**.

Configuring ClearPass Policy Manager to Enforce Registration

When ClearPass Policy Manager registration is enforced, the devices registered with ClearPass Policy Manager will be discovered by Bonjour devices, based on the ClearPass Policy Manager policy.

Configuring Change of Authorization (CoA)

When a RADIUS server is configured with Change of Authorization (CoA) with the ClearPass Policy Manager server, the guest users are allowed to register their devices. For more information on configuring RADIUS server with CoA, see [Configuring an External Server for Authentication on page 154](#).



You can also create a **CoA only server** in the **Services > AirGroup > Clear Pass Settings > CoA server** window.

Configuring an OAW-IAP for RTLS Support

AOS-W Instant supports the real-time tracking of devices when integrated with the AMP or a third-party Real Time Location Server such as Aeroscout Real Time Location Server. With the help of the RTLS, the devices can be monitored in real time or through history.

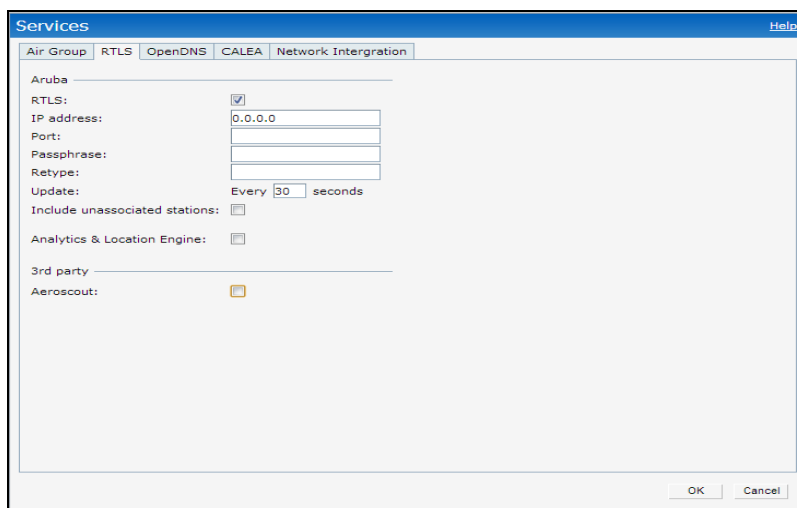
You can configure RTLS by using the AOS-W Instant UI or the CLI.

In the AOS-W Instant UI

To configure Aruba RTLS:

1. Click the **More > Services** link on the AOS-W Instant main window.
2. In the **Services** section, click the **RTLS** tab.
3. Under **Aruba**, select the **RTLS** check box to integrate AOS-W Instant with the AMP or Ekahau Real Time Location Server. The following figure shows the contents of the **RTLS** tab.

Figure 77 RTLS Window



4. Specify the IP address and port to which the location reports must be sent.
5. Specify the shared secret key in the **Passphrase** text box.
6. In the **Update** text box, specify the frequency at which the VC can send updates to the server. You can specify a value within the range of 5-3600 seconds. The default value is 5 seconds.
7. Select the **Include unassociated stations** check box to send reports to the RTLS server about the stations that are not associated to any OAW-IAP.
8. Click **OK**.

To configure third-party RTLS such as Aeroscout:

1. Select the **Aeroscout** check box to send the RFID tag information to an AeroScout RTLS.
2. Specify the IP address and port number of the AeroScout server to which location reports must be sent.
3. Select the **Include unassociated stations** check box to send reports on the stations that are not associated to any OAW-IAP to the Aeroscout RTLS server.
4. Click **OK**.

In the CLI

To configure OmniVista RTLS:

```
(Instant AP) (config)# airwave-rtls <IP-address> <port> <passphrase> <seconds> include-unassoc-  
sta  
(Instant AP) (config)# end
```

```
(Instant AP)# commit apply
```

To configure Aeroscout RTLS:

```
(Instant AP) (config)# aeroscout-rtls <IP-address> <port> include-unassoc-sta  
(Instant AP) (config)# end  
(Instant AP)# commit apply
```

Configuring an OAW-IAP for Analytics and Location Engine Support

The Analytics and Location Engine (ALE) is designed to gather client information from the network, process it, and share it through a standard API. The client information gathered by ALE can be used for business purposes by analyzing a client's Internet behavior such as shopping preferences.

ALE includes a location engine that calculates the associated and unassociated device location every 30 seconds by default. For every device on the network, ALE provides the following information through the Northbound API:

- Client username
- IP address
- MAC address
- Device type
- Application firewall data showing the destinations and applications used by associated devices
- Current location
- Historical location

ALE requires the OAW-IAP placement data to be able to calculate location for the devices in a network.

ALE with AOS-W Instant

The AOS-W Instant 6.3.1.1-4.0 release supports Analytics and Location Engine (ALE). The ALE server acts as a primary interface to all third-party applications and the OAW-IAP sends client information and all status information to the ALE server.

To integrate OAW-IAP with ALE, the ALE server address must be configured on an OAW-IAP. If the ALE server is configured with a host name, the VC performs a mutual certificated-based authentication with the ALE server before sending any information.

Enabling ALE Support on an OAW-IAP

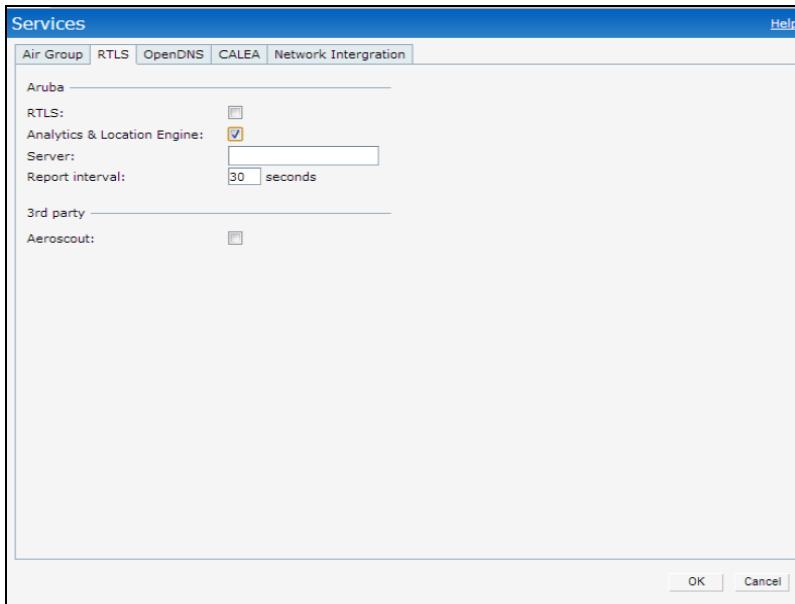
You can configure an OAW-IAP for ALE support by using the AOS-W Instant UI or the CLI.

In the AOS-W Instant UI

Configuring ALE support:

1. Click **More > Services**.
2. Click the **RTLS** tab.
3. Select the **Analytics & Location Engine** check box.

Figure 78 Services Window—ALE Integration



4. In the **Server** text box, specify the ALE server name or IP address.
5. In the **Report interval** text box, specify the reporting interval within the range of 6–60 seconds. The OAW-IAP sends messages to the ALE server at the specified interval. The default interval is 30 seconds.
6. Click **OK**.

In the CLI

To enable OAW-IAP integration with the ALE server:

```
(Instant AP) (config) # ale-server <server-name | IP-address>
(Instant AP) (config) # ale-report-interval <seconds>
(Instant AP) (config) # end
(Instant AP) # commit apply
```

Verifying ALE Configuration on an OAW-IAP

To view the configuration details:

```
(Instant AP) # show ale config
```

To verify the configuration status:

```
(Instant AP) # show ale status
```

Managing BLE Beacons

In AOS-W Instant 6.4.3.4-4.2.1.0, OAW-IAPs support Alcatel-Lucent Bluetooth Low Energy (BLE) devices, such as BT-100 and BT-105, which are used for location tracking and proximity detection. The BLE devices can be connected to an OAW-IAP and are monitored or managed by a cloud-based Beacon Management Console (BMC). The BLE Beacon Management feature allows you to configure parameters for managing the BLE beacons and establishing secure communication with the Beacon Management Console (BMC). You can also configure the BLE operation modes that determine the functions of the built-in BLE chip in the OAW-IAP.



The BLE beacon management and BLE operation mode feature is supported only on OAW-IAP334/335, OAW-IAP314/315, OAW-IAP324/325, OAW-IAP224/225, OAW-IAP205H, and OAW-IAP214/215 devices.

You can configure BLE operation modes and enable the BLE Beacon Management feature by using the AOS-W Instant UI or the CLI.

In the AOS-W Instant UI

Configuring BLE mode:

1. Click **More > Services**.
2. Click the **RTLS** tab. The tab details are displayed.
3. To manage the BLE devices using BMC, select **Manage BLE Beacons**.
4. Enter the authorization token. The authorization token is a text string of 1–255 characters used by the BLE devices in the HTTPS header when communicating with the BMC. This token is unique for each deployment.
5. In **Endpoint URL**, enter the URL of the server to which the BLE sends the monitoring data.
6. Select any of the following options from **Operation Mode** drop-down list:

Table 64: BLE Operation Modes

Mode	Description
Beaconing	The built-in BLE chip of the OAW-IAP functions as an iBeacon combined with the beacon management functionality.
Disabled	The built-in BLE chip of the OAW-IAP is turned off. The BLE operation mode is set to Disabled by default.
DynamicConsole	The built-in BLE chip of the OAW-IAP functions in the beaconing mode and dynamically enables access to OAW-IAP console over BLE when the link to the Local Management Switch (LMS) is lost.
PersistentConsole	The built-in BLE chip of the OAW-IAP provides access to the OAW-IAP console over BLE and also operates in the Beaconing mode.

7. Click **OK**.

In the CLI

To enable BLE beacon management:

```
(Instant AP) (config)# ble config <token> <url>
(Instant AP) (config)# end
(Instant AP)# commit apply
```

To configure a BLE operation mode:

```
(Instant AP) (config)# ble mode <opmode>
(Instant AP) (config)# end
(Instant AP)# commit apply
```

To view the BLE configuration details:

```
(Instant AP)# show ble-config
```

Clarity Live

OAW-IAP provides support for Inline Monitoring support using Clarity Live to identify client connectivity issues and sends user debug data to OmniVista. The client connectivity issues can be a problem with the client, Radius Authentication, DHCP, DNS, or it can be delay in the network. Clarity Live is used to identify the root cause of the problem, this feature can be used.

Inline Monitoring

This functionality of Clarity Live helps diagnose client connectivity issues. It provides the network administrator or engineers with more information regarding the exact stage at which the client connectivity fails or provides data where the dhcp or radius server is slow.

The OAW-IAP collects all information related to user transitions like association, authentication, and dhcp. Then, the OAW-IAP sends these records to a management server like OmniVista. The management server analyzes the data and concludes which dhcp or radius server was not working efficiently causing user connectivity issues. This enhancement allows the management server to isolate WLAN issues caused by external servers such as dhcp or radius.

HTTPS is the data transport protocol used to communicate basic statistics or state changes to OmniVista. Inline Monitoring makes use of HTTPS to send the statistics to OmniVista too.

The following events are used by OAW-IAP to send inline monitoring (Clarity Live) updates to OmniVista:

- **Authentication Failure Events**—The statistics or updates shared as part of this event are related to the management frame. These frames are processed by STM and are collected in the user space.
- **DHCP Failure Events**—In scenarios where the DHCP Server does not respond, information about the failure of the event can be collected by the OAW-IAP with the help of Clarity Live and sent to OmniVista. This functionality receives client DHCP transactions from the control plane.
- **DNS Failure Events**—The OAW-IAP measures the responsiveness of each DNS server with the help of Clarity Live. The monitoring includes minimum, maximum, and average response time of each DNS server. A maximum of 16 DNS servers can be monitored at a time and a maximum of 16 DNS server entries are made in the DNS table. If there are no queries from a particular DNS server for a long period of time, the DNS server entry can be removed and replaced with a new DNS server entry. The statistical data collected for the DNS server will be pushed to OmniVista before the entry is replaced by a new DNS entry.
- **STA Failure Events**—The station passive monitor statistic is generated when enabled on the OAW-IAP. The OAW-IAP generate the data periodically for every 60 seconds and sends it to OmniVista.



All of the above clarity configurations must be enabled or disabled at the same time whether if it is by the AOS-W Instant UI or the CLI. OmniVista will drop the message even if one of the four stats is disabled.

You can configure an OAW-IAP to generate inline monitoring statistics by using the AOS-W Instant UI or the CLI.

In the AOS-W Instant UI

To enable Clarity Live for generating inline monitoring statistics:

1. Click **More > Services**.
2. Click **Clarity**. The configuration options for the Clarity group are displayed.
3. Select the **Inline Auth stats** checkbox to enable the OAW-IAP to generate statistics and update messages for Authentication Failure Events.
4. Select the **Inline DHCP stats** checkbox to enable the OAW-IAP to generate statistics and update messages for DHCP Failure Events.
5. Select the **Inline DNS stats** checkbox to enable the OAW-IAP to generate statistics and update messages for DNS Failure Events.
6. Select the **Inline STA stats** checkbox to enable the OAW-IAP to generate statistics and update messages for STA Failure Events.
7. Click **OK**.

In the AOS-W Instant CLI

To configure inline monitoring statistics using the CLI:

```
(Instant AP) (config)# clarity
(Instant AP) (clarity)# inline-auth-stats
(Instant AP) (clarity)# inline-dhcp-stats
(Instant AP) (clarity)# inline-dns-stats
(Instant AP) (clarity)# inline-sta-stats
(Instant AP) (clarity)# end
(Instant AP) # commit apply
```

Verify Clarity Configuration on OAW-IAP

The following command is used to view the status of the Inline Monitoring events:

```
(Instant AP) # show clarity config
```

The following command is used to view the history of the authentication events:

```
(Instant AP) # show clarity history auth
```

The following command is used to view the history of the DHCP events:

```
(Instant AP) # show clarity history dhcp
```

The following command is used to view the history of the DNS events:

```
(Instant AP) # show clarity history dns
```

Configuring OpenDNS Credentials

When configured, the OpenDNS credentials are used by AOS-W Instant to access OpenDNS to provide enterprise level content filtering. You can configure OpenDNS credentials by using the AOS-W Instant UI or the CLI.

In the AOS-W Instant UI

To configure OpenDNS credentials:

1. Click **More > Services > OpenDNS**.
2. Enter the **Username** and **Password** to enable access to OpenDNS.
3. Click **OK** to apply the changes.

In the CLI

To configure OpenDNS credentials:

```
(Instant AP) (config)# opendns <username> <password>
(Instant AP) (config)# end
(Instant AP) # commit apply
```

Integrating an OAW-IAP with Palo Alto Networks Firewall

Palo Alto Networks (PAN) next-generation firewall offers contextual security for all users for safe enabling of applications. A simple firewall beyond basic IP address or TCP port numbers only provides a subset of the enhanced security required for enterprises to secure their networks. In the context of businesses using social networking sites, legacy firewalls are not able to differentiate valid authorized users from casual social networking users.

The Palo Alto next-generation firewall is based on user ID, which provides many methods for connecting the users to sources of identity information and associating them with firewall policy rules. For example, it provides an option to gather user information from Active Directory or Lightweight Directory Access Protocol (LDAP) server.

Integration with AOS-W Instant

The functionality provided by the PAN firewall based on user ID requires the collection of information from the network. OAW-IAP maintains the network (such as mapping IP address) and user information for its clients in the network and can provide the required information for the user ID on PAN firewall. Before sending the user-ID mapping information to the PAN firewall, the OAW-IAP must retrieve an API key that will be used for authentication for all APIs.

OAW-IAP provides the User ID mapping information to the PAN firewall for integration. The client user id for authentication will not be sent to the PAN firewall unless it has a domain prefix. The OAW-IAP checks for the domain information in the client username for all login and logout requests sent to the PAN firewall. If the user id already has a domain prefix, OAW-IAP forwards the request to the PAN firewall. Otherwise, the static client domain configured in the PAN firewall profile will be prefixed to the user id and then sent to the PAN firewall.

OAW-IAP and PAN firewall integration can be seamless with the XML-API that is available with PAN-OS 5.0 or later.

To integrate an OAW-IAP with PAN user ID, a global profile is added. This profile can be configured on an OAW-IAP with PAN firewall information such as IP address, port, username, password, firewall-enabled or firewall-disabled status.

The OAW-IAP sends messages to PAN based on the type of authentication and client status:

- After a client completes the authentication and is assigned an IP address, OAW-IAP sends the **login** message.
- After a client is disconnected or dissociated from the OAW-IAP, the OAW-IAP sends a **logout** message.

Configuring an OAW-IAP for PAN integration

You can configure an OAW-IAP for PAN firewall integration by using the AOS-W Instant UI or the CLI.

In the AOS-W Instant UI

To configure PAN firewall integration in an OAW-IAP:

1. Click **More > Services**.
2. Click **Network Integration**. The PAN firewall configuration options are displayed.

Figure 79 Services Window: Network Integration Tab

The screenshot shows the 'Services' window with the 'Network Integration' tab selected. The window has a blue header with 'Services' and a 'Help' link. Below the header are tabs for 'AirGroup', 'RTLS', 'OpenDNS', 'CALEA', and 'Network Integration'. The main content area is divided into two sections: 'Palo Alto Network firewall integration' and 'XML API Server Configuration'. The first section contains a form with fields for 'Enable' (checkbox), 'Username', 'Password', 'Retype', 'IP address', 'Port' (with '443' entered), and 'Client domain'. The second section contains a list box titled 'XML API Servers' with 'test' and 'test1' entries, and buttons for 'New', 'Edit', and 'Delete'. At the bottom right are 'OK' and 'Cancel' buttons.

3. Select the **Enable** check box to enable PAN firewall.
4. Provide the user credentials of the PAN firewall administrator in the **Username** and **Password** text boxes.
5. Enter the PAN firewall IP address.
6. Enter the port number within the range of 1–65,535. The default port is 443.
7. Specify the static **Client Domain** to be mapped to the client User IDs that do not have a domain name of its own.
8. Click **OK**.

In the CLI

To enable PAN firewall integration with the OAW-IAP:

```
(Instant AP) (config)# firewall-external-enforcement pan
(Instant AP) (firewall-external-enforcement pan)# enable
(Instant AP) (firewall-external-enforcement pan)# domain-name <name>
(Instant AP) (firewall-external-enforcement pan)# ip <ip-address>
(Instant AP) (firewall-external-enforcement pan)# port <port>
(Instant AP) (firewall-external-enforcement pan)# user <name> <password>
(Instant AP) (firewall-external-enforcement pan)# end
(Instant AP)# commit apply
```

Integrating an OAW-IAP with an XML API Interface

The XML API interface provides options to create and execute user management operations seamlessly on behalf of the clients or users.

Integration with AOS-W Instant

The XML API interface allows you to send specific XML commands to an OAW-IAP from an external server. These XML commands can be used to customize OAW-IAP client entries. You can use the XML API interface to add, delete, authenticate, query, or blacklist a user or a client.

The user authentication is supported only for users authenticated by captive portal authentication and not for the dot1x-authentication users.



The user add operation performed by the XML API interface is only used to modify the role of an existing user and not to create a new user.

You can now use HTTP or HTTPS to post commands to OAW-IAP. The communication process using the XML API Interface is as follows:

- An API command is issued in XML format from the server to the VC.
- The VC processes the XML request and identifies where the client is and sends the command to the correct slave OAW-IAP.
- Once the operation is completed, VC sends the XML response to the XML server.
- Users can use the response and take appropriate action to suit their requirements. The response from the VC is returned using the predefined formats.

Configuring an OAW-IAP for XML API integration

You can configure an OAW-IAP for XML API integration by using the AOS-W Instant UI or the CLI. OAW-IAP supports the configuration of up to 8 XML API server entries.

In the AOS-W Instant UI

Enabling XML API server entries:

1. Click **More > Services**.
2. Click **Network Integration**. The XML API Server configuration parameters are displayed.
3. Enter a name for the XML API Server in the **Name** text box.
4. Enter the subnet of the XML API Server in the **Subnet** text box.
5. Enter the subnet mask of the XML API Server in the **Mask** text box.
6. Enter a passcode in the **Passphrase** text box, to enable authorized access to the XML API Server.
7. Re-enter the passcode in the **Retype** box.
8. To add multiple entries, repeat the procedure.
9. Click **OK**.
10. To edit or delete the server entries, use the **Edit** and **Delete** buttons, respectively.

In the CLI

To enable XML API integration with the OAW-IAP:

```
(Instant AP) (config)# xml-api-server <xml_api_server_profile>
(Instant AP) (xml-api-server <profile-name>)# ip <subnet> [mask <mask>]
(Instant AP) (xml-api-server)# key <key>
(Instant AP) (xml-api-server)# end
(Instant AP)# commit apply
```

Creating an XML API Request

You can now create an XML request with an appropriate authentication command and send it to the VC through HTTPS post. The format of the URL to send the XML request is:

https://<virtualcontroller-ip/auth/command.xml>

- **virtualcontroller-ip**: The IP address of the VC that will receive the XML API request
- **command.xml** : The XML request that contains the XML API command.

The format of the XML API request is:

```
xml=<aruba command="<XML API command"></options>Value</options>
...
<options>Value</options>
</aruba>
```

You can specify any of the following commands in the XML request:

Table 65: XML API Command

Parameter	Description
user_add	If the user entry is already present in the user table, the command will modify the entry with the values defined in the XML request. For an existing user, this command will update any value that is supplied, with an exception of IP and MAC address. Session time-out is only applicable to captive portal users.
user_delete	This command deletes an existing user from the user table of the VC. NOTE: Do not use the user_delete command if the intention is to clear the association from the VC user table. If the client is dual-stack, it re-inherits the authentication state from the IPv6 address. If not dual-stack, the client reverts to the initial role.
user_authenticate	This command authenticates against the server group defined in the captive portal profile. This is only applicable to captive portal users.
user_blacklist	This command blacklists a user from connecting to your network. This command uses the default blacklist timeout of 3600 seconds. There is no corresponding clear command.
user_query	This command fetches the status and details of a user connected to your network. A dual-stack client can be queried by any of its IPv4 or IPv6 addresses, but only the queried IP address is displayed in the output.

Each XML API command requires certain mandatory options to successfully execute the task. The list of all available options are:

Table 66: XML API Command Options

Parameter	Description	Range / Defaults
ipaddr	IP address of the user in IPv4 or IPv6 format.	—
macaddr	MAC address of the user in aa:bb:cc:dd:ee:ff format.	Enter MAC address with colon.
user	Name of the user.	64-character string
role	This option is used to change the role of an existing user. This option applies to user_add and user_delete commands only.	64-character string

Parameter	Description	Range / Defaults
password	The password of the user for authentication.	—
session_timeout	The role will be changed to a pre-auto role after session timeout.	—
authentication	Authentication method used to authenticate the message and the sender. You can use any of MD5, SHA-1 or clear text methods of authentication. This option is ignored if shared secret is not configured. It is, however, mandatory if it is configured.	
key	This is the encoded MD5/SHA-1 hash of shared secret or plain text shared secret. This option is ignored if shared secret is not configured on the switch. The actual MD5/SHA-1 hash is 16/20 bytes and consists of binary data. It must be encoded as an ASCII-based HEX string before sending. It must be present when the VC is configured with an xml API key for the server. Encoded hash length is 32/40 bytes for MD5/SHA-1.	
version	The version of the XML API interface available in the VC. This is mandatory in all XML API requests.	Current version is XML API 1.0

CALEA Integration and Lawful Intercept Compliance

Lawful Intercept (LI) allows the Law Enforcement Agencies (LEA) to perform an authorized electronic surveillance. Depending on the country of operation, the service providers (SPs) are required to support LI in their respective networks.

In the United States, SPs are required to ensure LI compliance based on Communications Assistance for Law Enforcement Act (CALEA) specifications.

AOS-W Instant supports CALEA integration in a hierarchical and flat topology, mesh OAW-IAP network, the wired and wireless networks.



NOTE

Enable this feature only if lawful interception is authorized by a law enforcement agency.

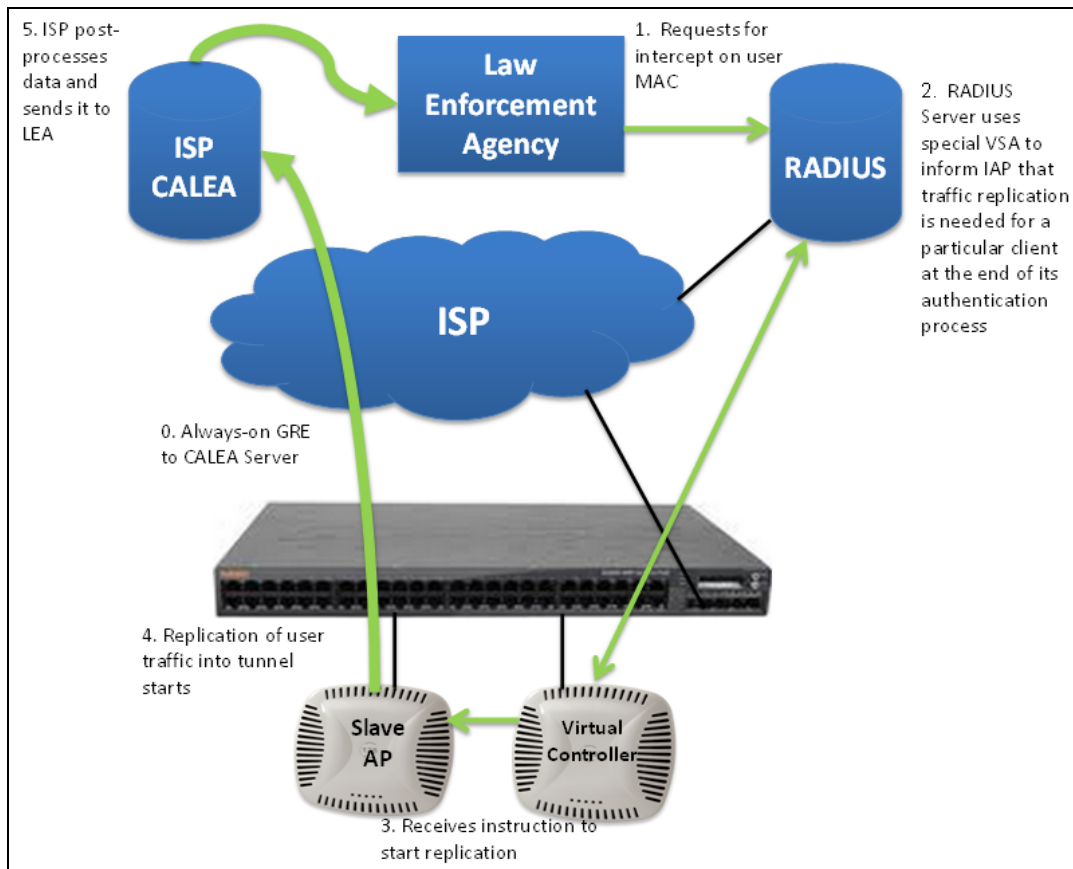
CALEA Server Integration

To support CALEA integration and ensure LI compliance, you can configure the OAW-IAPs to replicate a specific or selected client traffic and send it to a remote CALEA server.

Traffic Flow from OAW-IAP to CALEA Server

You can configure an OAW-IAP to send GRE-encapsulated packets to the CALEA server and replicate client traffic within the GRE tunnel. Each OAW-IAP sends GRE encapsulated packets only for its associated or connected clients. The following figure illustrates the traffic flow from the OAW-IAP to the CALEA server.

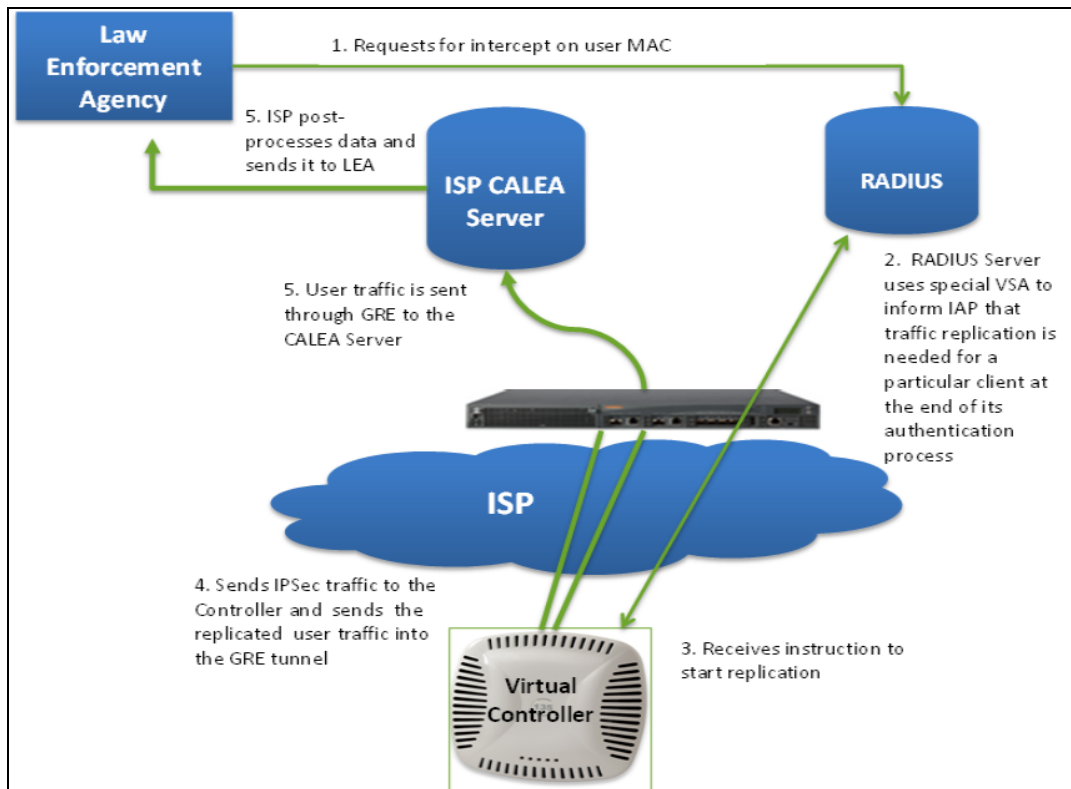
Figure 80 IAP to CALEA Server



Traffic Flow from OAW-IAP to CALEA Server through VPN

You can also deploy the CALEA server with the switch and configure an additional IPsec tunnel for corporate access. When CALEA server is configured with the switch, the client traffic is replicated by the slave OAW-IAP and client data is encapsulated by GRE on slave, and routed to the master OAW-IAP. The master OAW-IAP sends the IPsec client traffic to the switch. The switch handles the IPsec client traffic while GRE data is routed to the CALEA server. The following figure illustrates the traffic flow from OAW-IAP to the CALEA server through VPN.

Figure 81 OAW-IAP to CALEA Server through VPN



Ensure that IPsec tunnel is configured if the client data has to be routed to the ISP or CALEA server through VPN. For more information on configuring IPsec, see [Configuring an IPsec Tunnel on page 228](#).

Client Traffic Replication

Client traffic is replicated in the following ways:

- Through RADIUS VSA—In this method, the client traffic is replicated by using the RADIUS VSA to assign clients to a CALEA-related user role. To enable role assignment to clients, you need to create a user role and a CALEA access rule, and then assign the CALEA rule to the user role. Whenever a client that is configured to use a CALEA rule connects, a replication role is assigned.
- Through Change of Authorization (CoA)—In this method, a user session can start without replication. When the network administrator triggers a CoA from the RADIUS server, the user session is replicated. The replication is stopped when the user disconnects or by sending a CoA to change the replication role.

As the client information is shared between multiple OAW-IAPs in a cluster, the replication rules persist when clients roam within the cluster.

Configuring an OAW-IAP for CALEA Integration

To enable CALEA server integration, perform the following steps:

1. [Create a CALEA profile](#).
2. If a replication role must be assigned through the RADIUS VSA, [create an access rule and assign the access rule to a WLAN SSID or wired profile](#).
3. [Verify the configuration](#).

Creating a CALEA Profile

You can create a CALEA profile by using the AOS-W Instant UI or the CLI.

In the AOS-W Instant UI

To configure a CALEA profile:

1. Click **More > Services** link on the AOS-W Instant main window.
2. In the Services section, click **CALEA**. The **CALEA** tab details are displayed.
3. Specify the following parameters:
 - **IP address**—Specify the IP address of the CALEA server.
 - **Encapsulation type**—Select the encapsulation type. The current release of AOS-W Instant supports GRE only.
 - **GRE type**—Specify the GRE type.
 - **MTU**—Specify a size for the maximum transmission unit (MTU) within the range of 68–1500. After GRE encapsulation, if packet length exceeds the configured MTU, IP fragmentation occurs. The default MTU size is 1500.
4. Click **OK**.

In the CLI

To create a CALEA profile:

```
(Instant AP) (config)# calea
(Instant AP) (calea)# ip <IP-address>
(Instant AP) (calea)# ip mtu <size>
(Instant AP) (calea)# encapsulation-type <gre>
(Instant AP) (calea)# gre-type <type>
(Instant AP) (calea)# end
(Instant AP)# commit apply
```

Creating an Access Rule for CALEA

You can create an access rule for CALEA by using the AOS-W Instant UI or the CLI.

In the AOS-W Instant UI

To create an access rule:

1. To add the CALEA access rule to an existing profile:
 - a. Select an existing wireless (**Network > edit**) or,
 - b. Select a Wired (**More > Wired > Edit**) profile.
2. To add the access rule to a new profile:
 - a. Click **New** under the **Network** tab and create a WLAN profile or,
 - a. Click **More > Wired > New** and create a wired port profile.
3. On the **Access** tab, select the role for which you want create the access rule.
4. Under **Access Rules**, click **New**.
5. In the **New Rule** window that is displayed, select **CALEA**.
6. Click **OK**.
7. Create a role assignment rule if required.
8. Click **Finish**.

In the CLI

To create a CALEA access rule:

```
(Instant AP) (config)# wlan access-rule <name>
(Instant AP) (Access Rule <name>)# calea
(Instant AP) (Access Rule <name>)# end
(Instant AP)# commit apply
```

To assign the CALEA rule to a user role:

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

To associate the access rule with a wired profile:

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

Verifying the configuration

To verify the CALEA configuration:

```
(Instant AP)# show calea config
```

To view the tunnel encapsulation statistics:

```
(Instant AP)# show calea statistics
```

Example

To enable CALEA integration:

```
(Instant AP) (config)# calea
(Instant AP) (calea)# ip 192.0.2.7
(Instant AP) (calea)# ip mtu 1500
(Instant AP) (calea)# encapsulation-type GRE
(Instant AP) (calea)# gre-type 255
(Instant AP) (calea)# end
```

To enable a CALE access rule:

```
(Instant AP) (config)# wlan access-rule ProfileCalea
(Instant AP) (Access Rule "ProfileCalea")# calea
(Instant AP) (Access Rule "ProfileCalea")# end
(Instant AP)# commit apply
```

To assign the CALEA rule to user role:

```
(Instant AP) (config)# wlan ssid-profile Calea-Test
(Instant AP) (SSID Profile"Calea-Test")# enable
(Instant AP) (SSID Profile"Calea-Test")# index 0
(Instant AP) (SSID Profile"Calea-Test")# type employee
(Instant AP) (SSID Profile"Calea-Test")# essid QA-Calea-Test
(Instant AP) (SSID Profile"Calea-Test")# opmode wpa2-aes
(Instant AP) (SSID Profile"Calea-Test")# max-authentication-failures 0
(Instant AP) (SSID Profile"Calea-Test")# auth-server server1
(Instant AP) (SSID Profile"Calea-Test")# set-role Filter-Id equals 123456 calea-test
(Instant AP) (SSID Profile"Calea-Test")# rf-band 5.0
(Instant AP) (SSID Profile"Calea-Test")# captive-portal disable
(Instant AP) (SSID Profile"Calea-Test")# dtim-period 1
(Instant AP) (SSID Profile"Calea-Test")# inactivity-timeout 1000
(Instant AP) (SSID Profile"Calea-Test")# broadcast-filter none
(Instant AP) (SSID Profile"Calea-Test")# dmo-channel-utilization-threshold 90
(Instant AP) (SSID Profile"Calea-Test")# local-probe-req-thresh 0
(Instant AP) (SSID Profile"Calea-Test")# max-clients-threshold 64
(Instant AP) (SSID Profile"Calea-Test")# end
(Instant AP) (SSID Profile"Calea-Test")# commit apply
```

To verify the configuration:

```
(Instant AP)# show calea config
```



```
calea-ip :10.0.0.5
encapsulation-type :gre
gre-type :25944
ip mtu : 150
```

To view the tunnel encapsulation statistics:

```
(Instant AP)# show calea statistics
```

```
Rt resolve fail : 0
Dst resolve fail: 0
Alloc failure : 0
Fragged packets : 0
Jumbo packets : 263
Total Tx fail : 0
Total Tx ok : 263
```

This chapter describes cluster security and the procedure for configuring cluster security DTLS for secure communication. It includes the following topics:

- [Overview on page 306](#)
- [Enabling Cluster Security on page 307](#)
- [Cluster Security Debugging Logs on page 307](#)
- [on page 308](#)

Overview

Cluster security is a communication protocol that secures control plane messages between AOS-W Instant access points. Control plane messages such as configuration, cluster join, and other messages distributed between the devices in a cluster are secured using this protocol. Cluster security operates on the UDP port 4434 and uses DTLS protocol to secure messages.

Cluster Security Using DTLS

Cluster security provides secure communication using Datagram Transport Layer Security (DTLS). A DTLS connection is established between the OAW-IAPs communicating with each other in the cluster. Following are some of the advantages of using DTLS for cluster security:

- Mutual authentication is done between the OAW-IAPs in a cluster using device certificate.
- Peer MAC address validation against **AP whitelist** can be enabled in the configuration.
- Control plane messages between cluster members are transmitted securely using the DTLS connection established.

If auto-join is enabled, backward compatibility and recovery of OAW-IAPs is allowed on ARUBA UDP port 8211. Messages required for image synchronization and cluster security DTLS state synchronization are the only messages allowed.



If auto-join is disabled, the MAC address of a peer OAW-IAP is verified against the **AP whitelist** during device certificate validation.

Locked Mode Slave OAW-IAP

A slave OAW-IAP with non-factory default configuration is considered to be in locked mode of operation. These slave OAW-IAPs will not be able to join the existing non-DTLS cluster as backward compatibility and recovery is not allowed.

To recover the slave OAW-IAPs in locked mode:

- Execute the **disable-cluster-security-dtls** action command on the slave OAW-IAP , or
- Factory reset the slave OAW-IAP.

Enabling Cluster Security

You can enable cluster security using the AOS-W Instant UI or the CLI. Ensure that the following pre-requisites are satisfied:

Pre-requisites

1. NTP server must be reachable—If internet is reachable, pool.ntp.org will be used by default, otherwise a static NTP server needs to be configured.
2. UDP port 4434 should be permitted.

In the AOS-W Instant UI

To enable cluster security:

1. Navigate to **System > General**.
2. Select **Enabled** from the **Cluster security** drop-down list.
3. Click **OK**.



Reboot all the OAW-IAPs in the swarm for the configuration to take effect.

In the CLI:

To enable cluster security:

```
(Instant AP) (config)# cluster-security
(Instant AP) (cluster-security)# dtls
(Instant AP) (cluster-security)# end
(Instant AP)# commit apply
```

To disable cluster security DTLS:

```
(Instant AP) (config)# cluster-security
(Instant AP) (cluster-security)# no dtls
(Instant AP) (cluster-security)# end
(Instant AP)# commit apply
```

To change per module logging level of cluster security:

```
(Instant AP)# cluster-security logging module <module_name> log-level <level>
```

To set individual log level for each module:

```
(Instant AP)# cluster-security logging module <module_name> log-level-individual <level>
```

After enabling or disabling the cluster security option, ensure that the Config Sync Status is TRUE in the output of the show summary command, before rebooting the cluster.



Cluster security is not supported for L3 mobility.

Cluster Security Debugging Logs

Cluster security logging is organized into modules based on functionality. The following are the core modules which are useful and should be used for debugging:

peer—The peer module is used to log connection initiation, renegotiation, collision and active connection updates. The log-level should be set to **debug** level while debugging any issues.

conn—The connection module is used to log connection creation, establishment, data transfer and maintenance updates. The log-level should be set to **debug** level for debugging DTLS connection issues.

mcap—The module capture module is used to log messages sent and received to the socket. Set log-level to **debug** to log only control messages. Set log-level to **debug1** to log control and data messages.

The following command can be used to set per module logging level:

```
(Instant AP) # cluster-security logging module <module_name> log-level <level>
```

Once the log-level is set, logs can be viewed using:

```
(Instant AP) # show log papi-handler
```

Verifying the Configuration

The following show commands can be used to view the cluster security configuration:

To view current cluster security Configuration and running state

```
(Instant AP) # show cluster-security
```

To view the cluster security statistics:

```
(Instant AP) # show cluster-security stats
```

To view the cluster security connection table:

```
(Instant AP) # show cluster-security connections
```

To view the cluster security peers:

```
(Instant AP) # show cluster-security peers
```

To view the message handler process logs:

```
(Instant AP) # show log papi-handler <count>
```

This chapter provides information on managing and monitoring OAW-IAPs from the server:

Managing an OAW-IAP from OmniVista

OmniVista is a powerful platform and easy-to-use network operations system that manages Alcatel-Lucent wireless, wired, and remote access networks, as well as wired and wireless infrastructures from a wide range of third-party manufacturers. With its easy-to-use interface, OmniVista provides real-time monitoring, proactive alerts, historical reporting, as well as fast and efficient troubleshooting. It also offers tools that manage RF coverage, strengthen wireless security, and demonstrate regulatory compliance.

The 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.

The OmniVista features available in the AOS-W Instant network are described in the following sections:

Image Management

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

The following models can be used to upgrade the firmware:

- **Automatic**—In this model, the 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 for each VC or set the desired firmware preference per group of devices.

Resetting an OAW-IAP

An OAW-IAP device can be reset through OmniVista in the **Managed** mode:

1. In the **Modify Devices** section, select the OAW-IAP devices you want to reset to factory-default by selecting the check box beside it.
2. From the **Change Device Group Folder** drop-down list, select **Factory Reset selected devices**.
3. Click the **Factory Reset** tab.



On resetting the OAW-IAP device from OmniVista, all the configuration values will be set to default except for the **per-ap-settings** and **VC Key** value.

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.

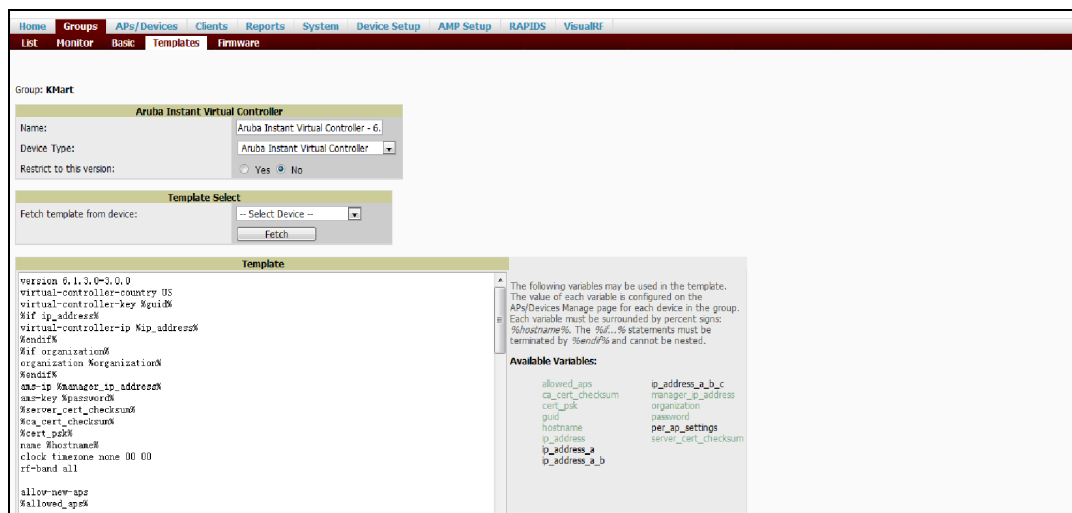
In the OmniVista User Interface (UI), you can select either **Manage Read/Write** or **Monitor-only+Firmware Upgrades** as management modes. When the OmniVista Management level is set to **Manage Read/Write**, the AOS-W Instant UI is in read-only mode. When the OmniVista Management level is set to **Monitor-only+Firmware Upgrades**, the AOS-W Instant UI changes to the read-write mode.

With the latest version of OmniVista, a new option in the AMP is available to put the OAW-IAP in config-only mode. In this mode, the OAW-IAP will receive the firmware upgrades and configurations, but will not send any statistics for monitoring. The load is reduced on OAW-IAP and OmniVista and this assists in scaling OmniVista effectively.

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 the following figure. It audits every device on an ongoing basis to ensure that configurations never vary from the enterprise policies. It alerts you whenever a violation is detected and automatically repairs the incorrectly configured devices.

Figure 82 *Template-Based Configuration*



Trending Reports

OmniVista saves up to 14 months of actionable information, including network performance data and user roaming patterns, so you can analyze how network usage and performance trends have changed over time. It also provides detailed capacity reports with which you can plan the capacity and appropriate strategies for your organization.

Intrusion Detection System (IDS)

OmniVista provides advanced, rules-based rogue classification. It automatically detects rogue OAW-IAPs irrespective of their location in the network and 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

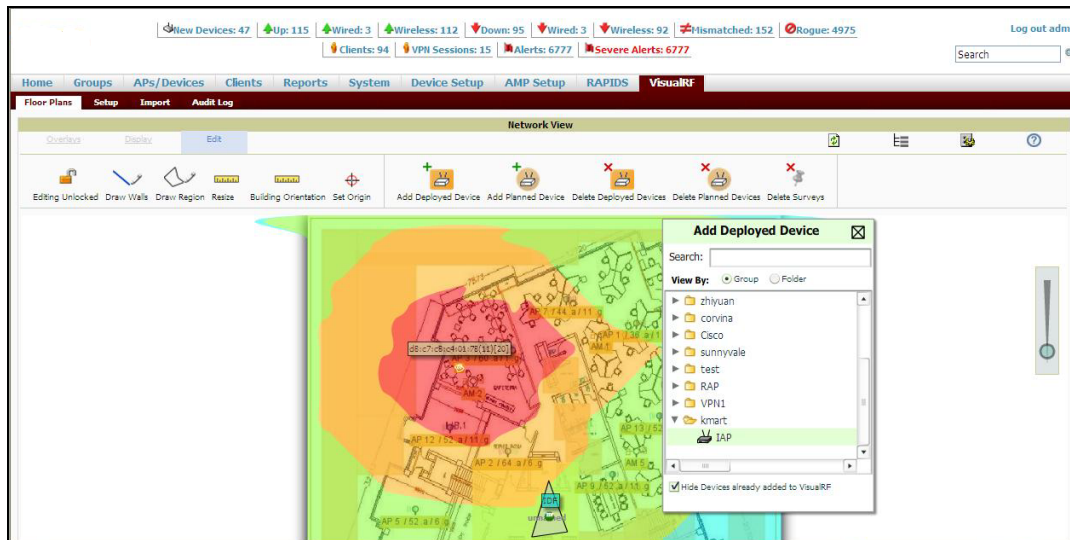
OmniVista supports Wireless Intrusion Detection System (WIDS) Event Reporting, which is provided by AOS-W Instant. This includes WIDS classification integration with the Rogue Access Point Detection Software (RAPIDS) module. RAPIDS is a powerful and easy-to-use tool for automatic detection of unauthorized wireless devices. It supports multiple methods of rogue detection and uses authorized wireless OAW-IAPs 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 AOS-W Instant

OmniVista supports RF visualization for AOS-W Instant. The VisualRF module provides a real-time picture of the actual radio environment of your wireless network and the ability to plan the wireless coverage of new sites. VisualRF uses sophisticated RF fingerprinting to accurately display coverage patterns and calculate the location of every Instant device in range. VisualRF provides graphical access to floor plans, client location, and RF visualization for floors, buildings, and campuses that host your network.

Figure 83 Adding an OAW-IAP in VisualRF



PSK-Based and Certificate-Based Authentication

On the DHCP server, two formats for option 43 are supported:

- **<organization>, <ams-ip>, <ams-key>**—If you select this format, the OAW-IAP authenticates the AMP server using the Pre-Shared Key (PSK) login process.
- **<organization>, <ams-domain>**—If you select this format, the OAW-IAP resolves the OmniVista domain name into one or two IP addresses as OmniVista Primary or OmniVista Backup, and then OAW-IAP starts a certificate-based authentication with AMP server, instead of the PSK login. When the AMP domain name is used, the OAW-IAP performs certificate-based authentication with the AMP server. The OAW-IAP initiates a Secure Socket Layer (SSL) connection with the OmniVista server. The OmniVista server verifies the signature and public key certificate from the OAW-IAP. If the signature matches, the OmniVista responds to the OAW-IAP with the login request.

Configurable Port for OAW-IAP and OmniVista Management Server Communication

You can now customize the port number of the AMP server through the **server_host:server_port** format, for example, **amp.aruba.com:4343**.

The following example shows how to configure the port number of the AMP server:

```
24:de:c6:cf:63:60 (config) # ams-ip 10.65.182.15:65535
24:de:c6:cf:63:60 (config) # end
24:de:c6:cf:63:60# commit apply
```

Configuring Organization String

The Organization string is a set of colon-separated strings created by the OmniVista administrator to accurately represent the deployment of each OAW-IAP. This string is defined by the installation personnel on the site.

You can use any of the following strings:

- AMP Role—"Org Admin" (initially disabled)
- AMP User—"Org Admin" (assigned to the role "Org Admin")
- Folder—"Org" (under the Top folder in AMP)
- Configuration Group—"Org"

You can also assign additional strings to create a hierarchy of subfolders under the folder named "Org". For example:

- subfolder1 for a folder under the "Org" folder
- subfolder2 for a folder under subfolder1

Shared Key

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

Configuring OmniVista Information

You can configure OmniVista information by using the AOS-W Instant UI or the CLI.

In the AOS-W Instant UI

To configure OmniVista information:

1. Click the OmniVista **Set Up Now** link of the main window. The **System** window is displayed with the OmniVista parameters on the **Admin** tab.
2. Enter the name of your organization in the **Organization name** text box. The name defined for the organization is displayed under the **Groups** tab in the OmniVista UI.
3. Enter the IP address or domain name of the OmniVista server in the **AirWave server** text box.
4. Enter the IP address or domain name of a backup OmniVista server in the **AirWave backup server** text box. The backup server provides connectivity when the primary server is down. If the OAW-IAP cannot send data to the primary server, the VC switches to the backup server automatically.
5. Enter the shared key in the **Shared key** text box and reconfirm. This shared key is used for configuring the first OAW-IAP in the AOS-W Instant network.
6. Click **OK**.

In the CLI

To configure OmniVista information:

```
(Instant AP) (config)# organization <name>
(Instant AP) (config)# ams-ip <IP-address or domain name>
(Instant AP) (config)# ams-backup-ip <IP-address or domain name>
(Instant AP) (config)# ams-key <key>
(Instant AP) (config)# end
(Instant AP)# commit apply
```

Configuring for OmniVista Discovery Through DHCP

The OmniVista can be discovered through the DHCP server. You can configure this only if OmniVista was not configured earlier or if you have deleted the precedent configuration.

On the DHCP server, the format for option 60 is "**InstantAP**", and the two formats for option 43 are "**<organization>,<ams-ip>,<ams-key>**" and "**<organization>,<ams-domain>**".

If you use the **<organization>,<ams-ip>,<ams-key>** format, the PSK-based authentication is used to access the AMP server.

If you use the **<organization>,<ams-domain>** format, the OAW-IAP resolves the domain name into two IP addresses—OmniVista Primary and OmniVista Backup—and then the OAW-IAP starts a certificate-based authentication with AMP server, instead of the PSK login.



For option 43, when you choose to enter the domain name, the IP address and key are not available.

Enabling DNS-Based Discovery of the Provisioning AMP Server

OAW-IAPs can now automatically discover the provisioning AMP server if the DHCP option 43 and Activate cannot perform zero-touch provisioning (ZTP) and transfer the OmniVista configuration to the OAW-IAP.

When a domain option **xxx** is included in the DHCP configuration, the OAW-IAP will search the DNS server records for **aruba-airwave.xxx**. When there is no domain option, the OAW-IAP will search only the server records for **aruba-airwave**.



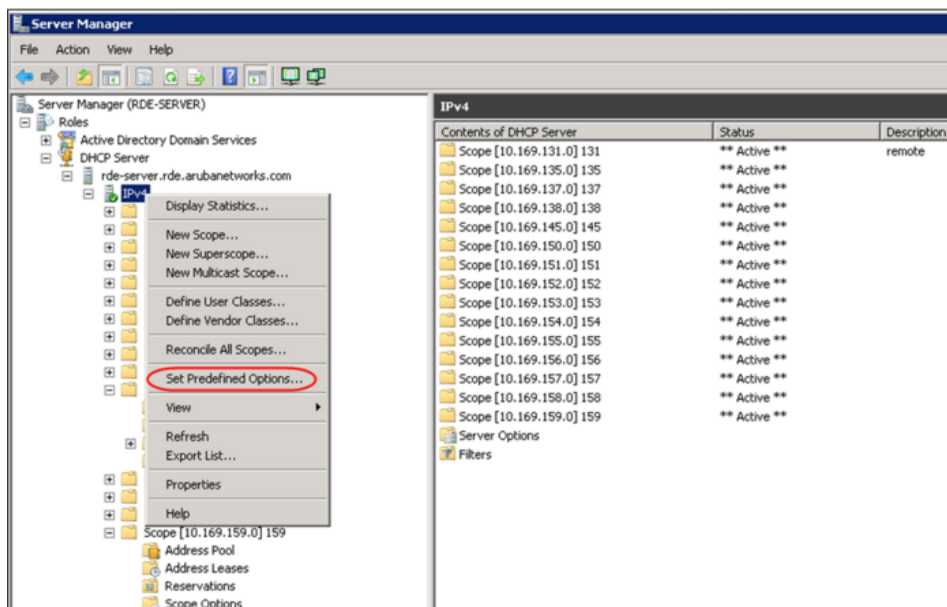
To enable OAW-IAPs to automatically discover the AMP server, create a DNS record for **aruba-airwave.xxx** or **aruba-airwave** in the DNS server. To use this feature on the OmniVista side, enable certificate-based login. For information on how to enable certificate-based login, see [PSK-Based and Certificate-Based Authentication on page 311](#).

Standard DHCP Options 60 and 43 on Windows Server 2008

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

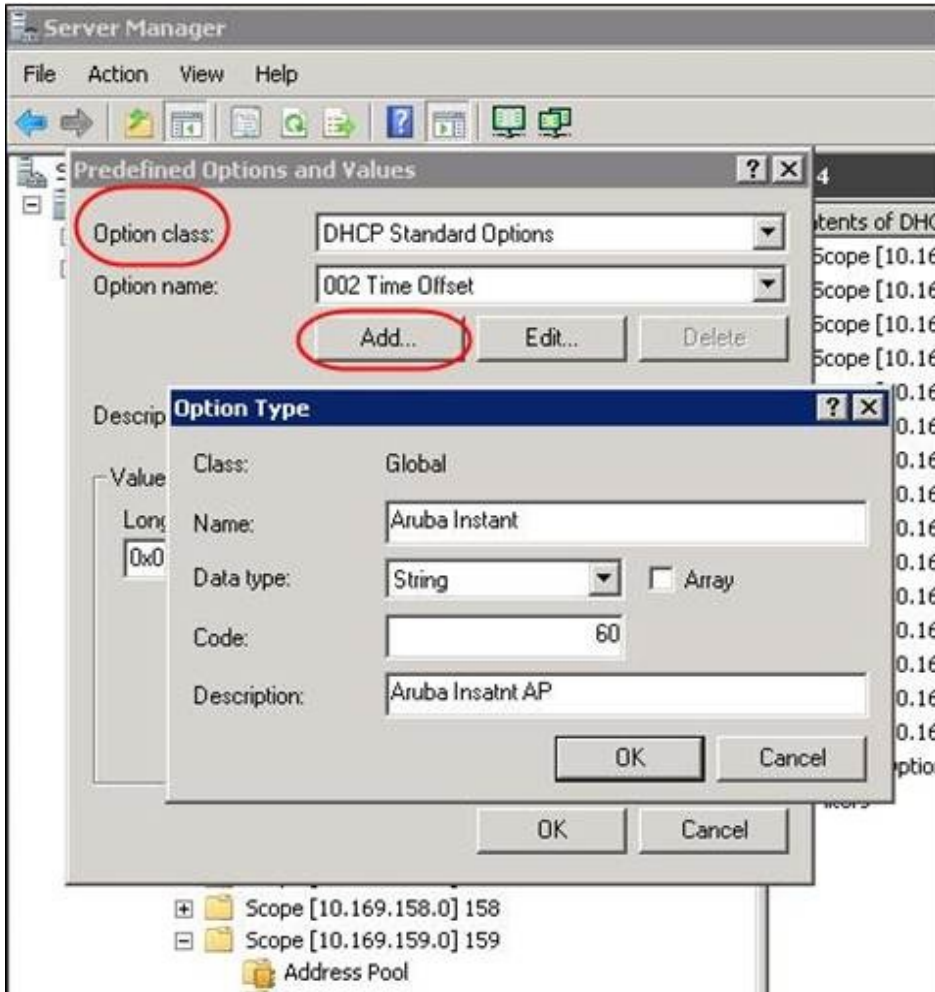
1. From a server running Windows Server 2008, navigate to **Server Manager > Roles > DHCP server > domain > DHCP Server > IPv4**.
2. Right-click **IPv4** and select **Set Predefined Options**.

Figure 84 *Instant and DHCP options for OmniVista: Set Predefined Options*



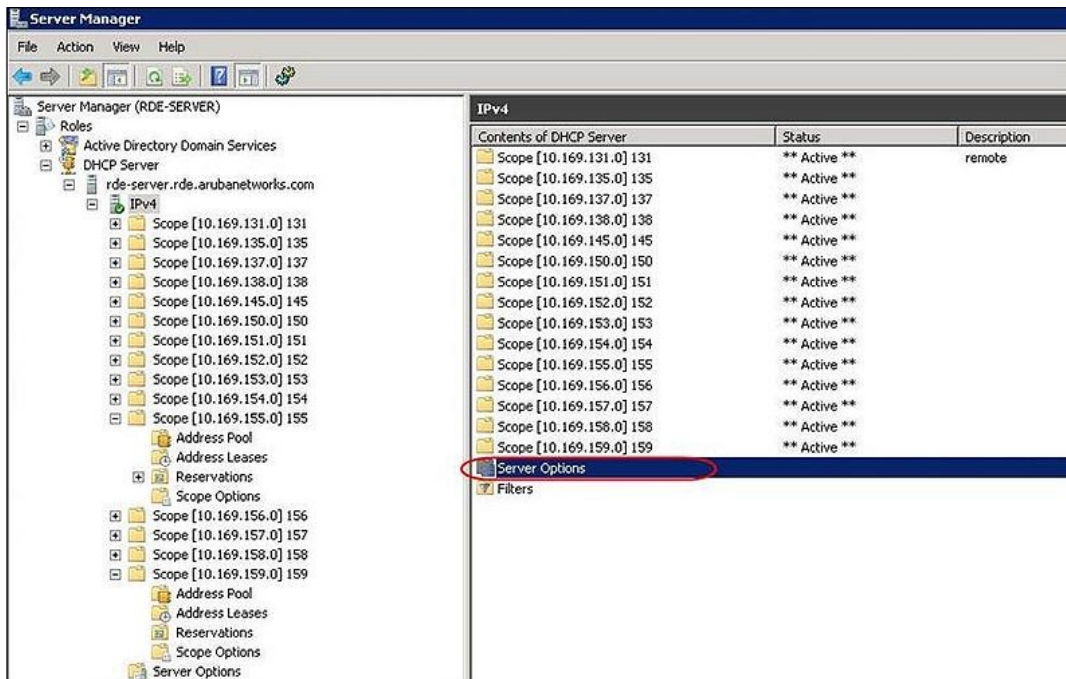
3. Select **DHCP Standard Options** in the **Option class** drop-down list and then click **Add**.
4. Enter the following information:
 - Name—AOS-W Instant
 - Data Type—String
 - Code—60
 - Description—AOS-W Instant AP

Figure 85 AOS-W Instant and DHCP options for OmniVista: Predefined Options and Values



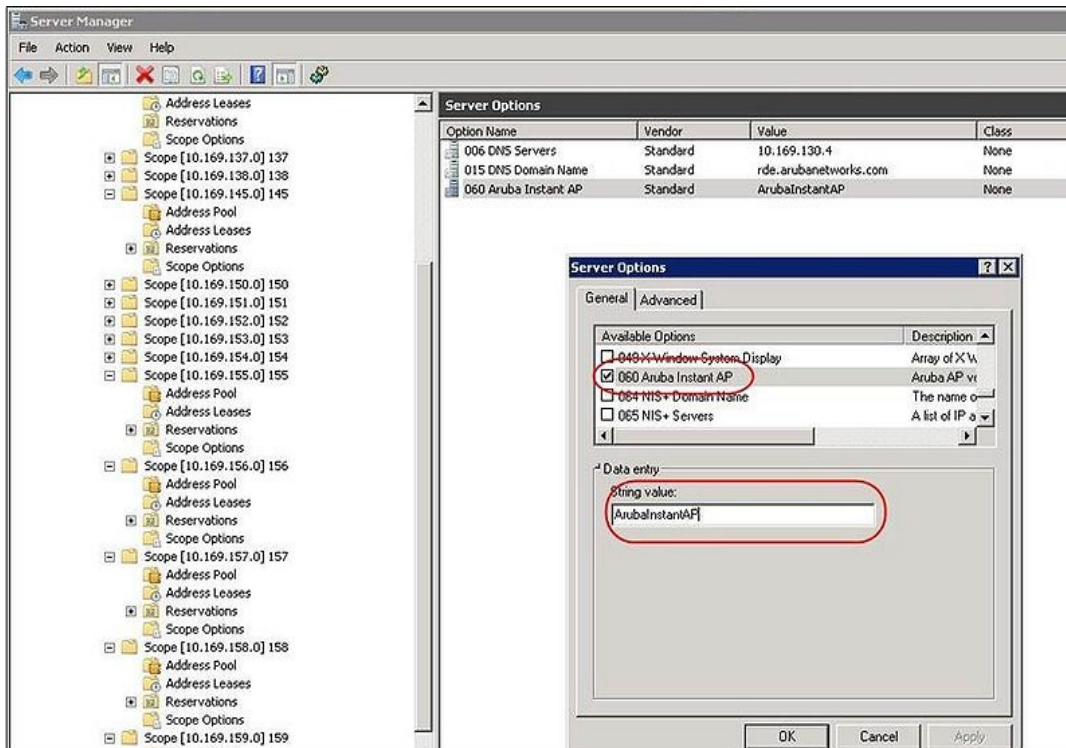
5. Navigate to **Server Manager** and select **Server Options** in the **IPv4** window. (This sets the value globally. Use options on a per-scope basis to override the global options.)
6. Right-click **Server Options** and select the configuration options.

Figure 86 AOS-W Instant and DHCP options for OmniVista: Server Options



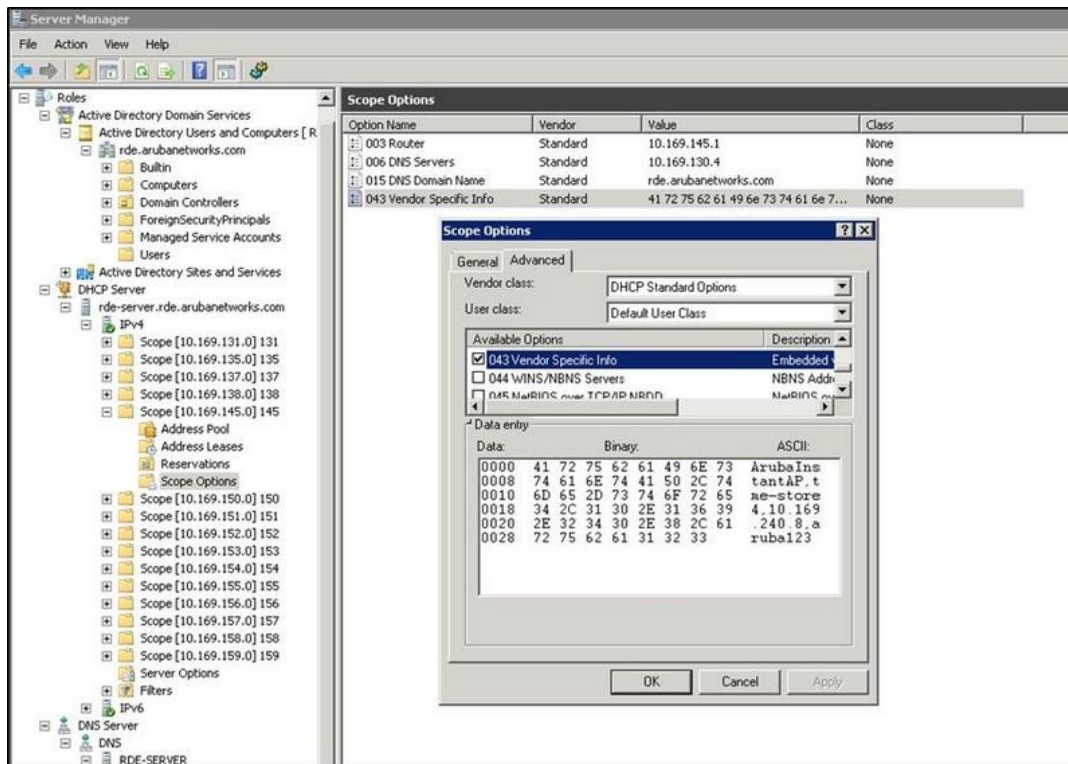
7. Select **060 Alcatel-Lucent Instant AP** in the **Server Options** window and enter **Alcatel-LucentInstantAP** in the **String value** text box.

Figure 87 AOS-W Instant and DHCP options for OmniVista—060 OAW-IAP in Server Options



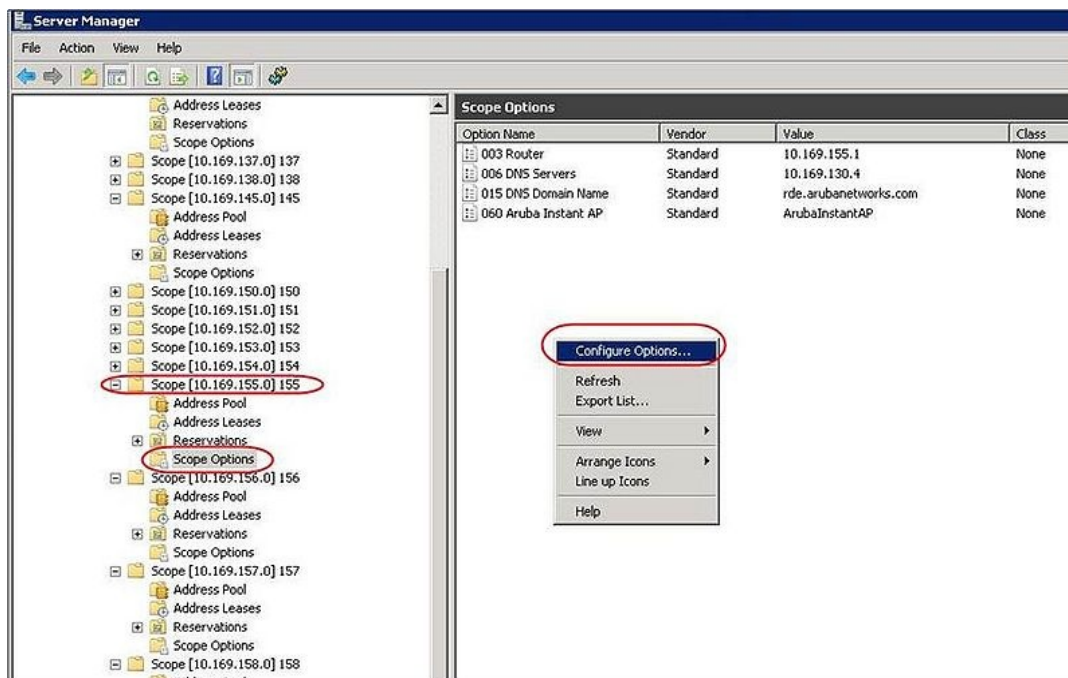
8. Select **043 Vendor Specific Info** and enter a value for either of the following in the ASCII text box:
 - **airwave-orgn, airwave-ip, airwave-key**; for example: Alcatel-Lucent,192.0.2.20, 12344567
 - **airwave-orgn, airwave-domain**; for example: Alcatel-Lucent, alcatellucent.support.com

Figure 88 AOS-W Instant and DHCP options for—043 Vendor-Specific Info



This creates DHCP options 60 and 43 on a global basis. You can do the same on a per-scope basis. The per-scope option overrides the global option.

Figure 89 AOS-W 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 OAW-IAPs in a network that already uses DHCP options 60 and 43 for other services. Some networks use DHCP standard options 60 and 43 to provide the DHCP clients information about certain services such as PXE. In such an environment, the standard DHCP options 60 and 43 cannot be used for OAW-IAPs.

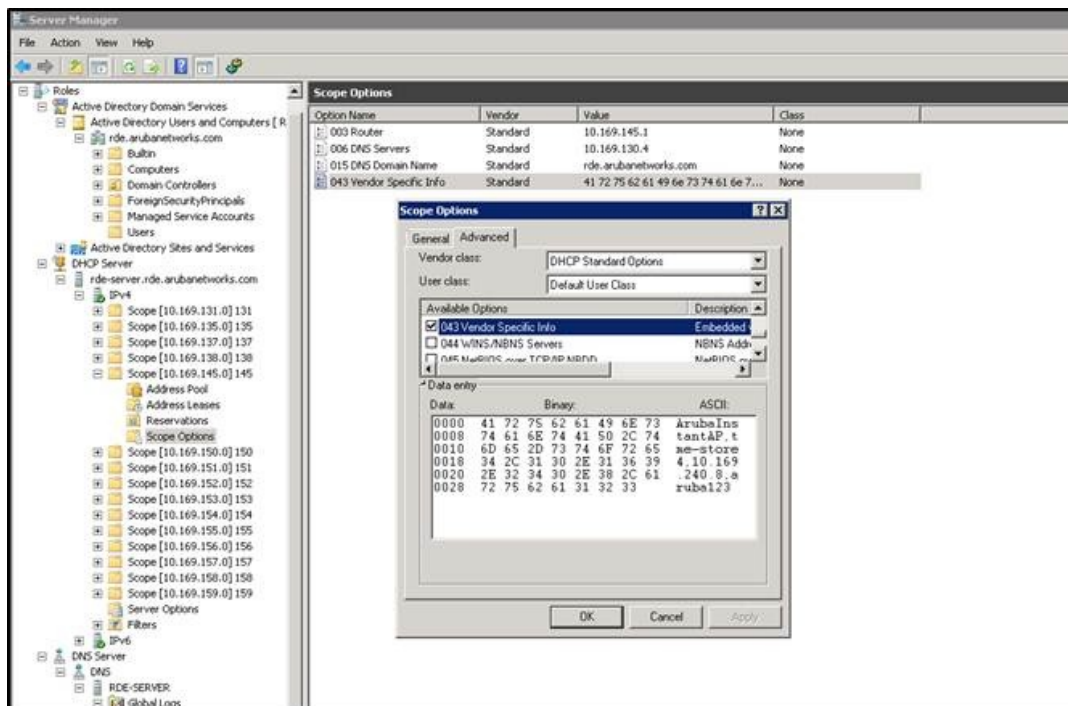
This method describes how to set up a DHCP server to send option 43 with OmniVista information to the OAW-IAP. This section assumes that option 43 is sent per scope, because option 60 is being shared by other devices as well.



The DHCP scope must be specific to AOS-W Instant, and the PXE devices that use options 60 and 43 must not connect to the subnet defined by this scope. This is because you can specify only one option 43 for a scope, and if other devices that use option 43 connect to this subnet, they are presented with the information specific to the OAW-IAP.

1. In Windows Server 2008, navigate to **Server Manager > Roles > DHCP Server > Domain DHCP Server > IPv4**.
2. Select a scope [subnet]. Scope [10.169.145.0]145 is selected in the example shown in the figure below.
3. Right-click and select **Advanced**, and then specify the following options:
 - Vendor class—DHCP Standard Options
 - User class—Default User Class
 - Available options—Select 043 Vendor-Specific Info
 - String Value—Alcatel-LucentInstantAP, tme-store4, 10.169.240.8, Alcatel-Lucent123 (which is the OAW-IAP description, organization string, OmniVista IP address or domain name, Pre-shared key, for OmniVista)

Figure 90 Vendor-Specific DHCP options



Upon completion, the OAW-IAP shows up as a new device in OmniVista, and a new group called **tme-store4** is created. Navigate to **APs/Devices > New > Group** to view this group.

Figure 91 OmniVista—New Group

Figure 92 OmniVista—Monitor

Device	Status	Detailed Status	Upstream	Upstream Status	Notes	APs	Clients	Usage	Uptime	Configuration	Folder	Controller	Location
d8:c7:c8:c4:43:19	Up	OK	-	-	-	0	0	-	4 mins	Good	.tme-store4	Instant-C443:19	-
Instant-C4:43:19	Up	OK	-	-	-	1	0	-	4 mins	Mismatched	.tme-store4	-	-

This chapter provides the following information:

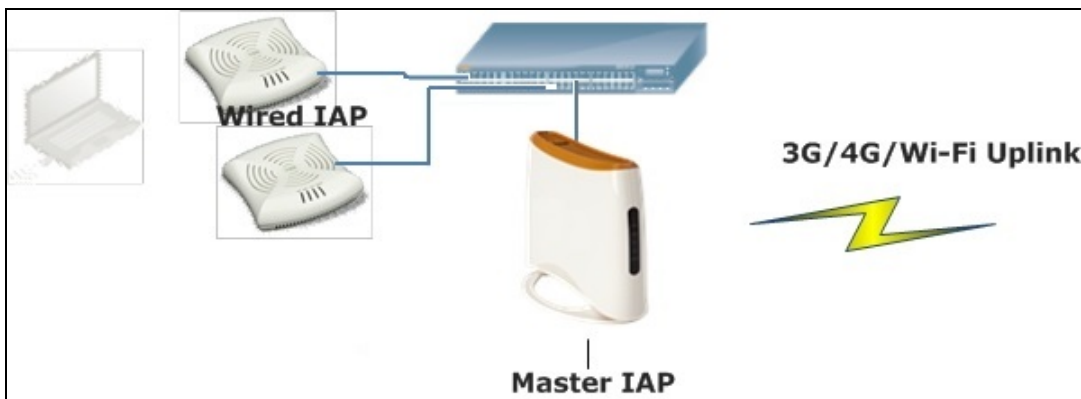
- [Uplink Interfaces on page 319](#)
- [Uplink Preferences and Switching on page 324](#)

Uplink Interfaces

AOS-W Instant network supports Ethernet, 3G and 4G USB modems, and the Wi-Fi uplink to provide access to the corporate AOS-W Instant network. The 3G/4G USB modems and the Wi-Fi uplink can be used to extend the connectivity to places where an Ethernet uplink cannot be configured. It also provides a reliable backup link for the Ethernet-based AOS-W Instant network.

The following figure illustrates a scenario in which the OAW-IAPs join the VC as slave OAW-IAPs through a wired or mesh Wi-Fi uplink:

Figure 93 *Uplink Types*



The following types of uplinks are supported on AOS-W Instant:

- [Ethernet Uplink](#)
- [Cellular Uplink](#)
- [Wi-Fi Uplink](#)

Ethernet Uplink

The Eth0 port on an OAW-IAP is enabled as an uplink port by default. You can view the type of uplink and the status of uplink of an OAW-IAP in the **Info** tab on selecting a client.

Figure 94 Uplink Status

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

Ethernet uplink supports the following types of configuration in this Instant release.

- PPPoE
- DHCP
- Static IP

You can use PPPoE for your uplink connectivity in both OAW-IAP and IAP-VPN deployments. PPPoE is supported only in a single OAW-IAP deployment.



Uplink redundancy with the PPPoE link is not supported.

When the Ethernet link is up, it is used as a PPPoE or DHCP uplink. After the PPPoE settings are configured, PPPoE has the highest priority for the uplink connections. The OAW-IAP can establish a PPPoE session with a PPPoE server at the ISP and get authenticated using Password Authentication Protocol (PAP) or the Challenge Handshake Authentication Protocol (CHAP). Depending upon the request from the PPPoE server, either the PAP or the CHAP credentials are used for authentication. After configuring PPPoE, reboot the OAW-IAP for the configuration to take effect. The PPPoE connection is dialed after the OAW-IAP comes up. The PPPoE configuration is checked during OAW-IAP boot and if the configuration is correct, Ethernet is used for the uplink connection.



When PPPoE is used, do not configure Dynamic RADIUS Proxy and IP address of the VC. An SSID created with default VLAN is not supported with PPPoE uplink.

You can also configure an alternate Ethernet uplink to enable uplink failover when an Ethernet port fails.

Configuring PPPoE Uplink Profile

You can configure PPPoE settings from the AOS-W Instant UI or the CLI.

In the AOS-W Instant UI

Configuring PPPoE settings:

1. Click the **System** link on the AOS-W Instant main window.
2. In the **System** section, click the **Show advanced options** link.
3. Perform the following steps in the **PPPoE** section in the **Uplink** tab:
 - a. Enter the PPPoE service name provided by your service provider in the **Service name** text box.
 - b. Enter the secret key used for Challenge Handshake Authentication Protocol (CHAP) authentication in the **CHAP secret** and **Retype** text boxes. You can use a maximum of 34 characters for the CHAP secret key.
 - c. Enter the username for the PPPoE connection in the **User** text box.

- d. Enter a password for the PPPoE connection and confirm the password in the **Password** and **Retype** text boxes.
4. Select a value from the **Local interface** drop-down list to set a local interface for the PPPoE uplink connections. The selected DHCP scope will be used as a local interface on the PPPoE interface and the Local, L3 DHCP gateway IP address as its local IP address. When configured, the local interface acts as an unnumbered PPPoE interface and allows the entire Local, L3 DHCP subnet to be allocated to clients.



The options in the **Local interface** drop-down list are displayed only if a Local, L3 DHCP scope is configured on the OAW-IAP.

5. Click **OK**.
6. Reboot the OAW-IAP for the configuration to take effect.

In the CLI

To configure a PPPoE uplink connection:

```
(Instant AP) (config) # pppoe-uplink-profile
(Instant AP) (pppoe-uplink-profile) # pppoe-svcname <service-name>
(Instant AP) (pppoe-uplink-profile) # pppoe-username <username>
(Instant AP) (pppoe-uplink-profile) # pppoe-passwd <password>
(Instant AP) (pppoe-uplink-profile) # pppoe-chapsecret <password>
(Instant AP) (pppoe-uplink-profile) # pppoe-unnumbered-local-l3-dhcp-profile <dhcp-profile>
(Instant AP) (pppoe-uplink-profile) # end
(Instant AP) # commit apply
```

To view the PPPoE configuration:

```
(Instant AP) # show pppoe config
```

```
PPPoE Configuration
-----
Type Value
---- -----
User testUser
Password 3c28ec1b82d3eef0e65371da2f39c4d49803e5b2bc88be0c
Service name internet03
CHAP secret 8e87644deda9364100719e017f88ebce
Unnumbered dhcp profile dhcpProfile1
```

To view the PPPoE status:

```
(Instant AP) # show pppoe status
```

```
pppoe uplink state:Suppressed.
```

Cellular Uplink

AOS-W Instant supports the use of 3G and 4G USB modems to provide the Internet backhaul to an AOS-W Instant network. The 3G or 4G USB modems can be used to extend client connectivity to places where an Ethernet uplink cannot be configured. This enables the OAW-IAPs to automatically choose the available network in a specific region.



OAW-RAP155/155P devices do not support the high-speed option (HSO) module.



When UML290 runs in auto-detect mode, the modem can switch from 4G network to 3G network or vice-versa based on the signal strength. To configure the UML290 for the 3G network only, manually set the USB type to **pantech-3g**. To configure the UML290 for the 4G network only, manually set the 4G USB type to **pantech-lte**.

Configuring Cellular Uplink Profiles

You can configure 3G or 4G uplinks by using the AOS-W Instant UI or the CLI.

In the AOS-W Instant UI

To configure 3G/4G uplinks:

1. Click the **System** link on the AOS-W Instant main window.
2. In the **System** window, click the **show advanced settings** link.
3. Click the **Uplink** tab.
4. To configure a 3G or 4G uplink, select the **Country** and **ISP**.
5. Click **OK**.
6. Reboot the OAW-IAP for changes to take effect.

In the CLI

To configure 3G/4G uplink manually:

```
(Instant AP) (config) # cellular-uplink-profile
(Instant AP) (cellular-uplink-profile) # usb-type <3G-usb-type>
(Instant AP) (cellular-uplink-profile) # 4g-usb-type <4g-usb>
(Instant AP) (cellular-uplink-profile) # modem-country <country>
(Instant AP) (cellular-uplink-profile) # modem-isp <service-provider-name>
(Instant AP) (cellular-uplink-profile) # usb-auth-type <usb-authentication_type>
(Instant AP) (cellular-uplink-profile) # usb-user <username>
(Instant AP) (cellular-uplink-profile) # usb-passwd <password>
(Instant AP) (cellular-uplink-profile) # usb-dev <device-ID>
(Instant AP) (cellular-uplink-profile) # usb-tty <tty-port>
(Instant AP) (cellular-uplink-profile) # usb-init <Initialization-parameter>
(Instant AP) (cellular-uplink-profile) # usb-dial <dial-parameter>
(Instant AP) (cellular-uplink-profile) # usb-modeswitch <usb-modem>
(Instant AP) (cellular-uplink-profile) # end
(Instant AP) # commit apply
```

To switch a modem from the storage mode to modem mode:

```
(Instant AP) (cellular-uplink-profile) # usb-modeswitch <usb-modem>
```

To view the cellular configuration:

```
(Instant AP) # show cellular config
```

Managing Cellular SIM PIN

OAW-IAPs now support the Subscriber Identity Module (SIM) Personal Identification Number (PIN) management functions such as locking, unlocking, and renewing the SIM PIN of the 3G/4G modems. In the current release, these functions can be configured only through the OAW-IAP CLI.

To prevent any fraudulent use of 3G/4G modems connected to an OAW-IAP, you can enable locking of the SIM PIN of the modems. When enabled, if an incorrect PIN code is provided in the three consecutive attempts, the SIM PIN is locked. To unlock the PIN, the users must use the Personal Unblocking Code (PUK) code provided by your ISP.



After enabling SIM PIN lock, reboot the OAW-IAP to apply the SIM PIN lock configuration changes.

To enable SIM PIN lock:

```
(Instant AP) # pin-enable <pin_current_used>
```

To disable SIM PIN locking:

```
(Instant AP) # no pin-enable <pin_current_used>
```

To unlock a PIN with the PUK code provided by the operator:

```
(Instant AP) # pin-puk <pin_puk> <pin_new>
```

To renew the PIN:

```
(Instant AP) # pin-renew <pin_current> <pin_new>
```

Wi-Fi Uplink

The Wi-Fi uplink is supported on all the OAW-IAP models, except for the 802.11ac OAW-IAP models (OAW-IAP-2xx Series access points). However only the master OAW-IAP uses this uplink. The Wi-Fi allows uplink to open, PSK-CCMP, and PSK-TKIP SSIDs.

- For single-radio OAW-IAPs, the radio serves wireless clients and the Wi-Fi uplink.
- For dual-radio OAW-IAPs, both radios can be used to serve clients but only one of them can be used for the Wi-Fi uplink.



When the Wi-Fi uplink is in use, the client IP is assigned by the internal DHCP server.

Configuring a Wi-Fi Uplink Profile

The following configuration conditions apply to the Wi-Fi uplink:

- To bind or unbind the Wi-Fi uplink on the 5 GHz band, reboot the OAW-IAP.
- If the Wi-Fi uplink is used on the 5 GHz band, mesh is disabled. The two links are mutually exclusive.
- For OAW-IAPs to connect to an AOS-W Instant-based WLAN using Wi-Fi uplink, the switch must run AOS-W Instant 6.2.1.0 or later.

In the AOS-W Instant UI

To provision an OAW-IAP with the Wi-Fi uplink:

1. If you are configuring a Wi-Fi uplink after restoring factory settings on an OAW-IAP, connect the OAW-IAP to an Ethernet cable to allow the OAW-IAP to get the IP address. Otherwise, go to step 2.
2. Click the **System** link on the AOS-W Instant main window.
3. In the **System** section, click the **Show advanced options** link. The advanced options are displayed.
4. Click the **Uplink** tab.
5. Under **Wi-Fi**, enter the name of the wireless network that is used for the Wi-Fi uplink in the **Name (SSID)** text box.
6. Select the type of key for uplink encryption and authentication from the **Key management** drop-down list. If the uplink wireless router uses mixed encryption, WPA-2 is recommended for the Wi-Fi uplink.
7. Select the band in which the VC currently operates, from the **band** drop-down list. The following options are available:
 - 2.4 GHz (default)
 - 5 GHz
8. Select a passphrase format from the **Passphrase format** drop-down list. The following options are available:
 - 8–63 alphanumeric characters
 - 64 hexadecimal characters



Ensure that the hexadecimal password string is exactly 64 digits in length.

9. Enter a Pre-Shared Key (PSK) passphrase in the **Passphrase** text box and click **OK**.

10. Navigate to **System > General > Show Advanced Options** view and set the **Extended SSID** parameter to **Disabled**.
11. Reboot the OAW-IAP to apply the changes. After the OAW-IAP reboot, the Wi-Fi and mesh links are automatically enabled.

In the CLI

To configure Wi-Fi uplink on an OAW-IAP:

```
(Instant AP) (config) # wlan sta-profile
(Instant AP) (sta uplink)# cipher-suite<clear | wpa-tkip-psk | wpa2-ccmp-psk>
(Instant AP) (sta uplink)# essid <ssid>
(Instant AP) (sta uplink)# uplink-band <band>
(Instant AP) (sta uplink)# wpa-passphrase <key>
(Instant AP) (sta uplink)# end
(Instant AP) # commit apply
```

To view the W-Fi uplink status in the CLI:

```
(Instant AP)# show wifi-uplink status
configured :NO
```

To view the configuration status in the CLI:

```
(Instant AP)# show wifi-uplink config
```

```
ESSID :
Cipher Suite :
Passphrase :
Band :
```

```
(Instant AP)# show wifi-uplink auth log
```

```
-----
wifi uplink auth configuration:
-----
```

```
wifi uplink auth log:
-----
```

```
[11116]2000-01-01 00:00:45.625: Global control interface '/tmp/supp_gbl'
```

Uplink Preferences and Switching

This topic describes the following procedures:

- [Enforcing Uplinks on page 324](#)
- [Setting an Uplink Priority on page 325](#)
- [Enabling Uplink Preemption on page 325](#)
- [Switching Uplinks Based on VPN and Internet Availability on page 326](#)
- [Viewing Uplink Status and Configuration on page 328](#)

Enforcing Uplinks

The following configuration conditions apply to the uplink enforcement:

- When an uplink is enforced, the OAW-IAP uses the specified uplink as the primary uplink regardless of uplink preemption configuration and the current uplink status.
- When an uplink is enforced and multiple Ethernet ports are configured, and if the uplink is enabled on the wired profiles, the OAW-IAP tries to find an alternate Ethernet link based on the priority configured.

- When no uplink is enforced and preemption is not enabled, and if the current uplink fails, the OAW-IAP tries to find an available uplink based on the priority configured. The uplink with the highest priority is used as the primary uplink. For example, if Wi-Fi-sta has the highest priority, it is used as the primary uplink.
- When no uplink is enforced and preemption is enabled, and if the current uplink fails, the OAW-IAP tries to find an available uplink based on the priority configured. If current uplink is active, the OAW-IAP periodically tries to use a higher-priority uplink and switches to the higher-priority uplink even if the current uplink is active.

You can enforce a specific uplink on an OAW-IAP by using the AOS-W Instant UI or the CLI.

In the AOS-W Instant UI

To enforce an uplink:

1. Click the **System > show advanced settings > Uplink**. The **Uplink** tab contents are displayed.
2. Under **Management**, select the type of uplink from the **Enforce Uplink** drop-down list. If Ethernet uplink is selected, the **Port** text box is displayed.
3. Specify the Ethernet interface port number.
4. Click **OK**. The selected uplink is enforced on the OAW-IAP.

In the CLI

To enforce an uplink:

```
(Instant AP) (config)# uplink
(Instant AP) (uplink)# enforce {cellular|ethernet | wifi | none}
(Instant AP) (uplink)# end
(Instant AP)# commit apply
```

Setting an Uplink Priority

You can set an uplink priority by using the AOS-W Instant UI or the CLI.

In the AOS-W Instant UI

Setting an uplink priority:

1. Click **System > show advanced settings > Uplink**.
2. Under **Uplink Priority List**, select the uplink, and click the icons in the **Uplink Priority List** section, to increase or decrease the priority. By default, the Eth0 uplink is set as a high-priority uplink.
3. Click **OK**. The selected uplink is prioritized over other uplinks.

In the CLI

Setting an uplink priority:

```
(Instant AP) (config)# uplink
(Instant AP) (uplink)# uplink-priority {cellular <priority> | ethernet <priority> | [port
<Interface-number> <priority>] | wifi <priority>}
(Instant AP) (uplink)# end
(Instant AP)# commit apply
```

Setting an Ethernet uplink priority :

```
(Instant AP) (uplink)# uplink-priority ethernet port 0 1
(Instant AP) (uplink)# end
(Instant AP)# commit apply
```

Enabling Uplink Preemption

The following configuration conditions apply to uplink preemption:

- Preemption can be enabled only when no uplink is enforced.

- When preemption is disabled and the current uplink goes down, the OAW-IAP tries to find an available uplink based on the uplink priority configuration.
- When preemption is enabled and if the current uplink is active, the OAW-IAP periodically tries to use a higher-priority uplink, and switches to a higher-priority uplink even if the current uplink is active.

You can enable uplink preemption by using AOS-W Instant UI or the CLI.

In the AOS-W Instant UI

To enable uplink preemption:

1. Click **System > show advanced settings > Uplink**. The **Uplink** tab contents are displayed.
2. Under **Management**, ensure that the **Enforce Uplink** is set to none.
3. Select **Enabled** from the **Pre-emption** drop-down list.
4. Click **OK**.

In the CLI

To configure uplink preemption:

```
(Instant AP) (config)# uplink
(Instant AP) (uplink)# preemption
(Instant AP) (uplink)# end
(Instant AP)# commit apply
```

Switching Uplinks Based on VPN and Internet Availability

The default priority for uplink switchover is Ethernet and then 3G/4G. The OAW-IAP can switch to the lower-priority uplink if the current uplink is down.

Switching Uplinks Based on VPN Status

AOS-W Instant supports switching uplinks based on the VPN status when deploying multiple uplinks (Ethernet, 3G/4G, and Wi-Fi). When VPN is used with multiple backhaul options, the OAW-IAP switches to an uplink connection based on the VPN connection status, instead of only using the Ethernet or the physical backhaul link.

The following configuration conditions apply to uplink switching:

- If the current uplink is Ethernet and the VPN connection is down, the OAW-IAP tries to reconnect to VPN. The retry time depends on the fast failover configuration and the primary or backup VPN tunnel. If this fails, the OAW-IAP waits for the VPN failover timeout and selects a different uplink such as 3G/4G or Wi-Fi.
- If the current uplink is 3G or Wi-Fi, and Ethernet has a physical link, the OAW-IAP periodically suspends user traffic to try and connect to the VPN on the Ethernet. If the OAW-IAP succeeds, the OAW-IAP switches to Ethernet. If the OAW-IAP does not succeed, it restores the VPN connection to the current uplink.

Uplink switching based on VPN status is automatically enabled if VPN is configured on the OAW-IAP. However, you can specify the duration in the **VPN failover timeout** text box to wait for an uplink switch. By default, this duration is set to 180 seconds. The OAW-IAP monitors the VPN status and when the VPN connection is not available for 3 minutes, the uplink switches to another available connection (if a low-priority uplink is detected and the uplink preference is set to none). When **VPN failover timeout** is set to 0, uplink does not switch over.

When uplink switching based on the Internet availability is enabled, the uplink switching based on VPN failover is automatically disabled.

Switching Uplinks Based on Internet Availability

You can configure AOS-W Instant to switch uplinks based on Internet availability.

When the uplink switchover based on Internet availability is enabled, the OAW-IAP continuously sends Internet Control Management Protocol (ICMP) packets to some well-known Internet servers. If the request is timed out due to a bad uplink connection or uplink interface failure, and the public Internet is not reachable from the current uplink, the OAW-IAP switches to a different connection.

You can set preferences for uplink switching by using the AOS-W Instant UI and the CLI.

In the AOS-W Instant UI

To configure uplink switching:

1. Click **System > show advanced settings > Uplink**. The **Uplink** tab contents are displayed.
2. Under **Management**, configure the following parameters:
 - **VPN failover timeout**—To configure uplink switching based on VPN status, specify the duration to wait for an uplink switch. The default duration is set to 180 seconds.
 - **Internet failover**—To configure uplink switching based on Internet availability, perform the following steps:
 - a. Select **Enabled** from the **Internet failover** drop-down list.
 - b. Specify the required values for the following parameters:
 - **Max allowed test packet loss**—The maximum number of ICMP test packets that are allowed to be lost to determine if the OAW-IAP must switch to a different uplink connection. You can specify a value within the range of 1–1000.
 - **Secs between test packets**—The frequency at which ICMP test packets are sent. You can specify a value within the range of 1–3600 seconds.
 - **Internet check timeout**—Internet check timeout is the duration for the test packet timeout. You can specify a value within the range of 0–3600 seconds and the default value is 10 seconds.
 - **Internet failover IP**—To configure an IP address to which the OAW-IAP must send OAW-IAP packets and verify if the Internet is reachable when the uplink is down. By default, the master OAW-IAP sends the ICMP packets to 8.8.8.8 IP address only if the out-of-service operation based on Internet availability (internet-down state) is configured on the SSID.
3. Click **OK**.



When **Internet failover** is enabled, the OAW-IAP ignores the VPN status, although uplink switching based on VPN status is enabled.

In the CLI

To enable uplink switching based on VPN status:

```
(Instant AP) (config) # uplink
(Instant AP) (uplink) # failover-vpn-timeout <seconds>
(Instant AP) (uplink) # end
(Instant AP) # commit apply
```

To enable uplink switching based on Internet availability:

```
(Instant AP) (config) # uplink
(Instant AP) (uplink) # failover-internet
(Instant AP) (uplink) # failover-internet-ip <ip>
(Instant AP) (uplink) # failover-internet-pkt-lost-cnt <count>
(Instant AP) (uplink) # failover-internet-pkt-send-freq <frequency>
(Instant AP) (uplink) # end
(Instant AP) # commit apply
```

Viewing Uplink Status and Configuration

To view the uplink status:

```
(Instant AP)# show uplink status
Uplink preemption           :enable
Uplink preemption interval  :600
Uplink enforce              :none
Ethernet uplink eth0       :DHCP
Uplink Table
-----
Type      State  Priority  In Use
-----  -
eth0      UP     2         Yes
Wifi-sta  INIT   1         No
3G/4G     INIT   3         No
Internet failover           :enable
Internet failover IP       :192.2.0.1
Max allowed test packet loss :10
Secs between test packets   :30
VPN failover timeout (secs) :180
Internet check timeout (secs) :10
ICMP pkt sent               :1
ICMP pkt lost               :1
Continuous pkt lost         :1
VPN down time                :0
AP1X type:NONE
Certification type:NONE
Validate server:NONE
```

To view the uplink configuration in the CLI:

```
(Instant AP)# show uplink config
Uplink preemption           :enable
Uplink preemption interval  :600
Uplink enforce              :none
Ethernet uplink eth0       :DHCP
Internet failover           :disable
Max allowed test packet loss :10
Secs between test packets   :30
VPN failover timeout (secs) :180
Internet check timeout (secs) :10
Secs between test packets   :30
```


The 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.

The IDS feature in the AOS-W Instant network enables you to detect rogue OAW-IAPs, interfering OAW-IAPs, and other devices that can potentially disrupt network operations.

This chapter describes the following procedures:

- [Detecting and Classifying Rogue OAW-IAPs on page 329](#)
- [OS Fingerprinting on page 329](#)
- [Configuring Wireless Intrusion Protection and Detection Levels on page 330](#)
- [Configuring IDS on page 335](#)

Detecting and Classifying Rogue OAW-IAPs

A rogue OAW-IAP is an unauthorized OAW-IAP plugged into the wired side of the network.

An interfering OAW-IAP is an OAW-IAP seen in the RF environment but it is not connected to the wired network. While the interfering OAW-IAP can potentially cause RF interference, it is not considered a direct security threat, because it is not connected to the wired network. However, an interfering OAW-IAP may be reclassified as a rogue OAW-IAP.

To detect the rogue OAW-IAPs, click the **IDS** link in the AOS-W Instant main window. The built-in IDS scans for access points that are not controlled by the VC. These are listed and classified as either Interfering or Rogue, depending on whether they are on a foreign network or your network.

Figure 95 *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:82:48:72	docomo	Interfering	1	G	11:31:07		00:26:c6:b7:7a:76	ethersphere-voip	Interfering	1	GN 20MZ	11:31:07	
00:0b:86:b6:29:31	NTT-SPOT	Interfering	1	G	11:31:07		1c1b0:94:a1:9e:b6	ethersphere-wpa2	Interfering	1	GN 20MZ	11:31:07	
00:24:6c:80:a4:b2	docomo	Interfering	1	G	11:31:07		58:94:6b:57:50:38	ethersphere-wpa2	Interfering	1	GN 20MZ	11:31:07	
00:24:6c:0f:9d:42	docomo	Interfering	1	G	11:31:07		24:77:03:7a:67:5c	UL_Dashboard	Interfering	1	G	11:31:07	
00:24:6c:b0:bce:e2	docomo	Interfering	1	G	11:31:07		00:1e:65:30:7e:d8	ethersphere-wpa2	Interfering	1	GN 20MZ	11:30:51	
00:24:6c:ae:9a:d0	aruba-ap	Interfering	1	GN 20MZ	11:31:07		04:46:65:8c:0b:ea	ethersphere-wpa2	Interfering	1	GN 20MZ	11:30:35	
00:0b:86:b6:34:b2	docomo	Interfering	1	G	11:31:07		24:77:03:7a:65:ac	ipv6-alpha	Interfering	1	GN 20MZ	11:30:35	
00:0b:86:b6:29:32	docomo	Interfering	1	G	11:31:07		00:37:6d:e2:df:b2	ethersphere-voip	Interfering	1	GN 20MZ	11:30:20	
00:24:6c:33:0e:11	NTT-SPOT	Interfering	1	G	11:31:07		00:03:2a:02:5b:b7	skvoicel	Interfering	1	G	11:30:20	
8cf3:7f:18:6d:08	hotspot_sach	Interfering	157	AN 40MZ	11:31:07		20:02:af:9e:5b:b5	ethersphere-wpa2	Interfering	1	GN 20MZ	11:29:34	
00:24:6c:33:0e:12	docomo	Interfering	1	G	11:31:07		00:17:ca:9e:7a:a6	ethersphere-voip	Interfering	1	B	11:29:05	
8cf3:7f:18:6d:20	nrvap1	Interfering	1	GN 20MZ	11:31:07		84:29:99:11:35:0d	mdns-roaming	Interfering	11	GN 20MZ	11:29:05	
48:c7:e8:27:33:65	sandip-test	Interfering	11	GN 20MZ	11:31:07		5c:0a:5b:13:a5:cd	ethersphere-voip	Interfering	11	GN 20MZ	11:28:50	
00:24:6c:0b:30:40	ZSPOT	Interfering	1	GN 20MZ	11:31:07		20:64:32:51:fc:3f	ipv6-alpha	Interfering	1	GN 20MZ	11:27:49	
00:24:6c:06:82:d0	ZSPOT	Interfering	1	GN 20MZ	11:31:07		20:64:32:81:d2:37	ethersphere-wpa2	Interfering	1	BN 20MZ	11:23:34	
00:24:6c:80:4b:f1	ARUBA-VISITOR	Interfering	1	GN 20MZ	11:31:07		58:94:6b:31:cf:00	mdns-roaming	Interfering	11	B	11:21:49	
00:0b:86:70:4b:61	san-mdns-pak	Interfering	1	GN 20MZ	11:31:07		00:16:6f:31:8b:8a	UL_Dashboard	Interfering	6	G	11:18:18	
48:c7:e8:27:33:c2	Milford_Staff	Interfering	1	GN 20MZ	11:31:07		00:26:c6:b6:6b:b8	ethersphere-voip	Interfering	6	GN 20MZ	11:18:18	

OS Fingerprinting

The OS Fingerprinting feature gathers information about the client that is connected to the AOS-W 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 AOS-W Instant network by default. The following operating systems are identified by AOS-W Instant:

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

Configuring Wireless Intrusion Protection and Detection Levels

WIP offers a wide selection of intrusion detection and protection features to protect the network against wireless threats.

Like most other security-related features of the AOS-W Instant network, the WIP can be configured on the OAW-IAP.

You can configure the following options:

- **Infrastructure Detection Policies**—Specifies the policy for detecting wireless attacks on access points.
- **Client Detection Policies**—Specifies the policy for detecting wireless attacks on clients.
- **Infrastructure Protection Policies**—Specifies the policy for protecting access points from wireless attacks.
- **Client Protection Policies**—Specifies the policy for protecting clients from wireless attacks.
- **Containment Methods**—Prevents unauthorized stations from connecting to your AOS-W Instant network.

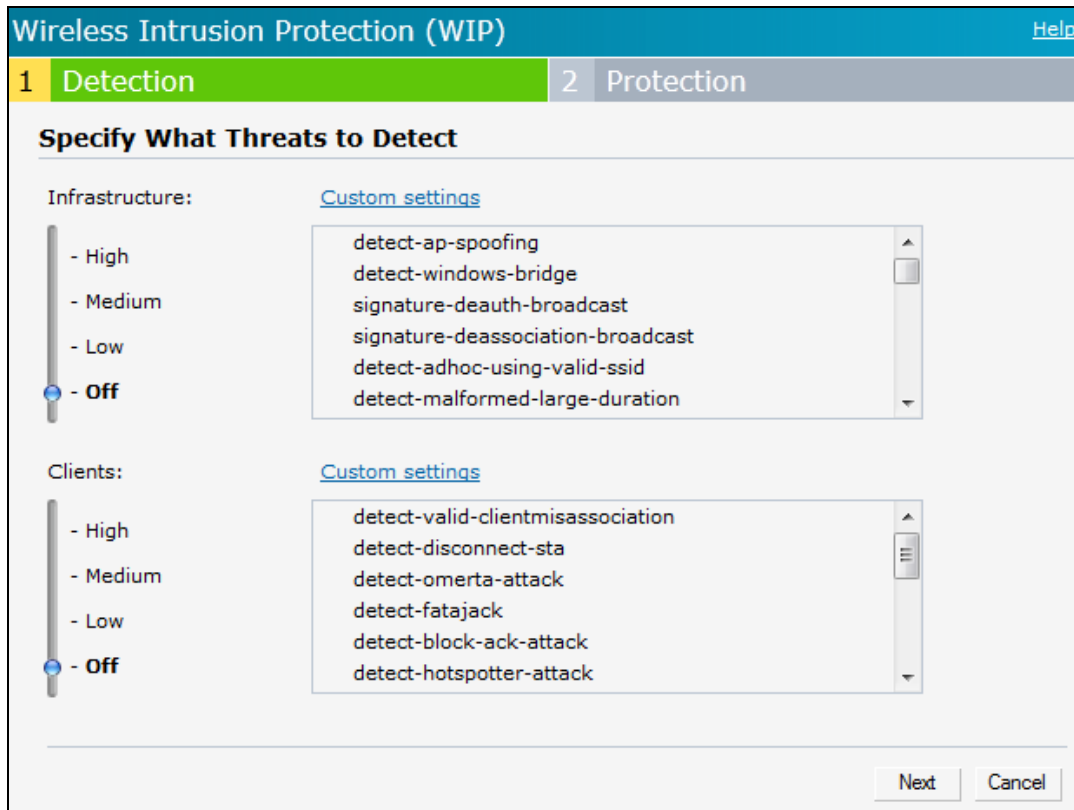
Each of these options contains several default levels that enable different sets of policies. An administrator can customize, enable, or disable these options accordingly.

The detection levels can be configured using the **IDS** window. To view the IDS window, click **More > IDS** link on the Instant main window.

The following levels of detection can be configured in the WIP Detection page:

- Off
- Low
- Medium
- High

Figure 96 *Wireless Intrusion Detection*



The following table describes the detection policies enabled in the Infrastructure Detection **Custom settings** text box:

Table 67: *Infrastructure Detection Policies*

Detection Level	Detection Policy
Off	Rogue Classification
Low	<ul style="list-style-type: none"> • Detect OAW-IAP Spoofing • Detect Windows Bridge • IDS Signature—Deauthentication Broadcast • IDS Signature—Deassociation Broadcast
Medium	<ul style="list-style-type: none"> • Detect ad hoc networks using VALID SSID—Valid SSID list is autoconfigured based on Instant OAW-IAP configuration • Detect Malformed Frame—Large Duration
High	<ul style="list-style-type: none"> • Detect OAW-IAP Impersonation • Detect ad hoc Networks • Detect Valid SSID Misuse • Detect Wireless Bridge • Detect 802.11 40 MHz intolerance settings • Detect Active 802.11 n Greenfield Mode

Table 67: *Infrastructure Detection Policies*

Detection Level	Detection Policy
	<ul style="list-style-type: none">• Detect OAW-IAP 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 enabled in the Client Detection **Custom settings** text box.

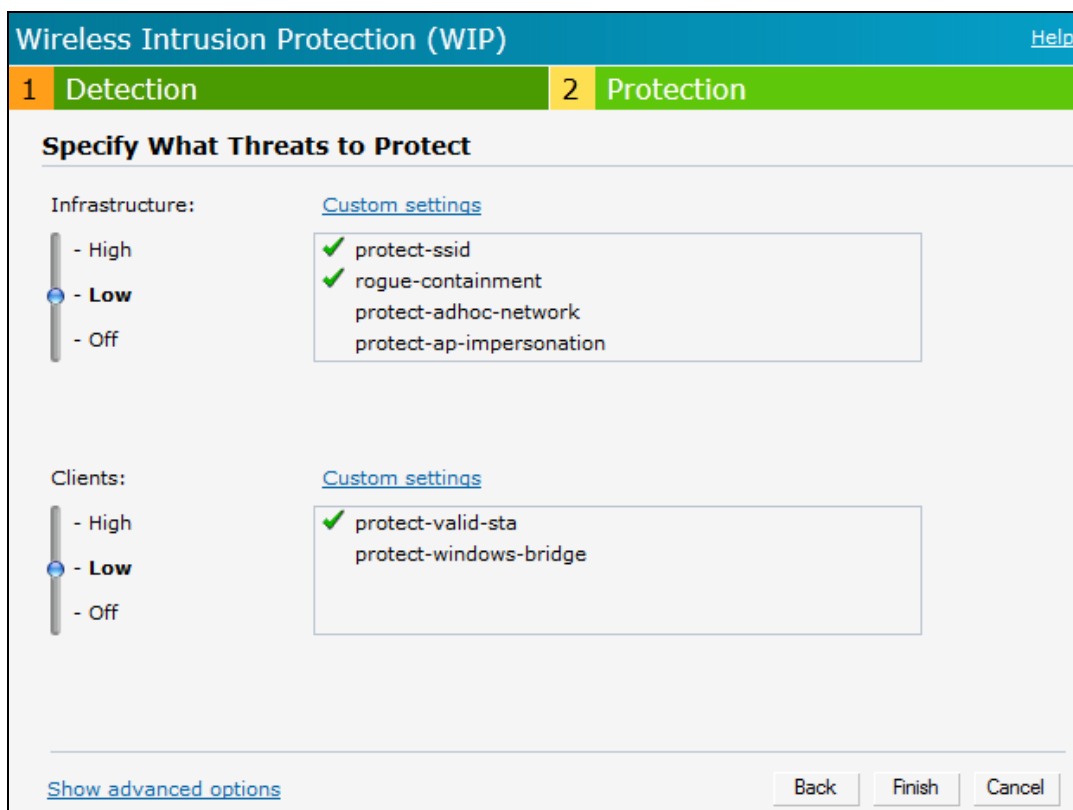
Table 68: *Client Detection Policies*

Detection Level	Detection Policy
Off	All detection policies are disabled.
Low	<ul style="list-style-type: none">• Detect Valid Station Misassociation
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

The following levels of detection can be configured in the WIP Protection page:

- Off
- Low
- High

Figure 97 *Wireless Intrusion Protection*



The following table describes the protection policies that are enabled in the Infrastructure Protection **Custom settings** text box:

Table 69: *Infrastructure Protection Policies*

Protection Level	Protection Policy
Off	All protection 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 ad hoc Networks Protect OAW-IAP Impersonation

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

Table 70: *Client Protection Policies*

Protection Level	Protection Policy
Off	All protection policies are disabled
Low	Protect Valid Station
High	Protect Windows Bridge

Containment Methods

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

AOS-W Instant supports the following types of containment mechanisms:

- Wired containment—When enabled, OAW-IAPs generate ARP packets on the wired network to contain wireless attacks.
 - wired-containment-ap-adj-mac—Enables a wired containment to Rogue OAW-IAPs whose wired interface MAC address is offset by one from its BSSID.
 - wired-containment-susp-l3-rogue—Enables the users to identify and contain an OAW-IAP with a preset MAC address that is different from the BSSID of the OAW-IAP, if the MAC address that the OAW-IAP provides is offset by one character from its wired MAC address.



Enable the **wired-containment-susp-l3-rogue** parameter only when a specific containment is required, to avoid a false alarm.

- Wireless containment—When enabled, the system attempts to disconnect all clients that are connected or attempting to connect to the identified Access Point.
 - None—Disables all the containment mechanisms.
 - Deauthenticate only—With deauthentication containment, the Access Point or client is contained by disrupting the client association on the wireless interface.
 - Tarpit containment—With Tarpit containment, the Access Point is contained by luring clients that are attempting to associate with it to a tarpit. The tarpit can be on the same channel or a different channel as the Access Point being contained.

Figure 98 Containment Methods

Configuring IDS

The IDS policy for OAW-IAPs can be created using the CLI.

To configure IDS using CLI:

```
(Instant AP) (config)# ids
(Instant AP) (IDS)# infrastructure-detection-level <type>
(Instant AP) (IDS)# client-detection-level <type>
(Instant AP) (IDS)# infrastructure-protection-level <type>
(Instant AP) (IDS)# client-protection-level <type>
(Instant AP) (IDS)# wireless-containment <type>
(Instant AP) (IDS)# wired-containment
(Instant AP) (IDS)# wired-containment-ap-adj-mac
(Instant AP) (IDS)# wired-containment-susp-l3-rogue
(Instant AP) (IDS)# detect-ap-spoofing
(Instant AP) (IDS)# detect-windows-bridge
(Instant AP) (IDS)# signature-deauth-broadcast
(Instant AP) (IDS)# signature-deassociation-broadcast
(Instant AP) (IDS)# detect-adhoc-using-valid-ssid
(Instant AP) (IDS)# detect-malformed-large-duration
(Instant AP) (IDS)# detect-ap-impersonation
(Instant AP) (IDS)# detect-adhoc-network
(Instant AP) (IDS)# detect-valid-ssid-misuse
(Instant AP) (IDS)# detect-wireless-bridge
(Instant AP) (IDS)# detect-ht-40mhz-intolerance
(Instant AP) (IDS)# detect-ht-greenfield
(Instant AP) (IDS)# detect-ap-flood
(Instant AP) (IDS)# detect-client-flood
(Instant AP) (IDS)# detect-bad-wep
(Instant AP) (IDS)# detect-cts-rate-anomaly
(Instant AP) (IDS)# detect-rts-rate-anomaly
(Instant AP) (IDS)# detect-invalid-addresscombination
(Instant AP) (IDS)# detect-malformed-htie
(Instant AP) (IDS)# detect-malformed-assoc-req
(Instant AP) (IDS)# detect-malformed-frame-auth
(Instant AP) (IDS)# detect-overflow-ie
(Instant AP) (IDS)# detect-overflow-eapol-key
(Instant AP) (IDS)# detect-beacon-wrong-channel
(Instant AP) (IDS)# detect-invalid-mac-oui
(Instant AP) (IDS)# detect-valid-clientmisassociation
(Instant AP) (IDS)# detect-disconnect-sta
(Instant AP) (IDS)# detect-omerta-attack
(Instant AP) (IDS)# detect-fatajack
(Instant AP) (IDS)# detect-block-ack-attack
(Instant AP) (IDS)# detect-hotspotter-attack
(Instant AP) (IDS)# detect-unencrypted-valid
(Instant AP) (IDS)# detect-power-save-dos-attack
(Instant AP) (IDS)# detect-eap-rate-anomaly
(Instant AP) (IDS)# detect-rate-anomalies
(Instant AP) (IDS)# detect-chopchop-attack
(Instant AP) (IDS)# detect-tkip-replay-attack
(Instant AP) (IDS)# signature-airjack
(Instant AP) (IDS)# signature-asleep
(Instant AP) (IDS)# protect-ssid
(Instant AP) (IDS)# rogue-containment
(Instant AP) (IDS)# protect-adhoc-network
(Instant AP) (IDS)# protect-ap-impersonation
(Instant AP) (IDS)# protect-valid-sta
(Instant AP) (IDS)# protect-windows-bridge
(Instant AP) (IDS)# end
(Instant AP) # commit apply
```

This chapter provides the following information:

- [Mesh Network Overview on page 336](#)
- [Setting up AOS-W Instant Mesh Network on page 337](#)
- [Configuring Wired Bridging on Ethernet 0 for Mesh Point on page 337](#)

Mesh Network Overview

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

Mesh OAW-IAPs

Mesh network requires at least one valid uplink (wired or 3G) connection. Any provisioned OAW-IAP that has a valid uplink (wired or 3G) functions as a mesh portal, and the OAW-IAP without an Ethernet link functions as a mesh point. The mesh portal can also act as a VC. Mesh portals and mesh points are also known as mesh nodes, a generic term used to describe OAW-IAPs configured for mesh.

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

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

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

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



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

For OAW-IAP-RW variants, the mesh network must be provisioned for the first time by plugging into the wired network. After that, mesh works on OAW-IAP-RWs like any other regulatory domain.

Mesh Portals

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

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



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

Mesh Points

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



A mesh point also supports LAN bridging. You can connect any wired device to the downlink port of the mesh point. In the case of single Ethernet port platforms such as OAW-IAP105, you can convert the Eth0 uplink port to a downlink port by enabling **Eth0 Bridging**. For additional information, see [Configuring Wired Bridging on Ethernet 0 for Mesh Point on page 337](#).

Setting up AOS-W Instant Mesh Network

Starting from AOS-W Instant 6.4.0.2-4.1.0.0 release, mesh functionality is disabled by default, because of which over-the-air provisioning of mesh OAW-IAPs is not supported.

To provision OAW-IAPs as mesh OAW-IAPs:

1. Connect the OAW-IAPs to a wired switch.
2. Ensure that the VC key is synchronized and the country code is configured.
3. Ensure that a valid SSID is configured on the OAW-IAP.
4. If the OAW-IAP has a factory default SSID (AOS-W Instant SSID), delete the SSID.
5. If an extended SSID (ESSID) is enabled on the VC, disable it and reboot the OAW-IAP cluster.
6. Disconnect the OAW-IAPs that you want to deploy as mesh points from the switch, and place the OAW-IAPs at a remote location. The OAW-IAPs come up without any wired uplink connection and function as mesh points. The OAW-IAPs with valid uplink connections function as mesh portals.



AOS-W Instant does not support the topology in which the OAW-IAPs are connected to the downlink Ethernet port of a mesh point.

Configuring Wired Bridging on Ethernet 0 for Mesh Point

AOS-W Instant supports wired bridging on the Enet0 port of an OAW-IAP. If OAW-IAP is configured to function as a mesh point, you can configure wired bridging.



Enabling wired bridging on this port of an OAW-IAP makes the port available as a downlink wired bridge and allows client access through the port.



When using 3G uplink, the wired port will be used as downlink.

You can configure support for wired bridging on the Enet0 port of an OAW-IAP by using the AOS-W Instant UI or the CLI.

In the AOS-W Instant UI

To configure Ethernet bridging:

1. On the **Access Points** tab, click the OAW-IAP to modify.
2. Click the **edit** link.
3. Click the **Uplink** tab.
4. Select **Enable** from the **Eth0 Bridging** drop-down list.
5. Click **OK**.
6. Reboot the OAW-IAP.

In the CLI

To configure Ethernet bridging:

```
(Instant AP)# enet0-bridging
```



Make the necessary changes to the wired-profile when eth0 is used as the downlink port. For more information, see [Configuring a Wired Profile on page 106](#).

This chapter provides the following information:

- [Layer-3 Mobility Overview](#) on page 339
- [Configuring L3-Mobility](#) on page 340

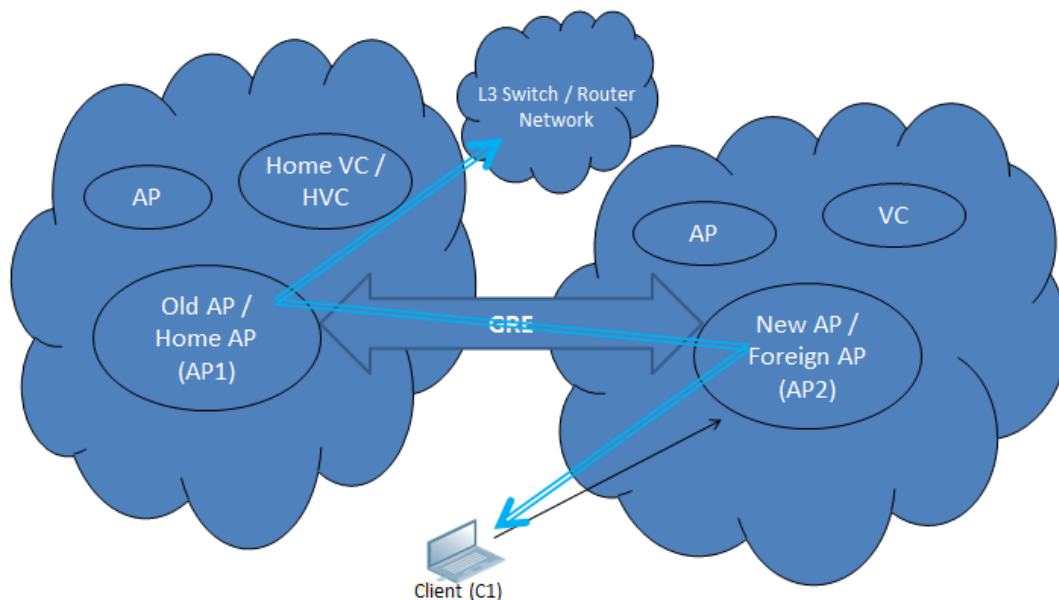
Layer-3 Mobility Overview

OAW-IAPs form a single AOS-W Instant network when they are in the same Layer-2 (L2) domain. As the number of clients increase, multiple subnets are required to avoid broadcast overhead. In such a scenario, a client must be allowed to roam away from the AOS-W Instant network to which it first connected (home network) to another network supporting the same WLAN access parameters (foreign network) and continue its existing sessions.

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

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

Figure 99 Routing of traffic when the client is away from its home network



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

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

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

Configuring L3-Mobility

To configure a mobility domain, you have to specify the list of all AOS-W Instant networks that form the mobility domain. To allow clients to roam seamlessly among all the OAW-IAPs, specify the VC IP for each foreign subnet. You may include the local AOS-W Instant or VC IP address, so that the same configuration can be used across all AOS-W Instant networks in the mobility domain.

It is recommended that you configure all client subnets in the mobility domain.

When the client subnets are configured, note the following scenarios:

- If a client is from a local subnet, it is identified as a local client. When a local client starts using the IP address, L3 roaming is terminated.
- If the client is from a foreign subnet, it is identified as a foreign client. When a foreign client starts using the IP address, L3 roaming is set up.

Home Agent Load Balancing

Home Agent Load Balancing is required in large networks where multiple tunnels might terminate on a single border or lobby OAW-IAP and overload it. When load balancing is enabled, the VC assigns the home OAW-IAP for roamed clients by applying a *round robin* policy. With this policy, the load for the OAW-IAPs acting as Home Agents for roamed clients is uniformly distributed across the OAW-IAP cluster.

Configuring a Mobility Domain for AOS-W Instant

You can configure L3 mobility domain by using the AOS-W Instant UI or the CLI.

In the AOS-W Instant UI

To configure a mobility domain:

1. Click the **System** link on the AOS-W Instant main window.
2. In the **Services** section, click the **Show advanced options** link. The advanced options are displayed.
3. Click **L3 Mobility**. The L3 Mobility window is displayed.

Figure 100 L3 Mobility Window

Home agent load balancing:

Virtual Controller IP Addresses

IP address	Subnet mask	VLAN ID	Virtual controller IP
------------	-------------	---------	-----------------------

New Edit Delete

Subnets

IP address	Subnet mask	VLAN ID	Virtual controller IP
------------	-------------	---------	-----------------------

New Edit Delete

4. Select **Enabled** from the **Home agent load balancing** drop-down list. By default, home agent load balancing is disabled.
5. Click **New** in the **Virtual Controller IP Addresses** section, add the IP address of a VC that is part of the mobility domain, and click **OK**.
6. Repeat Steps 2 to 5, to add the IP addresses of all VC that form the L3 mobility domain.
7. Click **New** in the **Subnets** section and specify the following:
 - a. Enter the client subnet in the **IP address** text box.
 - b. Enter the mask in the **Subnet mask** text box.
 - c. Enter the VLAN ID of the home network in the **VLAN ID** text box.
 - d. Enter the home VC IP address for this subnet in the **Virtual controller IP** text box.
8. Click **OK**.

In the CLI

To configure a mobility domain:

```
(Instant AP) (config) # l3-mobility
(Instant AP) (L3-mobility) # home-agent-load-balancing
(Instant AP) (L3-mobility) # virtual-controller <IP-address>
(Instant AP) (L3-mobility) # subnet <IP-address> <subnet-mask> <VLAN-ID> <virtual-controller-IP-
address>
(Instant AP) (L3-mobility) # end
(Instant AP) # commit apply
```

This chapter provides the following information:

- [Understanding Spectrum Data on page 342](#)
- [Configuring Spectrum Monitors and Hybrid OAW-IAPs on page 348](#)

Understanding Spectrum Data

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

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

The spectrum monitor is fully supported on all OAW-IAPs/OAW-IAPs with a few exceptions:

- OAW-RAP155 does not support Spectrum from AOS-W Instant 6.3.1.1-4.0.0.0 release.
- OAW-IAP105 supports the dedicated Spectrum mode, but not the Hybrid Spectrum mode.
- OAW-IAP3 do not support Spectrum display in the AOS-W Instant UI.

The spectrum data is collected by each OAW-IAP spectrum monitor and hybrid OAW-IAP. The spectrum data is not reported to the VC. The **Spectrum** link is visible in the UI (Access Point view) only if you have enabled the Spectrum Monitoring feature.

You can view the following spectrum data in the UI:

- [Device List](#)
- [Non-Wi-Fi Interferers](#)
- [Channel Metrics](#)
- [Channel Details](#)
- [Spectrum Alerts](#)

Device List

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

To view the device list, click **Spectrum** in the dashboard. The following figure shows an example of the device list details.

Figure 101 *Device List*

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

Table 71 shows the device details that are displayed:

Table 71: *Device Summary and Channel Information*

Column	Description
Type	<p>Device type. This parameter can be any of the following:</p> <ul style="list-style-type: none"> • Audio FF (fixed frequency) • Bluetooth • Cordless base FH (frequency hopper) • Cordless phone FF (fixed frequency) • Cordless network FH (frequency hopper) • Generic FF (fixed frequency) • Generic FH (frequency hopper) • Generic interferer • Microwave • Microwave inverter • Video • Xbox <p>NOTE: For additional details about non-Wi-Fi device types shown in this table, see Non-Wi-Fi Interferer Types.</p>
ID	ID number assigned to the device by the spectrum monitor or hybrid OAW-IAP radio. Spectrum monitors and hybrid OAW-IAPs assign a unique spectrum ID per device type.
Cfreq	Center frequency of the signal sent from the device.
Bandwidth	Channel bandwidth used by the device.
Channels-affected	Radio channels affected by the wireless device.
Signal-strength	Strength of the signal sent from the device, represented in dBm.

Table 71: Device Summary and Channel Information

Column	Description
Duty-cycle	Device duty cycle. This value represents the percent of time the device broadcasts a signal.
Add-time	Time at which the device was first detected.
Update-time	Time at which the device's status was updated.

Non-Wi-Fi Interferers

The following table describes each type of non-Wi-Fi interferer detected by the Spectrum Monitor feature:

Table 72: Non-Wi-Fi Interferer Types

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

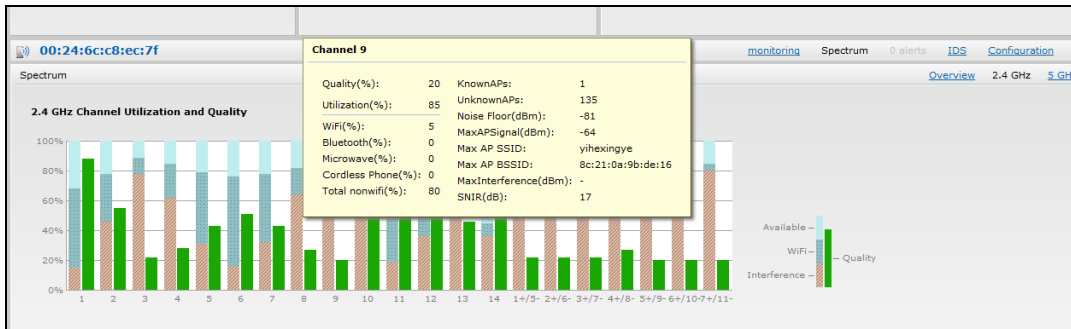
Table 72: Non-Wi-Fi Interferer Types

Non Wi-Fi Interferer	Description
Frequency Hopper (Xbox)	The Microsoft Xbox device uses a frequency hopping protocol in the 2.4 GHz band. These devices are classified as <i>Frequency Hopper (Xbox)</i> .
Frequency Hopper (Other)	When the classifier detects a frequency hopper that does not fall into any of the prior categories, it is classified as <i>Frequency Hopper (Other)</i> . Some examples include IEEE 802.11 FHSS devices, game consoles, and cordless/hands-free devices that do not use one of the known cordless phone protocols.
Microwave	Common residential microwave ovens with a single magnetron are classified as a <i>Microwave</i> . These types of microwave ovens may be used in cafeterias, break rooms, dormitories, and similar environments. Some industrial, healthcare, or manufacturing environments may also have other equipment that functions like a microwave and may also be classified as a Microwave device.
Microwave (Inverter)	Some newer-model microwave ovens have the inverter technology to control the power output and these microwave ovens may have a duty cycle close to 100%. These microwave ovens are classified as <i>Microwave (Inverter)</i> . Dual-magnetron industrial microwave ovens with higher duty cycle may also be classified as <i>Microwave (Inverter)</i> . There may be other equipment that functions like inverter microwaves in some industrial, healthcare, or manufacturing environments. Those devices may also be classified as <i>Microwave (Inverter)</i> .
Generic Interferer	Any non-frequency hopping device that does not fall into any of the prior categories described in this table is classified as a <i>Generic Interferer</i> . For example, a Microwave-like device that does not operate in the known operating frequencies used by the Microwave ovens may be classified as a <i>Generic Interferer</i> . Similarly wide-band interfering devices may be classified as <i>Generic Interferers</i> .

Channel Details

When you move the mouse over a channel, the channel details or the summary of the 2.4 GHz and 5 GHz channels as detected by a spectrum monitor are displayed. You can view the aggregate data for each channel seen by the spectrum monitor radio, including the maximum OAW-IAP power, interference, and the signal-to-noise-and-interference Ratio (SNIR). SNIR is the ratio of signal strength to the combined levels of interference and noise on that channel. Spectrum monitors display spectrum data of all channels in the selected band, and hybrid OAW-IAPs display data for the channel they are monitoring.

Figure 102 Channel Details



Channel Details Information shows the information that you can view in the Channel Details graph.

Table 73: Channel Details Information

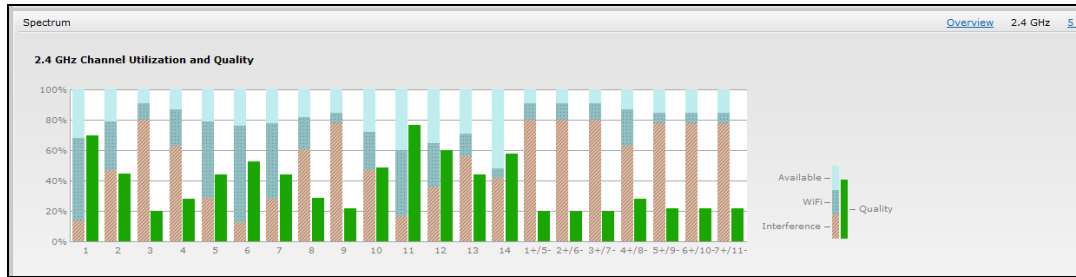
Column	Description
Channel	An 802.11a or 802.11g radio channel.
Quality(%)	Current relative quality of the channel.
Utilization(%)	The percentage of the channel being used.
Wi-Fi (%)	The percentage of the channel currently being used by Wi-Fi devices.
Type	Device type.
Total nonwifi (%)	The percentage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

Channel Metrics

The channel metrics graph displays channel quality, availability, and utilization metrics as seen by a spectrum monitor or hybrid OAW-IAP. You can view the channel utilization data based on 2 GHz and 5 GHz radio channels. The percentage of each channel that is currently being used by Wi-Fi devices, and the percentage of each channel being used by non-Wi-Fi devices and 802.11 adjacent channel interference (ACI). This chart shows the channel availability, the percentage of each channel that is available for use, and the current relative quality of selected channels in the 2.4 GHz or 5 GHz radio bands. While spectrum monitors can display data for all channels in their selected band, hybrid OAW-IAPs display data for a single monitored channel.

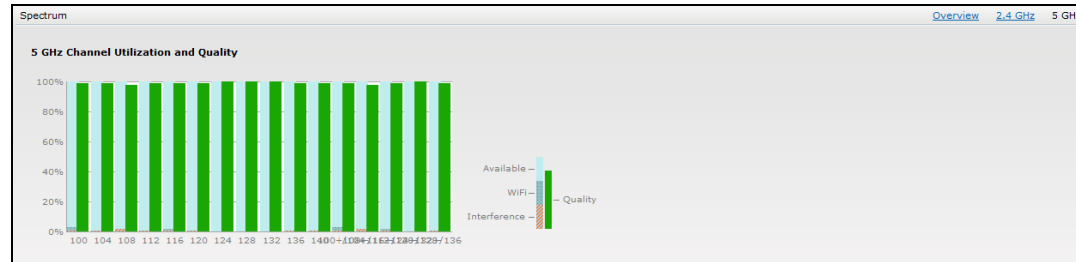
To view this graph, click **2.4 GHz** in the **Spectrum** section of the dashboard.

Figure 103 Channel Metrics for the 2.4 GHz Radio Channel



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

Figure 104 Channel Metrics for the 5 GHz Radio Channel



Channel Metrics shows the information displayed in the Channel Metrics graph.

Table 74: Channel Metrics

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

Spectrum Alerts

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

Configuring Spectrum Monitors and Hybrid OAW-IAPs

An OAW-IAP can be provisioned to function as a spectrum monitor or as a hybrid OAW-IAP. The radios on groups of OAW-IAPs can be converted to dedicated spectrum monitors or hybrid OAW-IAPs through the OAW-IAP group's 802.11a and 802.11g radio profiles.

Converting an OAW-IAP to a Hybrid OAW-IAP

You can convert all OAW-IAPs in an AOS-W Instant network into hybrid OAW-IAPs by selecting the **Background Spectrum Monitoring** option in the 802.11a and 802.11g radio profiles of an OAW-IAP. OAW-IAPs in **Access** mode continue to provide normal access service to clients, while providing the additional function of monitoring RF interference. If any OAW-IAP in the AOS-W Instant network does not support the Spectrum Monitoring feature, that OAW-IAP continues to function as a standard OAW-IAP, rather than a hybrid OAW-IAP. By default, the background spectrum monitoring option is disabled.

In the hybrid mode, spectrum monitoring is performed only on the home channel. In other words, if the OAW-IAP-channel width is 80 Mhz, spectrum monitoring is performed for 80 Mhz. If the channel width is 40, spectrum monitoring is performed for 40 MHz channel. In a dedicated air monitor mode, OAW-IAPs perform spectrum monitoring on all channels.

You can convert OAW-IAPs in an AOS-W Instant network to hybrid mode by using the AOS-W Instant UI or the CLI.

In the AOS-W Instant UI

To convert an OAW-IAP to a hybrid OAW-IAP:

1. Click the **RF** link on the AOS-W Instant main window.
2. In the **RF** section, click **Show advanced options** to view the **Radio** tab.
3. To enable a spectrum monitor on the 802.11g radio band, in the 2.4 GHz radio profile, select **Enabled** from the **Background Spectrum Monitoring** drop-down list.
4. To enable a spectrum monitor on the 802.11a radio band, in the 5 GHz radio profile, select **Enabled** from the **Background Spectrum Monitoring** drop-down list.
5. Click **OK**.

In the CLI

To configure 2.4 GHz radio settings:

```
(Instant AP) (config)# rf dot11g-radio-profile  
(Instant AP) (RF dot11g Radio Profile)# spectrum-monitor
```

To configure 5 GHz radio settings:

```
(Instant AP) (config)# rf dot11a-radio-profile  
(Instant AP) (RF dot11a Radio Profile)# spectrum-monitor
```

Converting an OAW-IAP to a Spectrum Monitor

In spectrum mode, spectrum monitoring is performed on entire bands and the OAW-IAP functions as a dedicated full-spectrum RF monitor, scanning all channels to detect interference, whether from the neighboring OAW-IAPs or from non-Wi-Fi devices such as microwaves and cordless phones.

By default, spectrum monitoring is performed on a higher band of the 5 GHz radio.

You can configure an OAW-IAP to function as a stand-alone spectrum monitor by using the AOS-W Instant UI or the CLI.

In the AOS-W Instant UI

To convert an OAW-IAP to a spectrum monitor:

1. In the **Access Points** tab, click the OAW-IAP that you want to convert to a spectrum monitor.
2. Click the **edit** link.
3. Click the **Radio** tab.
4. From the **Access Mode** drop-down list, select **Spectrum Monitor**.
5. Click **OK**.
6. Reboot the OAW-IAP for the changes to take effect.
7. To enable spectrum monitoring for any other band for the 5 GHz radio:
 - a. Click the **RF** link on the AOS-W Instantmain window.
 - b. In the **RF** section, click **Show advanced options** to view the **Radio** tab.
 - c. For the 5 GHz radio, specify the spectrum band you want that radio to monitor by selecting **Lower**, **Middle**, or **Higher** from the **Standalone spectrum band** drop-down list.
 - d. Click **OK**.

In the CLI

To convert an OAW-IAP to a spectrum monitor:

```
(Instant AP)# wifi0-mode {<access> | <monitor> | <spectrum-monitor>}  
(Instant AP)# wifi1-mode {<access> | <monitor> | <spectrum-monitor>}
```

To enable spectrum monitoring for any other band for the 5 GHz radio:

```
(Instant AP) (config)# rf dot11a-radio-profile  
(Instant AP) (RF dot11a Radio Profile)# spectrum-band <type>
```

To view the radio configuration:

```
(Instant AP)# show radio config  
2.4 GHz:  
Legacy Mode:disable  
Beacon Interval:100  
802.11d/802.11h:disable  
Interference Immunity Level:2  
Channel Switch Announcement Count:0  
Channel Reuse Type:disable  
Channel Reuse Threshold:0  
Background Spectrum Monitor:disable  
  
5.0 GHz:  
Legacy Mode:disable  
Beacon Interval:100  
802.11d/802.11h:disable  
Interference Immunity Level:2  
Channel Switch Announcement Count:0  
Channel Reuse Type:disable  
Channel Reuse Threshold:0  
Background Spectrum Monitor:disable  
Standalone Spectrum Band:5ghz-upper
```

This section provides information on the following procedures:

- [Upgrading an OAW-IAP on page 350](#)
- [Backing up and Restoring OAW-IAP Configuration Data on page 353](#)
- [Converting an OAW-IAP to a Remote AP and Campus AP on page 354](#)
- [Resetting a Remote AP or Campus AP to an OAW-IAP on page 360](#)
- [Rebooting the OAW-IAP on page 360](#)

Upgrading an OAW-IAP

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

Upgrading an OAW-IAP and Image Server

AOS-W Instant supports mixed OAW-IAP-class AOS-W Instant deployment with all OAW-IAPs as part of the same VC cluster.

Image Management Using OmniVista

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



The VC communicates with the OmniVista server if OmniVista is configured. If OmniVista is not configured on the OAW-IAP, the image is requested from the Image server.

Image Management Using Cloud Server

If the multiclass OAW-IAP network is not managed by OmniVista, image upgrades can be done through the Cloud-Based Image Check feature. When a new OAW-IAP joining the network needs to synchronize its software version with the version on the VC and if the new OAW-IAP belongs to a different class, the image file for the new OAW-IAP is provided by the cloud server.

Configuring HTTP Proxy on an OAW-IAP

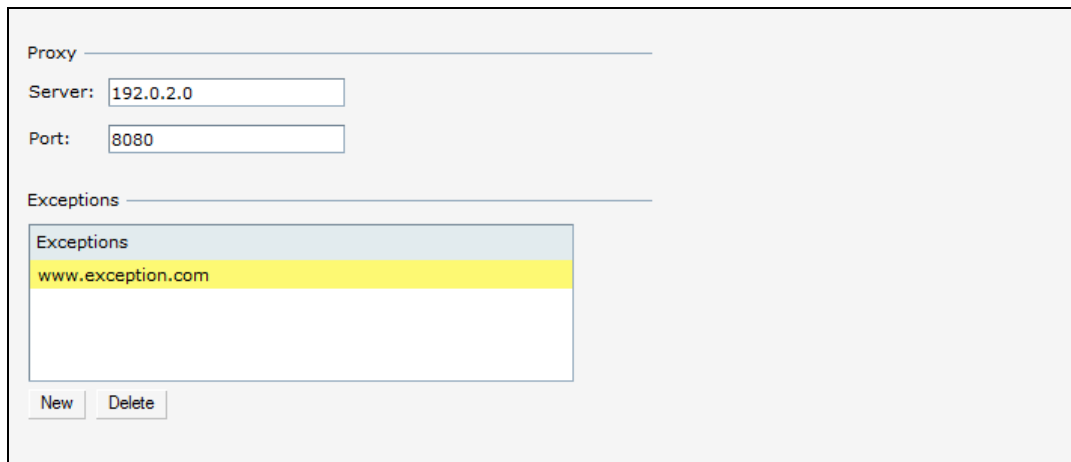
If your network requires a proxy server for Internet access, ensure that you configure the HTTP proxy on the OAW-IAP to download the image from the cloud server. After setting up the HTTP proxy settings, the OAW-IAP connects to the Activate server, AMP or OpenDNS server through a secure HTTP connection. You can also exempt certain applications from using the HTTP proxy (configured on an OAW-IAP) by providing their host name or IP address under exceptions.

In the AOS-W Instant UI

To configure the HTTP proxy settings:

1. Navigate to **System > Proxy**. The **Proxy** configuration window is displayed.

Figure 105 Proxy Configuration Window



2. Enter the HTTP proxy server IP address in the **Server** text box.
3. Enter the port number in the **Port** text box.
4. If you do not want the HTTP proxy to be applied for a particular host, click **New** to enter that IP address or domain name of that host in the **Exceptions** section.

In the CLI

To configure the HTTP proxy settings:

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

Upgrading an OAW-IAP Using Automatic Image Check

You can upgrade an OAW-IAP by using the Automatic Image Check feature. The automatic image checks are performed once, as soon as the OAW-IAP boots up and every week thereafter.

If the image check locates a new version of the AOS-W Instant software on the image server, the **New version available** link is displayed on the AOS-W Instant main window.



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

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

1. Go to **Maintenance > Automatic > Check for New Version**. After the image check is completed, one of the following messages is displayed:
 - 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 the version number is displayed.
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 is displayed:

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

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

Upgrading to a New Version Manually

If the Automatic Image Check feature is disabled, you can obtain an image file from a local file system or from a TFTP or HTTP URL.

To manually check for a new firmware image version and obtain an image file:

1. Navigate to **Maintenance > Firmware**.
2. Under **Manual** section, perform the following steps:
 - Select the **Image file** option. This method is only available for single-class OAW-IAPs. The following examples describe the image file format for different OAW-IAP models:
 - For OAW-IAP334/335—AlcatelInstant_Lupus_6.5.1.0-4.3.1.0.0_xxxx
 - For OAW-IAP314/315 and OAW-IAP324/325—AlcatelInstant_Hercules_6.5.1.0-4.3.1.0.0_xxxx
 - For OAW-IAP224/225, OAW-IAP228, OAW-IAP214/215, OAW-IAP274/275, OAW-IAP277—AlcatelInstant_Centaurus_6.5.1.0-4.3.1.0.0_xxxx
 - For OAW-IAP204/205 and OAW-IAP205H—AlcatelInstant_Taurus_6.5.1.0-4.3.1.0.0_xxxx
 - For OAW-RAP155/155P—AlcatelInstant_Aries_6.5.1.0-4.3.1.0.0_xxxx
 - For OAW-RAP108/109, OAW-IAP103, and OAW-IAP114/115—AlcatelInstant_Pegasus_6.5.1.0-4.3.1.0.0_xxxx
 - Select the **Image URL** option. Select this option to obtain an image file from a TFTP, FTP, or HTTP URL.
 - HTTP - http://<IP-address>/<image-file>. For example, http://<IP-address>/AlcatelInstant_Hercules_6.5.1.0-4.3.1.0.0_xxxx
 - TFTP - tftp://<IP-address>/<image-file>. For example, tftp://<IP-address>/AlcatelInstant_Hercules_6.5.1.0-4.3.1.0.0_xxxx
 - FTP - ftp://<IP-address>/<image-file>. For example, ftp://<IP-address>/AlcatelInstant_Hercules_6.5.1.0-4.3.1.0.0_xxxx
3. Clear the **Reboot all APs after upgrade** check box if required. The **Reboot all APs after upgrade** check box is selected by default to allow the OAW-IAPs to reboot automatically after a successful upgrade. To reboot the OAW-IAP at a later time, clear the **Reboot all APs after upgrade** check box.
4. Click **Upgrade Now** to upgrade the OAW-IAP to the newer version.

Upgrading an Image Using CLI

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

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

To upgrade an image without rebooting the OAW-IAP:

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

To view the upgrade information:

```
(Instant AP) # show upgrade info
```

```
Image Upgrade Progress
```

```
-----
Mac                IP Address  AP Class  Status  Image Info  Error Detail
----                -
d8:c7:c8:c4:42:98  10.17.101.1 Hercules  image-ok  image file  none
Auto reboot       :enable
```


Use external URL :disable

Backing up and Restoring OAW-IAP Configuration Data

You can back up the OAW-IAP configuration data and restore the configuration when required.

Viewing Current Configuration

To view the current configuration on the OAW-IAP:

- In the UI, navigate to **Maintenance > Configuration > Current Configuration**.
- In the CLI, enter the following command at the command prompt:

```
(Instant AP)# show running-config
```

Backing up Configuration Data

To back up the OAW-IAP configuration data:

1. Navigate to the **Maintenance > Configuration** page.
2. Click **Backup Configuration**.
3. Click **Continue** to confirm the backup. The *instant.cfg* containing the OAW-IAP configuration data is saved in your local file system.
4. To view the configuration that is backed up by the OAW-IAP, enter the following command at the command prompt:

```
(Instant AP)# show backup-config
```

Restoring Configuration

To restore configuration:

1. Navigate to the **Maintenance > Configuration** page.
2. Click **Restore Configuration**.
3. Click **Browse** to browse your local system and select the configuration file.
4. Click **Restore Now**.
5. Click **Restore Configuration** to confirm restoration. The configuration is restored and the OAW-IAP reboots to load the new configuration.

```
(Instant AP) (config)# copy config tftp://x.x.x.x/configi.cfg
```

Converting an OAW-IAP to a Remote AP and Campus AP

This section provides the following information:

- [Regulatory Domain Restrictions for OAW-IAP to RAP or CAP Conversion on page 354](#)
- [Converting an OAW-IAP to a Remote AP on page 356](#)
- [Converting an OAW-IAP to a Campus AP on page 359](#)
- [Converting an OAW-IAP to Stand-Alone Mode on page 359](#)
- [Converting an OAW-IAP using CLI on page 360](#)

Regulatory Domain Restrictions for OAW-IAP to RAP or CAP Conversion

You can provision an OAW-IAP as a Campus AP or a Remote AP in a switch-based network. Before converting an OAW-IAP, ensure that there is a regulatory domain match between the OAW-IAP and the switch.

The following table describes the regulatory domain restrictions that apply for the OAW-IAP-to-AOS-W Instant OAW-AP conversion:

Table 75: OAW-IAP-to-AOS-W Instant Conversion

OAW-IAP Variant	OAW-IAP Regulatory Domain	Switch Regulatory Domain			AOS-W Instant release
		US	Unrestricted	IS	
OAW-IAP314/315 OAW-IAP334/335	US	Y	X	X	AOS-W Instant 6.5.0.0 or later
	RW	X	Y	Y	
	JP	X	Y	X	
OAW-IAP324/325	US	Y	X	X	AOS-W Instant 6.4.4.0 or later
	RW	X	Y	Y	
	JP	X	Y	X	
OAW-IAP277	US	Y	X	X	AOS-W Instant 6.4.3.0 or later
	RW	X	Y	Y	
	JP	X	Y	X	
OAW-IAP228	US	Y	X	X	AOS-W Instant 6.4.3.0 or later
	RW	X	Y	Y	
	JP	X	Y	X	

Table 75: OAW-IAP-to-AOS-W Instant Conversion

OAW-IAP Variant	OAW-IAP Regulatory Domain	Switch Regulatory Domain			AOS-W Instant release
		US	Unrestricted	IS	
OAW-IAP205H	US	Y	X	X	AOS-W Instant 6.4.3.0 or later
	RW	X	Y	Y	
	JP	X	Y	X	
	IS	X	X	Y	
OAW-IAP21x	US	Y	X	X	AOS-W Instant 6.4.2.0 or later
	RW	X	Y	Y	
	JP	X	Y	X	
	IS	X	X	Y	
OAW-IAP205	US	Y	X	X	AOS-W Instant 6.4.1.0 or later
	RW	X	Y	Y	
	JP	X	Y	X	
	IS	X	X	Y	
OAW-IAP274/275	US	Y	X	X	AOS-W Instant 6.4 or later
	RW	X	Y	Y	
	JP	X	Y	X	
	IS	X	X	Y	
OAW-IAP103H	US	Y	X	X	AOS-W Instant 6.4 or later
	RW	X	Y	Y	
	JP	X	Y	X	
	IS	X	X	Y	

Table 75: OAW-IAP-to-AOS-W Instant Conversion

OAW-IAP Variant	OAW-IAP Regulatory Domain	Switch Regulatory Domain			AOS-W Instant release
		US	Unrestricted	IS	
OAW-IAP114/115	US	Y	X	X	AOS-W Instant 6.3.1.3 or later
	JP	X	Y	X	
	IS	X	X	Y	
OAW-IAP22x	US	Y	X	X	AOS-W Instant 6.3.1.3 or later
	RW	X	Y	Y	
	JP	X	Y	X	
	IS	X	X	Y	
OAW-IAP11x and OAW-IAP22x	US	Y	X	X	AOS-W Instant 6.3.1.0, AOS-W Instant 6.3.1.1, and AOS-W Instant 6.3.1.2
	RW	X	X	X	
	JP	X	Y	X	
	IS	X	X	Y	
OAW-IAP22x	US	Y	X	X	AOS-W Instant 6.3.0
	RW/JP/IS	X	X	X	
All other OAW-IAPs	US	Y	X	X	Versions prior to AOS-W Instant 6.3.0, AOS-W Instant 6.3.x.x, AOS-W Instant 6.4, and AOS-W Instant 6.4.x.x
	Unrestricted	X	Y	X	
	IS	X	X	Y	
	JP	X	Y	X	

Converting an OAW-IAP to a Remote AP

For converting an OAW-IAP to a Remote AP, the VC sends the Remote AP convert command to all the other OAW-IAPs. The VC, along with the slave OAW-IAPs, sets a VPN tunnel to the remote switch, and downloads the firmware through FTP. The VC uses IPsec to communicate to the OmniAccess WLAN Switch over the Internet.

- If the OAW-IAP obtains OmniVista information through DHCP (Option 43 and Option 60), it establishes an HTTPS connection to the OmniVista server, downloads the configuration, and operates in the OAW-IAP mode.
- If the OAW-IAP does not get OmniVista information through DHCP provisioning, it tries provisioning through the Activate server in the cloud by sending a serial number MAC address. If an entry for the OAW-

IAP is present in Activate and is provisioned as an OAW-IAP > Remote AP, Activate responds with mobility switch IP address, OAW-IAP group, and OAW-IAP type. The OAW-IAP then contacts the switch, establishes certificate-based secure communication, and obtains configuration and image from the switch. The OAW-IAP reboots and comes up as a Remote AP. The OAW-IAP then establishes an IPsec connection with the switch and begins operating in the Remote AP mode.

- If an OAW-IAP entry is present in Activate and a provisioning rule is configured to return the IP address or host name of the OmniVista server, the OAW-IAP downloads configuration from OmniVista and operates in the OAW-IAP mode.
- If there is no response from Activate, the access point comes up with default configuration and operates in the OAW-IAP mode.



A mesh point cannot be converted to Remote AP, because mesh access points do not support VPN connection.

An OAW-IAP can be converted to a Campus AP and Remote AP only if the switch is running AOS-W Instant 6.1.4 or later versions:

The following table describes the supported OAW-IAP platforms and minimal AOS-W Instant version required for the Campus AP or Remote AP conversion.

Table 76: OAW-IAP Platforms and Minimum AOS-W Instant Versions for OAW-IAP-to-Remote AP Conversion

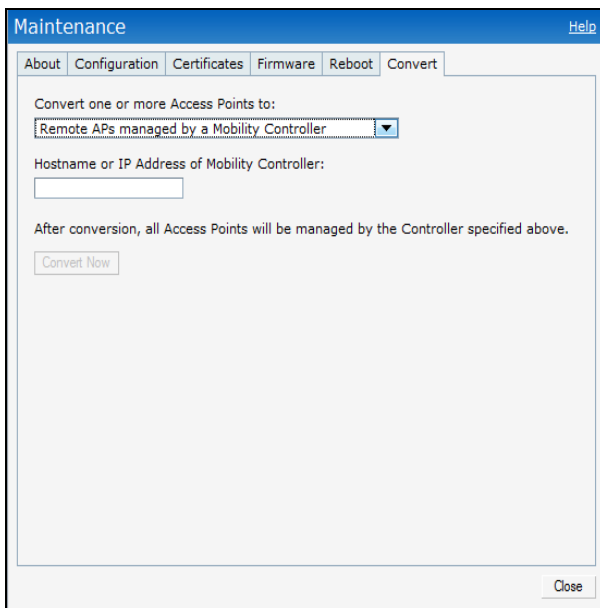
OAW-IAP Platform	AOS-W Instant Release	AOS-W Instant Release
OAW-IAP314/315 OAW-IAP334/335	AOS-W Instant 6.5.0.0 or later versions	AOS-W Instant 4.3.0 or later versions
OAW-IAP324/325	AOS-W Instant 6.4.4.0 or later versions	AOS-W Instant 4.2.2 or later versions
OAW-IAP205H OAW-IAP228 OAW-IAP277	AOS-W Instant 6.4.3.1 or later versions	AOS-W Instant 4.2 or later versions
OAW-IAP214/215	AOS-W Instant 6.4.2.0 or later versions	AOS-W Instant 4.1.1 or later versions
OAW-IAP204/205	AOS-W Instant 6.4.1.0 or later versions	AOS-W Instant 4.1.1 or later versions
OAW-IAP274/275	AOS-W Instant 6.4 or later versions	AOS-W Instant 4.1 or later versions
OAW-IAP103	AOS-W Instant 6.4 or later versions	AOS-W Instant 4.1 or later versions
OAW-IAP114/115	AOS-W Instant 6.3.1.1 or later versions	AOS-W Instant 4.0 or later versions

OAW-IAP Platform	AOS-W Instant Release	AOS-W Instant Release
OAW-IAP224/225	AOS-W Instant 6.3.1.1 or later versions	AOS-W Instant 4.0 or later versions
OAW-RAP155/155P	AOS-W Instant 6.3.0 or later versions	AOS-W Instant 3.3 or later versions
OAW-RAP108/109	AOS-W Instant 6.2.0.0 or later versions	AOS-W Instant 3.2 or later versions

To convert an OAW-IAP to a Remote AP:

1. Click **Maintenance** in the AOS-W Instant main window.
2. Click the **Convert** tab. The **Convert** tab contents are displayed.

Figure 106 Maintenance—Convert Tab



3. Select **Remote APs managed by a Mobility Controller** from the drop-down list.
4. Enter the host name (fully qualified domain name) or the IP address of the switch in the **Hostname or IP Address of Mobility Controller** text box. Contact your local network administrator to obtain the IP address.



Ensure that the OmniAccess WLAN Switch IP address is reachable by the OAW-IAPs.

5. Click **Convert Now** to complete the conversion. The OAW-IAP reboots and begins operating in the Remote AP mode.
6. After conversion, the OAW-IAP is managed by the mobility switch.



For OAW-IAPs to function as Remote APs, configure the OAW-IAP in the Remote AP whitelist and enable the FTP service on the switch.



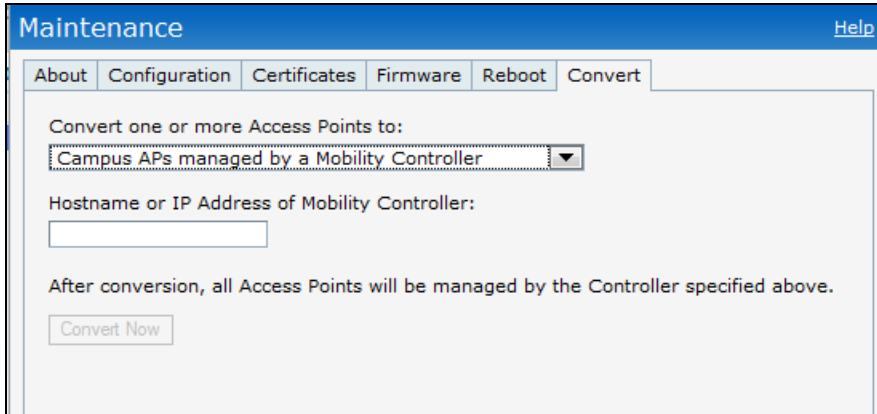
If the VPN setup fails and an error message is displayed, click **OK**, copy the error logs, and share them with your local administrator.

Converting an OAW-IAP to a Campus AP

To convert an OAW-IAP to a Campus AP:

1. Click **Maintenance** in the AOS-W Instant main window.
2. Click the **Convert** tab. The **Convert** tab contents are displayed.

Figure 107 *Converting an OAW-IAP to Campus AP*



The screenshot shows the 'Maintenance' window with the 'Convert' tab selected. The window title is 'Maintenance' and there is a 'Help' link in the top right corner. The 'Convert' tab is active, and the following options are visible:

- Convert one or more Access Points to:
 - Campus APs managed by a Mobility Controller (selected in the drop-down list)
- Hostname or IP Address of Mobility Controller:
 - [Empty text box]
- After conversion, all Access Points will be managed by the Controller specified above.
- Convert Now (button)

3. Select **Campus APs managed by a Mobility Controller** from the drop-down list.
4. Enter the host name, Fully Qualified Domain Name (FQDN), or the IP address of the switch in the **Hostname or IP Address of Mobility Controller** text box. Contact your local administrator to obtain these details.
5. Click **Convert Now** to complete the conversion.

Converting an OAW-IAP to Stand-Alone Mode

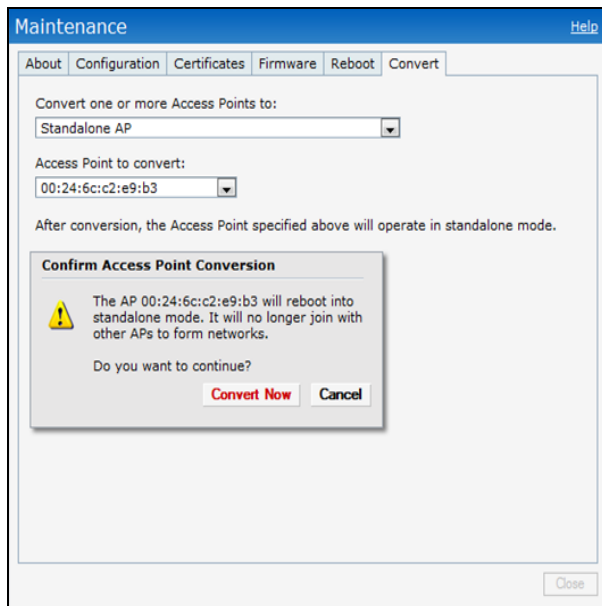
This feature allows you to deploy an OAW-IAP as an autonomous OAW-IAP, which is a separate entity from the existing VC cluster in the Layer 2 domain.

When an OAW-IAP is converted to function in stand-alone mode, it cannot join a cluster of OAW-IAPs even if the OAW-IAP is in the same VLAN. If the OAW-IAP is in the cluster mode, it can form a cluster with other VC OAW-IAPs in the same VLAN.

To deploy an OAW-IAP as a stand-alone or autonomous OAW-IAP:

1. Click **Maintenance** in the AOS-W Instant main window.
2. Click the **Convert** tab. The **Convert** tab contents are displayed.

Figure 108 Stand-Alone OAW-IAP Conversion



3. Select **Standalone AP** from the drop-down list.
4. Select the Access Point from the **Access Point to Convert** drop-down list.
5. Click **Convert Now** to complete the conversion. The OAW-IAP now operates in the stand-alone mode.

Converting an OAW-IAP using CLI

To convert an OAW-IAP to a remote AP or campus AP:

```
(Instant AP) # convert-aos-ap <mode> <controller-IP-address>
```

To convert an OAW-IAP to a stand-alone OAW-IAP or to provision an OAW-IAP in the cluster mode:

```
(Instant AP) # swarm-mode <mode>
```

Resetting a Remote AP or Campus AP to an OAW-IAP

The reset knob located on the rear of an OAW-IAP can be used to reset the OAW-IAP to factory default settings.

To reset an OAW-IAP, perform the following steps:

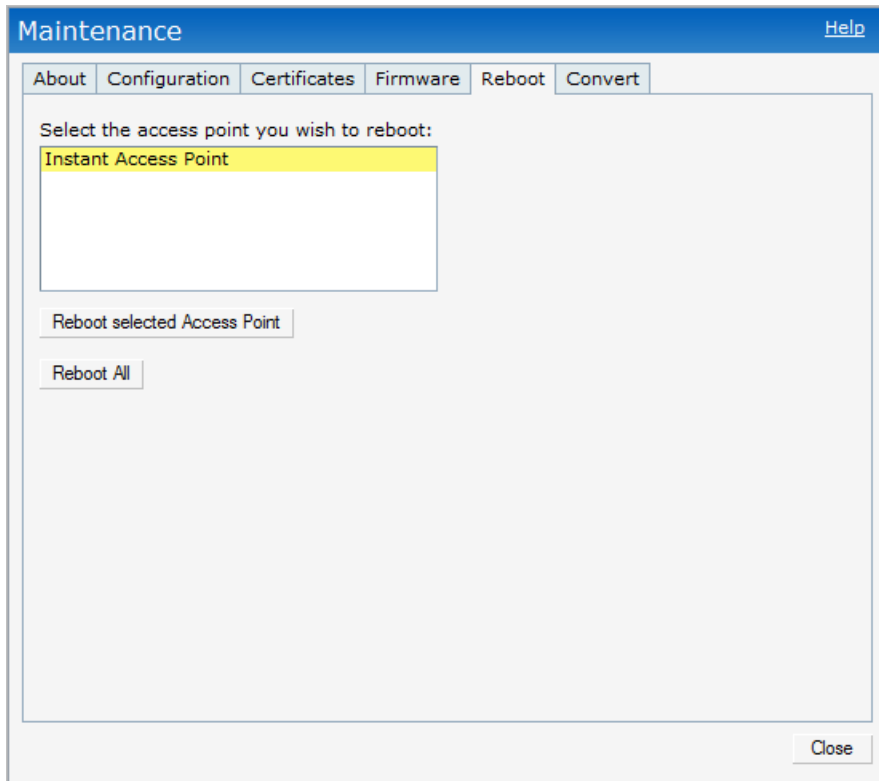
1. Turn off the OAW-IAP.
2. Press and hold the reset knob using a small and narrow object such as a paperclip.
3. Turn on the OAW-IAP without releasing the reset knob. The power LED flashes within 5 seconds indicating that the reset is completed.
4. Release the reset knob. The OAW-IAP reboots with the factory default settings.

Rebooting the OAW-IAP

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

1. Click **Maintenance** in the AOS-W Instant main window.
2. Click the **Reboot** tab.

Figure 109 *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 AP** message is displayed. Click **Reboot Now** to proceed. The **Reboot in Progress** message is displayed indicating that the reboot is in progress. The **Reboot Successful** message is displayed after the process is complete. If the system fails to boot, the **Unable to contact Access Points after reboot was initiated** message is displayed.
5. Click **OK**.

This chapter describes the following topics:

- [Configuring SNMP on page 362](#)
- [Configuring a Syslog Server on page 366](#)
- [Configuring TFTP Dump Server on page 367](#)
- [Running Debug Commands on page 368](#)
- [Uplink Bandwidth Monitoring on page 372](#)

Configuring SNMP

This section provides the following information:

- [SNMP Parameters for OAW-IAP on page 362](#)
- [Configuring SNMP on page 363](#)
- [Configuring SNMP Traps on page 365](#)

SNMP Parameters for OAW-IAP

AOS-W Instant supports SNMPv1, SNMPv2, and SNMPv3 for reporting purposes only. An OAW-IAP cannot use Simple Network Management Protocol (SNMP) to set values in an Alcatel-Lucent system.

You can configure the following parameters for an OAW-IAP:

Table 77: *SNMP Parameters for OAW-IAP*

Parameter	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 VC and the SNMP agent.
If you are using SNMPv3 to obtain values from the OAW-IAP, 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

Table 77: SNMP Parameters for OAW-IAP

Parameter	Description
Authentication protocol password	If messages sent on behalf of this user can be authenticated, a (private) authentication key is used with the authentication protocol. This is a string password for MD5 or SHA based on the conditions mentioned 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 that 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 with the privacy protocol is used.

Configuring SNMP

This section describes the procedure for configuring SNMPv1, SNMPv2, and SNMPv3 community strings by using the AOS-W Instant UI or the CLI.

Creating Community Strings for SNMPv1 and SNMPv2 Using AOS-W Instant UI

To create community strings for SNMPv1 and SNMPv2:

1. Click the **System** link on the AOS-W Instant main window.
2. In the **System** window that is displayed, click the **Monitoring** tab.

Figure 110 Monitoring Tab: SNMP Configuration Parameters

3. Click **New** under the **Community Strings for SNMPv1 and SNMPv2** box.
4. Enter the string in the **New Community String** text box.
5. Click **OK**.
6. To delete a community string, select the string, and click **Delete**.

Creating Community Strings for SNMPv3 Using AOS-W Instant UI

To create community strings for SNMPv3:

1. Click the **System** link on the AOS-W Instant main window.
2. In the **System** window that is displayed, click the **Monitoring** tab.
3. Click **New** under the **Users for SNMPV3** box.

Figure 111 *SNMPv3 User*

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

Configuring SNMP Community Strings in the CLI

To configure an SNMP engine ID and host:

```
(Instant AP) (config)# snmp-server engine-id <engine-ID>
(Instant AP) (config)# host <ipaddr> version {1 <name> udp-port <port>}|{2c|3 <name> [inform]
[udp-port <port>]}
```

To configure SNMPv1 and SNMPv2 community strings:

```
(Instant AP) (config)# snmp-server community <password>
```

To configure SNMPv3 community strings:

```
(Instant AP) (config)# snmp-server user <name> <auth-protocol> <password> <privacy-protocol>
<password>
```

To view SNMP configuration:

```
(Instant AP)# show snmp-configuration
```

```

Engine ID:D8C7C8C44298
Community Strings
-----
Name
----
SNMPv3 Users
-----
Name Authentication Type Encryption Type
-----
SNMP Trap Hosts
-----
IP Address Version Name Port Inform
-----

```

Configuring SNMP Traps

AOS-W Instant supports the configuration of external trap receivers. Only the OAW-IAP acting as the VC generates traps. The traps for OAW-IAP cluster are generated with VC IP as the source IP, if VC IP is configured. The Object Identifier (OID) of the traps is 1.3.6.1.4.1.14823.2.3.3.1.200.2.X.

You can configure SNMP traps by using the AOS-W Instant UI or the CLI.

In the AOS-W Instant UI

To configure an SNMP trap receiver:

1. Navigate to **System > Show advanced options > Monitoring**.
2. Under **SNMP Traps**, enter a name in the **SNMP Engine ID** text box. It indicates the name of the SNMP agent on the OAW-IAP. The SNMPv3 agent has an engine ID that uniquely identifies the agent in the device and is unique to that internal network.
3. Click **New** and update the following information:
 - **IP Address**—Enter the **IP Address** of the new SNMP Trap receiver.
 - **Version**—Select the SNMP version— **v1**, **v2c**, **v3** from the drop-down list. The version specifies the format of traps generated by the access point.
 - **Community/Username**—Specify the community string for SNMPv1 and SNMPv2c traps and a username for SNMPv3 traps.
 - **Port**—Enter the port to which the traps are sent. The default value is 162.
 - **Inform**—When enabled, traps are sent as SNMP INFORM messages. It is applicable to SNMPv3 only. The default value is **Yes**.
4. Click **OK** to view the trap receiver information in the **SNMP Trap Receivers** window.

In the CLI

To configure SNMP traps:

```

(Instant AP) (config)# snmp-server host <IP-address> {version 1 | version 2 | version 3} <name>
udp-port <port> inform
(Instant AP) (config)# end
(Instant AP)# commit apply

```



AOS-W Instant supports SNMP Management Information Bases (MIBs) along with Alcatel-Lucent-MIBs. For information about MIBs and SNMP traps, refer to the *AOS-W Instant 6.5.1.0-4.3.1.0 MIB Reference Guide*.

Configuring a Syslog Server

You can specify a syslog server for sending syslog messages to the external servers by using the AOS-W Instant UI or the CLI.

In the AOS-W Instant UI

To configure a Syslog server and Syslog facility levels:

1. In the AOS-W Instant main window, click the **System** link.
2. Click **Show advanced options** to display the advanced options.
3. Click the **Monitoring** tab.

Figure 112 Syslog Server

The screenshot shows the configuration interface for a Syslog server. It includes fields for the Syslog server IP (0.0.0.0) and TFTP Dump Server IP (0.0.0.0). Below these are Syslog Facility Levels for various categories: Syslog, System, Ap-Debug, User, Network, User-Debug, Security, and Wireless, each with a dropdown menu set to 'Warning'. The SNMP section contains two tables: 'Community Strings for SNMPV1 and SNMPV2' and 'Users for SNMPV3'. The 'Users for SNMPV3' table has columns for Name, Authentication Protocol, and Privacy Protocol. There are 'New' and 'Delete' buttons for both tables. At the bottom, there is an 'SNMP Traps' section with a table for 'SNMP Trap Receivers' with columns for IP Address, Version, Community/Username, Port, and Inform. There are also 'New' and 'Delete' buttons for this section. At the very bottom, there is a 'Hide advanced options' link, 'OK', and 'Cancel' buttons.

4. In the **Syslog server** text box, enter the IP address of the server to which you want to send system logs.



The syslog source address is sent individually by the OAW-IAPs in the cluster and never the VC IP. Even the master OAW-IAP sends the syslog source address from its actual IP address.

5. Select the required values to configure syslog facility levels. Syslog Facility is an information field associated with a syslog message. It is an application or operating system component that generates a log message. The following seven facilities are supported by Syslog:
 - **AP-Debug**—Detailed log about the OAW-IAP 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 logs about client debugging.

- **Wireless**—Log about radio.

The following table describes the logging levels in order of severity, from the most to the least severe.

Table 78: 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 noncritical and normal nature. The default value for all Syslog facilities.
Informational	Messages of general interest to system users.
Debug	Messages containing information useful for debugging.

6. Click **OK**.

In the CLI

To configure a syslog server:

```
(Instant AP) (config)# syslog-server <IP-address>
```

To configure syslog facility levels:

```
(Instant AP) (config)# syslog-level <logging-level>[ap-debug |network |security |system |user |
user-debug | wireless]
(Instant AP) (config)# end
(Instant AP)# commit apply
```

To view syslog logging levels:

```
(Instant AP)# show syslog-level
```

```
Logging Level
-----
Facility Level
-----
ap-debug warn
network warn
security warn
system warn
user warn
user-debug warn
wireless error
```

Configuring TFTP Dump Server

You can configure a TFTP server for storing core dump files by using the AOS-W Instant UI or the CLI.

In the AOS-W Instant UI

To configure a TFTP server:

1. In the AOS-W Instant main window, click the **System** link.
2. Click **Show advanced options** to display the advanced options.
3. Click the **Monitoring** tab.
4. Enter the IP address of the TFTP server in the **TFTP Dump Server** text box.
5. Click **OK**.

In the CLI

To configure a TFTP server:

```
(Instant AP) (config)# tftp-dump-server <IP-address>
(Instant AP) (config)# end
(Instant AP)# commit apply
```

Running Debug Commands

To run the debugging commands from the UI:

1. Navigate to **More > Support** on the AOS-W Instant main window.
2. Select the required option from the **Command** drop-down list.
3. Select **All Access Points** or **Instant Access Point(VC)** from the **Target** drop-down list.
4. Click **Run**. When you run debug commands and click **Save**, the output of all the selected commands is displayed in a single page.

The **Support** window allows you to run commands for each access point and VC in a cluster. For a complete list of commands supported in a particular release train, execute the **show support-commands** command at the OAW-IAP CLI. The output of this command displays the list of support commands that you can run through the UI and the corresponding CLI commands. For more information on these commands, refer to the respective command page in the *AOS-W Instant 6.5.0.0-4.3.0.0 CLI Reference Guide*.

```
(Instant AP) # show support-commands
```

```
Support Commands
```

```
-----
```

Description	Command Name
-----	-----
AP Tech Support Dump	show tech-support
AP Tech Support Dump Supplemental	show tech-support supplemental
AP Provisioning Status	show activate status
AP 3G/4G Status	show cellular status
AP 802.1X Statistics	show ap debug dot1x-statistics
AP Access Rule Table	show access-rule-all
AP Inbound Firewall Rules	show inbound-firewall-rules
AP Active	show aps
AP AirGroup Cache	show airgroup cache entries
AP AirGroup CPPM Entries	show airgroup cppm entries
AP AirGroup CPPM Servers	show airgroup cppm server
AP AirGroup Debug Statistics	show airgroup debug statistics
AP AirGroup Servers	show airgroup servers verbose
AP AirGroup User	show airgroup users verbose
AP ALE Configuration	show ale config
AP ALE Status	show ale status
AP Allowed Channels	show ap allowed-channels
AP Allowed MAX-EIRP	show ap allowed-max-EIRP
AP All Supported Timezones	show clock timezone all
AP ARM Bandwidth Management	show ap arm bandwidth-management

AP ARM Channels	show arm-channels
AP ARM Configuration	show arm config
AP ARM History	show ap arm history
AP ARM Neighbors	show ap arm neighbors
AP ARM RF Summary	show ap arm rf-summary
AP ARM Scan Times	show ap arm scan-times
AP ARP Table	show arp
AP Association Table	show ap association
AP Authentication Frames	show ap debug auth-trace-buf
AP Auth-Survivability Cache	show auth-survivability cached-info
AP Auth-Survivability Debug Log	show auth-survivability debug-log
AP BSSID Table	show ap bss-table
AP Captive Portal Domains	show captive-portal-domains
AP Captive Portal Auto White List	show captive-portal auto-white-list
AP Client Match Status	show ap debug client-match
AP Client Match History	show ap client-match-history
AP Client Match Action	show ap client-match-actions
AP Client Match Live	show ap client-match-live
AP Client Match Triggers	show ap client-match-triggers
AP Client Table	show ap debug client-table
AP Client View	show ap client-view
AP Country Codes	show country-codes
AP CPU Details	show cpu details
AP CPU Utilization	show cpu
AP Crash Info	show ap debug crash-info
AP Current Time	show clock
AP Current Timezone	show clock timezone
AP Datapath ACL Table Allocation	show datapath acl-allocation
AP Datapath ACL Tables	show datapath acl-all
AP Datapath Bridge Table	show datapath bridge
AP Datapath DMO session	show datapath dmo-session
AP Datapath DMO station	show datapath dmo-station
AP Datapath Dns Id Map	show datapath dns-id-map
AP Datapath Multicast Table	show datapath mcast
AP Datapath Nat Pool	show datapath nat-pool
AP Datapath Route Table	show datapath route
AP Datapath Session Table	show datapath session
AP Datapath DPI Session Table	show datapath session dpi
AP Datapath DPI Session Table Verbose	show datapath session dpi verbose
AP Datapath Statistics	show datapath statistics
AP Datapath User Table	show datapath user
AP Datapath VLAN Table	show datapath vlan
AP DPI Debug statistics	show dpi debug statistics
AP Daylight Saving Time	show clock summer-time
AP Derivation Rules	show derivation-rules
AP Driver Configuration	show ap debug driver-config
AP Election Statistics	show election statistics
AP External Captive Portal Status	show external-captive-portal
AP Environment Variable	show ap-env
AP ESSID Table	show network
AP Flash Configuration	show ap flash-config
AP IGMP Group Table	show ip igmp
AP Interface Counters	show interface counters
AP Interface Status	show port status
AP Internal DHCP Status	show dhcp-allocation
AP IP Interface	show ip interface brief
AP IP Route Table	show ip route
AP L3 Mobility Datapath	show l3-mobility datapath
AP L3 Mobility Events log	show log l3-mobility
AP L3 Mobility Status	show l3-mobility status
AP LACP Status	show lacp status
AP Log All	show log debug

AP Log AP-Debug	show log ap-debug
AP Log Conversion	show log convert
AP Log Driver	show log driver
AP Log Kernel	show log kernel
AP Log Network	show log network
AP Log PPPd	show log pppd
AP Log Rapper	show log rapper
AP Log Rapper Counter	show log rapper-counter
AP Log Rapper Brief	show log rapper-brief
AP Log Sapid	show log sapd
AP Log Security	show log security
AP Log System	show log system
AP Log Tunnel Status Management	show log apifmgr
AP Log Upgrade	show log upgrade
AP Log User-Debug	show log user-debug
AP Log User	show log user
AP Log VPN Tunnel	show log vpn-tunnel
AP Log Wireless	show log wireless
AP Management Frames	show ap debug mgmt-frames
AP Memory Allocation State Dumps	show malloc-state-dumps
AP Memory Utilization	show memory
AP Mesh Counters	show ap mesh counters
AP Mesh Link	show ap mesh link
AP Mesh Neighbors	show ap mesh neighbours
AP Monitor Active Laser Beams	show ap monitor active-laser-beams
AP Monitor AP Table	show ap monitor ap-list
AP Monitor ARP Cache	show ap monitor ARP Cache
AP Monitor Client Table	show ap monitor sta-list
AP Monitor Containment Information	show ap monitor containment-info
AP Monitor Potential AP Table	show ap monitor pot-ap-list
AP Monitor Potential Client Table	show ap monitor pot-sta-list
AP Monitor Router	show ap monitor routers
AP Monitor Scan Information	show ap monitor scan-info
AP Monitor Status	show ap monitor status
AP Persistent Clients	show ap debug persistent-clients
AP PMK Cache	show ap pmkcache
AP PPPoE uplink debug	show pppoe debug-logs
AP PPPoE uplink status	show pppoe status
AP Processes	show process
AP Radio 0 Client Probe Report	show ap client-probe-report 0
AP Radio 0 Stats	show ap debug radio-stats 0
AP Radio 0 info	show ap debug radio-info 0
AP Radio 1 Client Probe Report	show ap client-probe-report 1
AP Radio 1 Stats	show ap debug radio-stats 1
AP Radio 1 info	show ap debug radio-info 1
AP RADIUS Statistics	show ap debug radius-statistics
AP Termination RADIUS Statistics	show ap debug radius-statistics termination
AP Shaping Table	show ap debug shaping-table
AP Sockets	show socket
AP STM Configuration	show ap debug stm-config
AP Swarm State	show swarm state
AP System Status	show ap debug system-status
AP System Summary	show summary support
AP Uplink Status	show uplink status
AP User Table	show clients
AP Valid Channels	show valid-channels
AP Version	show version
AP Virtual Beacon Report	show ap virtual-beacon-report
AP VPN Config	show vpn config
AP VPN Status	show vpn status
AP IAP-VPN Retry Counters	show vpn tunnels
AP Wired Port Settings	show wired-port-settings

AP Wired User Table	show clients wired
AP Checksum	show ap checksum
AP Spectrum AP table	show ap spectrum ap-list
AP Spectrum channel table	show ap spectrum channel-details
AP Spectrum channel metrics	show ap spectrum channel-metrics
AP Spectrum channel summary	show ap spectrum channel-summary
AP Spectrum client table	show ap spectrum client-list
AP Spectrum device duty cycle	show ap spectrum device-duty-cycle
AP Spectrum non-wifi device history	show ap spectrum device-history
AP Spectrum non-wifi device table	show ap spectrum device-list
AP Spectrum non-wifi device log	show ap spectrum device-log
AP Spectrum number of device	show ap spectrum device-summary
AP Spectrum interference-power table	show ap spectrum interference-power
AP Spectrum status	show ap spectrum status
VC 802.1x Certificate	show lxcert
VC All Certificates	show cert all
VC radsec Certificates	show radseccert
VC Captive Portal domains	show captive-portal-domains
VC About	show about
VC Active Configuration	show running-config
VC AirGroup Service	show airgroupservice
VC AirGroup Status	show airgroup status
VC Allowed AP Table	show allowed-aps
VC AMP Status	show ap debug airwave
VC AMP Current State Data	show ap debug airwave-state
VC AMP Current Stats Data	show ap debug airwave-stats
VC AMP Data Sent	show ap debug airwave-data-sent
VC AMP Events Pending	show ap debug airwave-events-pending
VC AMP Last Configuration Received	show ap debug airwave-config-received
VC AMP Single Sign-on Key	show ap debug airwave-signon-key
VC AMP Configuration Restore Status	show ap debug airwave-restore-status
VC Central Current State Data	show ap debug cloud-state
VC Central Current Stats Data	show ap debug cloud-stats
VC Central Data Sent	show ap debug cloud-data-sent
VC Central Events Pending	show ap debug cloud-events-pending
VC Central Last Configuration Received	show ap debug cloud-config-received
VC Central Single Sign-on Key	show ap debug cloud-signon-key
VC Central Configuration Restore Status	show ap debug cloud-restore-status
VC Application Services	show app-services
VC Cloud Server Status	show ap debug cloud-server
VC DHCP Option 43 Received	show dhcpc-opts
VC Global Alerts	show alert global
VC Global Statistics	show stats global
VC IDS AP List	show ids aps
VC IDS Client List	show ids clients
VC Internal DHCP Server Configuration	show ip dhcp database
VC L2TPv3 config	show l2tpv3 config
VC L2TPv3 session status	show l2tpv3 session status
VC L2TPv3 system wide global statistics	show l2tpv3 system statistics
VC L2TPv3 tunnel configuration	show l2tpv3 tunnel config
VC L2TPv3 tunnel status	show l2tpv3 tunnel status
VC Local User Database	show users
VC OpenDNS Configuration and Status	show.opendns support
VC Provisioning Log	show log provision
VC Radius Attributes	show radius-attributes
VC Radius Servers	show radius-servers support
AP Radius Status	show radius status
VC Saved Configuration	show configuration
VC Scanning Stats	show aps scanning
VC Show SBR Table	show datapath sbr
VC SNMP Configuration	show snmp-configuration
VC Uplink 3G/4G Configuration	show cellular config

VC Uplink Management Configuration	show uplink config
VC WISPr Configuration	show wispr config
VC XML API Server Information	show xml-api-server
VC rfc3576-radius statistics	show ap debug rfc3576-radius-statistics



Use the support commands under the supervision of Alcatel-Lucent technical support.

Uplink Bandwidth Monitoring

An OAW-IAP uses Iperf3 as a TCP or UDP client to run a speed test and measure the bandwidth on an uplink. The results from the speed test are collated by the OAW-IAP and published to Analytics and Location Engine (ALE). The speed tests can be run only on the master OAW-IAP of the cluster. You may choose to configure and execute a speed test profile during boot time and additionally at specific time intervals using the configuration mode or execute the speed test at any preferred time using the privileged EXEC mode in the CLI.

To configure and automatically run speed tests at specific time intervals:

```
(Instant AP) (config)# speed-test
(Instant AP) (speed-test)# include-reverse
(Instant AP) (speed-test)# server-ip <server>
(Instant AP) (speed-test)# server-port <port>
(Instant AP) (speed-test)# protocol <tcp/udp>
(Instant AP) (speed-test)# on-boot
(Instant AP) (speed-test)# time-interval <interval>
(Instant AP) (speed-test)# bandwidth <bandwidth>
(Instant AP) (speed-test)# sec-to-measure <secs>
(Instant AP) (speed-test)# end
(Instant AP)# commit apply
```

To configure and execute a speed test at any point in time:

```
(Instant AP)# speed-test <server> <protocol> [<bandwidth>|<include-reverse>|<sec-to-measure>
|<server-port>]
(Instant AP)# end
```

To view the speed test results:

```
(Instant AP)# show speed-test data
(Instant AP)# end
```

Following is an example of the speed-test result

```
(Instant AP)# show speed-test data
Speed Test results :
Time of Execution :Fri, 11 Nov 2016 07:06:29
Server IP :10.17.138.2
Local IP :10.17.138.92
Local Port :62716
Remote Port :5201
MAC :40:e3:d6:cf:f5:2e
System Name :40:e3:d6:cf:f5:2e
Protocol :TCP
Duration :10
Upstream Bytes :496028352
Upstream Bandwidth (Mbps) :395.97
upstream retries :0
Downstream Bytes :615227296
Downstream bandwidth (Mbps) :492.18
```

The following command shows the number of times the uplink bandwidth report was sent to the ALE server.

To display the uplink bandwidth counter:

```
(Instant AP)# show ale stats
ALE Stats
```

```
-----  
Type Value  
-----  
VC package 0  
RSSI package 0  
APPRF package 0  
URLv package 0  
STATE package 0  
STAT package 0  
UPLINK BW package 0  
Total 0
```

This chapter contains the following topics:

- [Understanding Hotspot Profiles on page 374](#)
- [Configuring Hotspot Profiles on page 376](#)
- [Sample Configuration on page 387](#)



In the current release, AOS-W Instant supports the hotspot profile configuration only through the CLI.

Understanding Hotspot Profiles

Hotspot 2.0 (Passpoint Release 1) is a Wi-Fi Alliance specification based on the 802.11u protocol, which allows wireless clients to discover hotspots using management frames (such as beacon, association request, and association response), connect to networks, and roam between networks without additional authentication.

Hotspot 2.0 provides the following services:

- Network discovery and selection—Allows the clients to discover suitable and available networks by advertising the access network type, roaming consortium, and venue information through the management frames. For network discovery and selection, Generic Advertisement Service (GAS) and Access Network Query Protocol (ANQP) are used.
- QoS Mapping—Provides a mapping between the network-layer QoS packet marking and over-the-air QoS frame marking based on user priority.

When a hotspot is configured in a network:

- The clients search for available hotspots using the beacon management frame.
- When a hotspot is found, the client sends queries to obtain information about the type of network authentication and IP address, and IP address availability using the Generic Advertisement Service (GAS) action frames.
- Based on the response of the advertisement server (response to the GAS Action Frames), the relevant hotspot is selected and the client attempts to associate with it.
- Based on the authentication mode used for mobility clients, the client authenticates to access the network.

Generic Advertisement Service (GAS)

GAS is a request-response protocol, that provides L2 transport mechanism between a wireless client and a server in the network prior to authentication. It helps to determine an 802.11 infrastructure before associating clients and allows clients to send queries to multiple 802.11 networks in parallel.

An OAW-IAP can include its SP Organization Identifier (OI) indicating the identity of the SP in beacons and probe responses to clients. When a client recognizes an OAW-IAP's OI, it attempts to associate to that OAW-IAP using the security credentials corresponding to that SP. If the client does not recognize the AP's OI, the client sends a Generic Advertisement Service (GAS) query to the OAW-IAP to request more information about the network before associating. A client transmits a GAS Query using a GAS Initial Request frame and the OAW-IAP provides the query response or information on how to receive the query response in a GAS Initial Response frame. To transmit a GAS query for any advertisement protocol, the advertisement protocol ID must include the advertisement protocol information element (IE) with details of the advertisement protocol and its corresponding advertisement control.

Access Network Query Protocol (ANQP)

ANQP provides a range of information, such as IP address type and availability, roaming partners accessible through a hotspot, and the Extensible Authentication Protocol (EAP) method supported for authentication, for a query and response protocol. The ANQP Information Elements (IEs) provide additional data that can be sent from an OAW-IAP to the client to identify the OAW-IAP's network and service provider. If a client requests this information through a GAS query, the hotspot OAW-IAP sends the ANQP capability list in the GAS Initial Response frame indicating support for the following IEs:

- Venue Name
- Domain Name
- Network Authentication Type
- Roaming Consortium List
- Network Access Identifier Realm
- 3GPP Cellular Network Data
- IP Address Availability

Hotspot 2.0 Query Protocol (H2QP)

The H2QP profiles provide a range of information on Hotspot 2.0 elements such as hotspot protocol and port, operating-class, operator names, WAN status, and uplink and downlink metrics.

Information Elements (IEs) and Management Frames

The Hotspot 2.0 configuration supports the following IEs:

- Interworking IE—Provides information about the Interworking service capabilities such as the Internet availability in a specific service provider network.
- Advertisement Protocol IE—Provides information about the advertisement protocol that a client can use for communication with the advertisement servers in a network.
- Roaming Consortium IE—Provides information about the service provider network for roaming clients, which can be used to authenticate with the OAW-IAP.

The IEs are included in the following Management Frames when 802.11u is enabled:

- Beacon Frame
- Probe Request Frame
- Probe Response frame
- Association Request
- Re-Association request

NAI Realm List

An Network Access Identifier (NAI) Realm profile identifies and describes a NAI realm to which the clients can connect. The NAI realm settings on an OAW-IAP act as an advertisement profile to determine the NAI realm elements that must be included as part of a GAS Response frame.

Configuring Hotspot Profiles

To configure a hotspot profile, perform the following steps:

1. Create the required ANQP and H2QP advertisement profiles.
2. Create a hotspot profile.
3. Associate the required ANQP and H2QP advertisement profiles created in step 1 to the hotspot profile created in step 2.
4. Create an SSID Profile with enterprise security and WPA-2 encryption settings and then associate the SSID with the hotspot profile created in step 2.

Creating Advertisement Profiles for Hotspot Configuration

A hotspot profile contains one or several advertisement profiles. The following advertisement profiles can be configured through the AOS-W Instant CLI:

- ANQP advertisement profiles
 - NAI Realm profile
 - Venue Name Profile
 - Network Authentication Profile
 - Roaming Consortium Profile
 - 3GPP Profile
 - IP Address availability Profile
 - Domain Name Profile
- H2QP advertisement profiles
 - Operator Friendly Name Profile
 - Connection Capability Profile
 - Operating-Class Profile
 - WAN-Metrics Profile

Configuring an NAI Realm Profile

You can configure a Network Access Identifier (NAI) Realm profile to define the NAI realm information, which can be sent as an ANQP IE in a GAS query response.

To configure a NAI profile:

```
(Instant AP) (config)# hotspot anqp-nai-realm-profile <name>
(Instant AP) (nai-realm <name>)# nai-realm-name <name>
(Instant AP) (nai-realm <name>)# nai-realm-encoding {<utf8>|<rfc4282>}
(Instant AP) (nai-realm <name>)# nai-realm-eap-method <eap-method>
(Instant AP) (nai-realm <name>)# nai-realm-auth-id-1 <authentication-ID>
(Instant AP) (nai-realm <name>)# nai-realm-auth-id-2 <authentication-ID>
(Instant AP) (nai-realm <name>)# nai-realm-auth-value-1 <authentication-value>
(Instant AP) (nai-realm <name>)# nai-realm-auth-value-2 <authentication-value>
(Instant AP) (nai-realm <name>)# nai-home-realm
(Instant AP) (nai-realm <name>)# enable
(Instant AP) (nai-realm <name>)# end
(Instant AP)# commit apply
```


You can specify any of the following EAP methods for the **nai-realm-eap-method <eap-method>** command:

- **identity**—To use EAP Identity type. The associated numeric value is 1.
- **notification**—To allow the hotspot realm to use EAP Notification messages for authentication. The associated numeric value is 2.
- **one-time-password**—To use Authentication with a single-use password. The associated numeric value is 5.
- **generic-token-card**—To use EAP Generic Token Card (EAP-GTC). The associated numeric value is 6.
- **eap-tls**—To use EAP-Transport Layer Security. The associated numeric value is 13.
- **eap-sim**—To use EAP for Global System for Mobile Communication (GSM) Subscriber Identity Modules (SIM). The associated numeric value is 18.
- **eap-ttls**—To use EAP-Tunneled Transport Layer Security. The associated numeric value is 21.
- **peap**—To use protected Extensible Authentication Protocol. The associated numeric value is 25.
- **crypto-card**—To use crypto card authentication. The associated numeric value is 28.
- **peapmschapv2**—To use PEAP with Microsoft Challenge Handshake Authentication Protocol version 2 (MSCHAPv2). The associated numeric value is 29.
- **eap-aka**—To use EAP for Universal Mobile Telecommunications System (UMTS) Authentication and Key Agreement (AKA). The associated numeric value is 50.

The following table lists the possible authentication IDs and their respective values:

Table 79: NAI Realm Profile Configuration Parameters

Authentication ID	Authentication Value
<p>reserved</p> <ul style="list-style-type: none"> ● Uses the reserved authentication method. ● The associated numeric value is 0. 	—
<p>expanded-eap</p> <ul style="list-style-type: none"> ● Uses the expanded EAP authentication method. ● The associated numeric value is 1. 	Use expanded-eap as the authentication value.
<p>non-eap-inner-auth</p> <ul style="list-style-type: none"> ● Uses non-EAP inner authentication type. ● The associated numeric value is 2. 	<p>The following authentication values apply:</p> <ul style="list-style-type: none"> ● reserved—The associated numeric value is 0. ● pap—The associated numeric value is 1. ● chap—The associated numeric value is 2. ● mschap—The associated numeric value is 3. ● mschapv2—The associated numeric value is 4.

Table 79: NAI Realm Profile Configuration Parameters

Authentication ID	Authentication Value
eap-inner-auth <ul style="list-style-type: none"> • Uses EAP inner authentication type. • The associated numeric value is 3. 	The following authentication values apply: <ul style="list-style-type: none"> • reserved—The associated numeric value is 0. • pap—The associated numeric value is 1. • chap—The associated numeric value is 2. • mschap—The associated numeric value is 3. • mschapv2—The associated numeric value is 4.
exp-inner-eap <ul style="list-style-type: none"> • Uses the expanded inner EAP authentication method. • The associated numeric value is 4. 	Use the exp-inner-eap authentication value.
credential <ul style="list-style-type: none"> • Uses credential authentication. • The associated numeric value is 5. 	The following authentication values apply: <ul style="list-style-type: none"> • sim—The associated numeric value is 1. • usim—The associated numeric value is 2. • nfc-secure—The associated numeric value is 3. • hw-token—The associated numeric value is 4. • softoken—The associated numeric value is 5. • certificate—The associated numeric value is 6. • uname-password—The associated numeric value is 7. • none—The associated numeric value is 8. • reserved—The associated numeric value is 9. • vendor-specific—The associated numeric value is 10.

Configuring a Venue Name Profile

You can configure a venue name profile to send the venue information as an ANQP IE in a GAS query response.

To configure a venue name profile:

```
(Instant AP) (config)# hotspot anqp-venue-name-profile <name>
(Instant AP) (venue-name <name>)# venue-name <name>
(Instant AP) (venue-name <name>)# venue-group <group-name>
(Instant AP) (venue-name <name>)# venue-type <type>
(Instant AP) (venue-name <name>)# venue-lang-code <language>
(Instant AP) (venue-name <name>)# enable
(Instant AP) (venue-name <name>)# end
(Instant AP)# commit apply
```

You can specify any of the following venue groups and the corresponding venue types:

Table 80: Venue Types

Venue Group	Associated Venue Type Value
<p>unspecified The associated numeric value is 0.</p>	<p>—</p>
<p>assembly The associated numeric value is 1.</p>	<ul style="list-style-type: none"> • unspecified—The associated numeric value is 0. • arena—The associated numeric value is 1. • stadium—The associated numeric value is 2. • passenger-terminal—The associated numeric value is 3. • amphitheater—The associated numeric value is 4. • amusement-park—The associated numeric value is 5. • place-of-worship—The associated numeric value is 6. • convention-center—The associated numeric value is 7. • library—The associated numeric value is 8. • museum—The associated numeric value is 9. • restaurant—The associated numeric value is 10. • theater—The associated numeric value is 11. • bar—The associated numeric value is 12. • coffee-shop—The associated numeric value is 13. • zoo-or-aquarium—The associated numeric value is 14. • emergency-cord-center—The associated numeric value is 15.
<p>business The associated numeric value is 2.</p>	<ul style="list-style-type: none"> • unspecified—The associated numeric value is 0. • doctor—The associated numeric value is 1. • bank—The associated numeric value is 2. • fire-station—The associated numeric value is 3. • police-station—The associated numeric value is 4. • post-office—The associated numeric value is 6. • professional-office—The associated numeric value is 7. • research-and-dev-facility—The associated numeric value is 8. • attorney-office—The associated numeric value is 9.
<p>educational The associated numeric value is 3.</p>	<ul style="list-style-type: none"> • unspecified—The associated numeric value is 0. • school-primary—The associated numeric value is 1. • school-secondary—The associated numeric value is 2. • univ-or-college—The associated numeric value is 3.
<p>factory-and-industrial The associated numeric value is 4.</p>	<ul style="list-style-type: none"> • unspecified—The associated numeric value is 0. • factory—The associated numeric value is 1.
<p>institutional</p>	<ul style="list-style-type: none"> • unspecified—The associated numeric value is 0.

Table 80: Venue Types

Venue Group	Associated Venue Type Value
<p>The associated numeric value is 5.</p>	<ul style="list-style-type: none"> ● hospital—The associated numeric value is 1. ● long-term-care—The associated numeric value is 2. ● alc-drug-rehab—The associated numeric value is 3. ● group-home—The associated numeric value is 4. ● prison-or-jail—The associated numeric value is 5.
<p>mercantile The associated numeric value is 6.</p>	<ul style="list-style-type: none"> ● unspecified—The associated numeric value is 0. ● retail-store—The associated numeric value is 1. ● grocery-market—The associated numeric value is 2. ● auto-service-station—The associated numeric value is 3. ● shopping-mall—The associated numeric value is 4. ● gas-station—The associated numeric value is 5.
<p>residential The associated numeric value is 7.</p>	<ul style="list-style-type: none"> ● unspecified—The associated numeric value is 0. ● private-residence—The associated numeric value is 1. ● hotel—The associated numeric value is 2. ● dormitory—The associated numeric value is 3. ● boarding-house—The associated numeric value is 4.
<p>storage The associated numeric value is 8.</p>	<p>unspecified—The associated numeric value is 0.</p>
<p>utility-misc The associated numeric value is 9.</p>	<p>unspecified—The associated numeric value is 0.</p>
<p>vehicular The associated numeric value is 10.</p>	<ul style="list-style-type: none"> ● unspecified—The associated numeric value is 0. ● automobile-or-truck—The associated numeric value is 1. ● airplane—The associated numeric value is 2. ● bus—The associated numeric value is 3. ● ferry—The associated numeric value is 4. ● ship—The associated numeric value is 5. ● train—The associated numeric value is 6. ● motor-bike—The associated numeric value is 7.
<p>outdoor The associated numeric value is 11.</p>	<ul style="list-style-type: none"> ● unspecified—The associated numeric value is 0 ● muni-mesh-network—The associated numeric value is 1. ● city-park—The associated numeric value is 2. ● rest-area—The associated numeric value is 3. ● traffic-control—The associated numeric value is 4. ● bus-stop—The associated numeric value is 5. ● kiosk—The associated numeric value is 6.

Configuring a Network Authentication Profile

You can configure a network authentication profile to define the authentication type used by the hotspot network.

To configure a network authentication profile:

```
(Instant AP) (config)# hotspot anqp-nwk-auth-profile <name>
(Instant AP) (network-auth <name>)# nwk-auth-type <type>
(Instant AP) (network-auth <name>)# url <URL>
(Instant AP) (network-auth <name>)# enable
(Instant AP) (network-auth <name>)# end
(Instant AP)# commit apply
```

You can specify any of the following network authentication type for the **nwk-auth-type <type>** command:

- **accept-term-and-cond**—When configured, the network requires the user to accept terms and conditions. This option requires you to specify a redirection URL string as an IP address, FQDN or URL.
- **online-enrollment**—When configured, the network supports the online enrollment.
- **http-redirect**—When configured, additional information on the network is provided through HTTP/HTTPS redirection.
- **dns-redirect**—When configured, additional information on the network is provided through DNS redirection. This option requires you to specify a redirection URL string as an IP address, FQDN, or URL.

Configuring a Roaming Consortium Profile

You can configure a roaming consortium profile to send the roaming consortium information as an ANQP IE in a GAS query response.

To configure a roaming consortium profile:

```
(Instant AP) (config)# hotspot anqp-roam-cons-profile <name>
(Instant AP) (roaming-consortium <name>)# roam-cons-oi <roam-cons-oi>
(Instant AP) (roaming-consortium <name>)# roam-cons-oi-len <roam-cons-oi-len>
(Instant AP) (roaming-consortium <name>)# enable
(Instant AP) (roaming-consortium <name>)# end
(Instant AP)# commit apply
```

Specify a hexadecimal string of 3–5 octets for **roam-cons-oi <roam-cons-oi>**.

Based on the Organization Identifier (OI) specified, you can specify the following parameters for the length of OI in **roam-cons-oi-len <roam-cons-oi-len>**.

- For 0: 0 Octets in the OI (Null)
- For 3: OI length is 24-bits (3 Octets)
- For 5: OI length is 36-bits (5 Octets)

Configuring a 3GPP Profile

You can configure a 3rd Generation Partnership Project (3GPP) profile to define information for the 3G Cellular Network for hotspots.

To configure a 3GPP profile:

```
(Instant AP) (config)# hotspot anqp-3gpp-profile <name>
(Instant AP) (3gpp <name>)# 3gpp-plmn1 <plmn-ID>
(Instant AP) (3gpp <name>)# enable
(Instant AP) (3gpp <name>)# end
(Instant AP)# commit apply
```

The Public Land Mobile Network (PLMN) ID is a combination of the mobile country code and network code. You can specify up to 6 PLMN IDs for a 3GPP profile.

Configuring an IP Address Availability Profile

You can configure an available IP address types to send information on IP address availability as an ANQP IE in a GAS query response.

To configure an IP address availability profile:

```
(Instant AP) (config)# hotspot anqp-ip-addr-avail-profile <name>
(Instant AP) (IP-addr-avail <name>)# ipv4-addr-avail
(Instant AP) (IP-addr-avail <name>)# ipv6-addr-avail
(Instant AP) (IP-addr-avail <name>)# enable
(Instant AP) (IP-addr-avail <name>)# end
(Instant AP)# commit apply
```

Configuring a Domain Profile

You can configure a domain profile to send the domain names as an ANQP IE in a GAS query response.

To configure a domain name profile, execute the following commands:

```
(Instant AP) (config)# hotspot anqp-domain-name-profile <name>
(Instant AP) (domain-name <name>)# domain-name <domain-name>
(Instant AP) (domain-name <name>)# enable
(Instant AP) (domain-name <name>)# end
(Instant AP)# commit apply
```

Configuring an Operator-Friendly Profile

You can configure an operator-friendly name profile to define the identify the operator.

To configure an H2QP operator-friendly name profile:

```
(Instant AP) (config)# hotspot h2qp-oper-name-profile <name>
(Instant AP) (operator-friendly-name <name>)# op-fr-name <op-fr-name>
(Instant AP) (operator-friendly-name <name>)# op-lang-code <op-lang-code>
(Instant AP) (operator-friendly-name <name>)# enable
(Instant AP) (operator-friendly-name <name>)# end
(Instant AP)# commit apply
```

Configuring a Connection Capability Profile

You can configure a connection capability profile to define information such as the hotspot IP protocols and associated port numbers that are available for communication.

To configure an H2QP connection capability profile:

```
(Instant AP) (config) # hotspot h2qp-conn-cap-profile <name>
(Instant AP) (connection-capabilities <name>)# esp-port
(Instant AP) (connection-capabilities <name>)# icmp
(Instant AP) (connection-capabilities <name>)# tcp-ftp
(Instant AP) (connection-capabilities <name>)# tcp-http
(Instant AP) (connection-capabilities <name>)# tcp-pptp-vpn
(Instant AP) (connection-capabilities <name>)# tcp-ssh
(Instant AP) (connection-capabilities <name>)# tcp-tls-vpn
(Instant AP) (connection-capabilities <name>)# tcp-voip
(Instant AP) (connection-capabilities <name>)# udp-ike2
(Instant AP) (connection-capabilities <name>)# udp-ipsec-vpn
(Instant AP) (connection-capabilities <name>)# udp-voip
(Instant AP) (connection-capabilities <name>)# enable
(Instant AP) (connection-capabilities <name>)# end
(Instant AP)# commit apply
```

Configuring an Operating-Class Profile

You can configure an operating-class profile to list the channels on which the hotspot is capable of operating.

To configure an H2QP operating-class profile:

```
(Instant AP) (config) # hotspot h2qp-oper-class-profile <name>
```

```
(Instant AP) (operator-class <name>)# op-class <class-ID>
(Instant AP) (operator-class <name>)# enable
(Instant AP) (operator-class <name>)# end
(Instant AP)# commit apply
```

Configuring a WAN Metrics Profile

You can configure a WAN metrics profile to define information about access network characteristics such as link status and metrics.

To configure a WAN metrics profile:

```
(Instant AP) (config)# hotspot h2qp-wan-metrics-profile <name>
(Instant AP) (WAN-metrics <name>)# at-capacity
(Instant AP) (WAN-metrics <name>)# downlink-load <load>
(Instant AP) (WAN-metrics <name>)# downlink-speed <speed>
(Instant AP) (WAN-metrics <name>)# load-duration <duration>
(Instant AP) (WAN-metrics <name>)# symm-link
(Instant AP) (WAN-metrics <name>)# uplink-load <load>
(Instant AP) (WAN-metrics <name>)# uplink-speed <speed>
(Instant AP) (WAN-metrics <name>)# wan-metrics-link-status <status>
(Instant AP) (WAN-metrics <name>)# end
(Instant AP)# commit apply
```

You can specify the following WAN downlink and uplink parameters:

- **Downlink load**—Indicates the percentage of the WAN downlink currently utilized. The default value of 0 indicates that the downlink speed is unknown or unspecified.
- **Downlink speed**—Indicates the WAN downlink speed in Kbps.
- **Uplink load**—Indicates the percentage of the WAN uplink currently utilized. The default value of 0 indicates that the downlink speed is unknown or unspecified.
- **Uplink speed**—Indicates the WAN uplink speed in Kbps.
- **Load duration**—Indicates the duration in seconds during which the downlink utilization is measured.
- **Symmetric links**—Indicates if the uplink and downlink have the same speed.
- **WAN Link Status**—Indicates if the WAN is down (link-down), up (link-up), or in test state (link-under-test).

Creating a Hotspot Profile

To create a hotspot profile:

```
(Instant AP) (config)# hotspot hs-profile <name>
(Instant AP) (Hotspot2.0 <name>)# asra
(Instant AP) (Hotspot2.0 <name>)# access-network-type <type>
(Instant AP) (Hotspot2.0 <name>)# addtl-roam-cons-ois <roam-consortium-OIs>
(Instant AP) (Hotspot2.0 <name>)# comeback-mode
(Instant AP) (Hotspot2.0 <name>)# gas-comeback <delay-interval>
(Instant AP) (Hotspot2.0 <name>)# group-frame-block
(Instant AP) (Hotspot2.0 <name>)# hessid <hotspot-ssid>
(Instant AP) (Hotspot2.0 <name>)# internet
(Instant AP) (Hotspot2.0 <name>)# p2p-cross-connect
(Instant AP) (Hotspot2.0 <name>)# p2p-dev-mgmt
(Instant AP) (Hotspot2.0 <name>)# pame-bi
(Instant AP) (Hotspot2.0 <name>)# query-response-length-limit <integer>
(Instant AP) (Hotspot2.0 <name>)# roam-cons-len-1 <integer>
(Instant AP) (Hotspot2.0 <name>)# roam-cons-len-2 <integer>
(Instant AP) (Hotspot2.0 <name>)# roam-cons-len-3 <integer>
(Instant AP) (Hotspot2.0 <name>)# roam-cons-oi-1 <integer>
(Instant AP) (Hotspot2.0 <name>)# roam-cons-oi-2 <integer>
(Instant AP) (Hotspot2.0 <name>)# roam-cons-oi-3 <integer>
(Instant AP) (Hotspot2.0 <name>)# venue-group <group>
(Instant AP) (Hotspot2.0 <name>)# venue-type <type>
```

```
(Instant AP) (Hotspot2.0 <name>) # enable
(Instant AP) (Hotspot2.0 <name>) # end
(Instant AP) # commit apply
```

The hotspot profile configuration parameters are described in the following table:

Table 81: Hotspot Profile Configuration Parameters

Parameter	Description
access-network-type <type>	<p>Specify any of the following 802.11u network types.</p> <ul style="list-style-type: none"> • private—This network is accessible for authorized users only. For example, home networks or enterprise networks that require user authentication. The corresponding integer value for this network type is 0. • private-with-guest—This network is accessible to guest users based on guest authentication methods. For example, enterprise networks that allow guest users with captive portal authentication. The corresponding integer value for this network type is 1. • chargeable-public—This network provides access to the Internet based on payment. For example, a subscription-based Internet access in a coffee shop or a hotel offering chargeable in-room Internet access service. The corresponding integer value for this network type is 2. • free-public—This network is accessible to all without any charges applied. For example, a hotspot in airport or other public places that provide Internet access with no additional cost. The corresponding integer value for this network type is 3. • personal-device—This network is accessible for personal devices. For example, a laptop or camera configured with a printer for the purpose of printing. The corresponding integer value for this network type is 4. • emergency-services—This network is limited to accessing emergency services only. The corresponding integer value for this network type is 5. • test—This network is used for test purposes only. The corresponding integer value for this network type is 14. • wildcard—This network indicates a wildcard network. The corresponding integer value for this network type is 15.
addtl-roam-cons-ois	Specify the number of additional roaming consortium Organization Identifiers (OIs) advertised by the OAW-IAP. You can specify up to three additional OIs.
asra	Enable the Additional Steps Required for Access (asra) to indicate if additional steps are required for authentication. When enabled, the following information is sent to the client in response to an ANQP query. For ASRA, ensure that the network authentication type is associated.
comeback-mode	Enable this parameter to allow the client to obtain a GAS Request and Response as a Comeback-Request and Comeback-Response. By default, this comeback mode is disabled.
gas-comeback-delay	Specify a GAS comeback delay interval in milliseconds to allow the client to retrieve the query response using a comeback request action frame when the GAS response is delayed. You can specify a value within the range of 100-2000 milliseconds and the default value is 500 milliseconds.

Table 81: Hotspot Profile Configuration Parameters

Parameter	Description
group-frame-block	Enable this parameter if you want to stop the OAW-IAP from sending forward downstream group-addressed frames.
hessid	Specify a Homogenous Extended Service Set Identifier (HESSID) in a hexadecimal format separated by colons.
internet	Specify this parameter to allow the OAW-IAP to send an Information Element (IE) indicating that the network allows Internet access.
p2p-cross-connect	Specify this parameter to advertise support for P2P cross-connections.
p2p-dev-mgmt	Specify this parameter to advertise support for P2P device management.
pame-bi	Specify this parameter to enable Pre-Association Message Exchange BSSID Independent (PAME-BI) bit, with which the OAW-IAP can indicate that the Advertisement Server can return a query response independent of the BSSID used in the GAS Frame exchange.
query-response-length-limit	Specify this parameter to set the maximum length of the GAS query response, in octets. You can specify a value within the range of 1–127. The default value is 127.
roam-cons-len-1 roam-cons-len-2 roam-cons-len-3	Specify the length of the organization identifier (OI). That is, the value for the length of OIs of roam-cons-len-1 , roam-cons-len-2 , or roam-cons-len-3 . The roaming consortium OI is based on the following parameters: <ul style="list-style-type: none"> ● 0: Zero Octets in the OI (Null) ● 3: OI length is 24-bits (3 Octets) ● 5: OI length is 36-bits (5 Octets)
venue-group	Specify one of the following venue groups <ul style="list-style-type: none"> ● unspecified ● assembly ● business ● educational ● factory-and-industrial ● institutional ● mercantile ● outdoor ● residential ● storage ● utility-misc ● vehicular <p>By default, the business venue group is used.</p>
venue-type	Specify a venue type to be advertised in the ANQP IEs from OAW-IAPs associated with this hotspot profile. For more information about the supported venue types for each venue group, see Table 80 .

Associating an Advertisement Profile to a Hotspot Profile

To associate a hotspot profile with an advertisement profile:

```
(Instant AP) (config)# hotspot hs-profile <name>
(Instant AP) (Hotspot2.0 <name>)# advertisement-protocol <protocol>
(Instant AP) (Hotspot2.0 <name>)# advertisement-profile anqp-3gpp <name>
(Instant AP) (Hotspot2.0 <name>)# advertisement-profile anqp-domain-name <name>
(Instant AP) (Hotspot2.0 <name>)# advertisement-profile anqp-ip-addr-avail <name>
(Instant AP) (Hotspot2.0 <name>)# advertisement-profile anqp-nai-realm <name>
(Instant AP) (Hotspot2.0 <name>)# advertisement-profile anqp-nwk-auth <name>
(Instant AP) (Hotspot2.0 <name>)# advertisement-profile anqp-roam-cons <name>
(Instant AP) (Hotspot2.0 <name>)# advertisement-profile anqp-venue-name <name>
(Instant AP) (Hotspot2.0 <name>)# advertisement-profile h2qp-conn-cap <name>
(Instant AP) (Hotspot2.0 <name>)# advertisement-profile h2qp-oper-class <name>
(Instant AP) (Hotspot2.0 <name>)# advertisement-profile h2qp-oper-name <name>
(Instant AP) (Hotspot2.0 <name>)# advertisement-profile h2qp-wan-metrics <name>
(Instant AP) (Hotspot2.0 <name>)# end
(Instant AP)# commit apply
```

The configuration parameters for associating an advertisement profile with a hotspot profile are described in the following table:

Table 82: Advertisement Profile Association Parameters

Parameter	Description
advertisement-profile	Specify the advertisement profile to associate with this hotspot profile. For information on advertisement profiles, see Creating Advertisement Profiles for Hotspot Configuration on page 376 .
advertisement-protocol	Specify the advertisement protocol type; for example, specify the Access Network Query Protocol (ANQP) as anqp .

Creating a WLAN SSID and Associating Hotspot Profile

To create a WLAN SSID with Enterprise Security and WPA-2 Encryption Settings:

```
(Instant AP) (config)# wlan ssid-profile <name>
(Instant AP) (SSID Profile <name>)# essid <ESSID-name>
(Instant AP) (SSID Profile <name>)# type {<Employee> | <Voice>| <Guest>}
(Instant AP) (SSID Profile <name>)# wlan <vlan-ID>
(Instant AP) (SSID Profile <name>)# set-vlan <attribute>{equals|not-equals|starts-with|ends-with|contains} <operator> <VLAN-ID>| value-of}
(Instant AP) (SSID Profile <name>)# opmode {wpa2-aes|wpa-tkip,wpa2-aes}
(Instant AP) (SSID Profile <name>)# blacklist
(Instant AP) (SSID Profile <name>)# mac-authentication
(Instant AP) (SSID Profile <name>)# l2-auth-failthrough
(Instant AP) (SSID Profile <name>)# termination
(Instant AP) (SSID Profile <name>)# external-server
(Instant AP) (SSID Profile <name>)# auth-server <server-name>
(Instant AP) (SSID Profile <name>)# server-load-balancing
(Instant AP) (SSID Profile <name>)# radius-accounting
(Instant AP) (SSID Profile <name>)# radius-accounting-mode {user-authentication| user-association}
(Instant AP) (SSID Profile <name>)# radius-interim-accounting-interval <minutes>
(Instant AP) (SSID Profile <name>)# radius-reauth-interval <minutes>
(Instant AP) (SSID Profile <name>)# set-role-by-ssid
(Instant AP) (SSID Profile <name>)# end
(Instant AP)# commit apply
```

Sample Configuration

Step 1: Creating ANQP and H2QP Advertisement Profiles

```
(Instant AP) # configure terminal
(Instant AP) (config) # hotspot anqp-nai-realm-profile nr1
(Instant AP) (nai-realm "nr1") # nai-realm-name name1
(Instant AP) (nai-realm "nr1") # nai-realm-encoding utf8
(Instant AP) (nai-realm "nr1") # nai-realm-eap-method eap-sim
(Instant AP) (nai-realm "nr1") # nai-realm-auth-id-1 non-eap-inner-auth
(Instant AP) (nai-realm "nr1") # nai-realm-auth-value-1 mschapv2
(Instant AP) (nai-realm "nr1") # nai-home-realm
(Instant AP) (nai-realm "nr1") # exit

(Instant AP) (config) # hotspot anqp-venue-name-profile vn1
(Instant AP) (venue-name "vn1") # venue-group business
(Instant AP) (venue-name "vn1") # venue-type research-and-dev-facility
(Instant AP) (venue-name "vn1") # venue-lang-code eng
(Instant AP) (venue-name "vn1") # venue-name VenueName
(Instant AP) (venue-name "vn1") # exit

(Instant AP) (config) # hotspot anqp-nwk-auth-profile na1
(Instant AP) (network-auth "na1") # nwk-auth-type accept-term-and-cond
(Instant AP) (network-auth "na1") # url www.nwkauth.com
(Instant AP) (network-auth "na1") # exit

(Instant AP) (config) # hotspot anqp-roam-cons-profile rc1
(Instant AP) (roaming-consortium "rc1") # roam-cons-oi-len 3
(Instant AP) (roaming-consortium "rc1") # roam-cons-oi 888888
(Instant AP) (roaming-consortium "rc1") # exit

(Instant AP) (config) # hotspot anqp-3gpp-profile 3g
(Instant AP) (3gpp "3g") # 3gpp-plmn1 40486
(Instant AP) (3gpp "3g") # exit

(Instant AP) (config) # hotspot anqp-ip-addr-avail-profile ip1
(Instant AP) (IP-addr-avail "ip1") # no ipv4-addr-avail
(Instant AP) (IP-addr-avail "ip1") # ipv6-addr-avail
(Instant AP) (IP-addr-avail "ip1") # exit

(Instant AP) (config) # hotspot anqp-domain-name-profile dn1
(Instant AP) (domain-name "dn1") # domain-name DomainName
(Instant AP) (domain-name "dn1") # exit

(Instant AP) (config) # hotspot h2qp-oper-name-profile on1
(Instant AP) (operator-friendly-name"on1") # op-lang-code eng
(Instant AP) (operator-friendly-name"on1") # op-fr-name OperatorFriendlyName
(Instant AP) (operator-friendly-name"on1") # exit

(Instant AP) (config) # hotspot h2qp-conn-cap-profile <name>
(Instant AP) (connection-capabilities <name>) # esp-port
(Instant AP) (connection-capabilities <name>) # icmp
(Instant AP) (connection-capabilities <name>) # tcp-ftp
(Instant AP) (connection-capabilities <name>) # tcp-http
(Instant AP) (connection-capabilities <name>) # tcp-pptp-vpn
(Instant AP) (connection-capabilities <name>) # tcp-ssh
(Instant AP) (connection-capabilities <name>) # tcp-tls-vpn
(Instant AP) (connection-capabilities <name>) # tcp-voip
(Instant AP) (connection-capabilities <name>) # udp-ike2
(Instant AP) (connection-capabilities <name>) # udp-ipsec-vpn
(Instant AP) (connection-capabilities <name>) # udp-voip
(Instant AP) (connection-capabilities <name>) # enable
(Instant AP) (connection-capabilities <name>) # exit
```

```

(Instant AP) (config) # hotspot h2qp-oper-class-profile <profile>
(Instant AP) (operator-class <name>)# op-class <class-ID>
(Instant AP) (operator-class <name>)# enable
(Instant AP) (operator-class <name>)# exit

(Instant AP) (config)# hotspot h2qp-wan-metrics-profile <name>
(Instant AP) (WAN-metrics <name>)# at-capacity
(Instant AP) (WAN-metrics <name>)# downlink-load <load>
(Instant AP) (WAN-metrics <name>)# downlink-speed <speed>
(Instant AP) (WAN-metrics <name>)# load-duration <duration>
(Instant AP) (WAN-metrics <name>)# symm-link
(Instant AP) (WAN-metrics <name>)# uplink-load <load>
(Instant AP) (WAN-metrics <name>)# uplink-speed <speed>
(Instant AP) (WAN-metrics <name>)# wan-metrics-link-status <status>
(Instant AP) (WAN-metrics <name>)# exit

```

Step 2: Creating a hotspot profile

```

(Instant AP) # configure terminal
(Instant AP) (config)# hotspot hs-profile hs1
(Instant AP) (Hotspot2.0 "hs1")# enable
(Instant AP) (Hotspot2.0 "hs1")# comeback-mode
(Instant AP) (Hotspot2.0 "hs1")# gas-comeback-delay 10
(Instant AP) (Hotspot2.0 "hs1")# no asra
(Instant AP) (Hotspot2.0 "hs1")# no internet
(Instant AP) (Hotspot2.0 "hs1")# query-response-length-limit 20
(Instant AP) (Hotspot2.0 "hs1")# access-network-type chargeable-public
(Instant AP) (Hotspot2.0 "hs1")# roam-cons-len-1 3
(Instant AP) (Hotspot2.0 "hs1")# roam-cons-oi-1 123456
(Instant AP) (Hotspot2.0 "hs1")# roam-cons-len-2 3
(Instant AP) (Hotspot2.0 "hs1")# roam-cons-oi-2 223355
(Instant AP) (Hotspot2.0 "hs1")# addtl-roam-cons-ois 0
(Instant AP) (Hotspot2.0 "hs1")# venue-group business
(Instant AP) (Hotspot2.0 "hs1")# venue-type research-and-dev-facility
(Instant AP) (Hotspot2.0 "hs1")# pame-bi
(Instant AP) (Hotspot2.0 "hs1")# group-frame-block
(Instant AP) (Hotspot2.0 "hs1")# p2p-dev-mgmt
(Instant AP) (Hotspot2.0 "hs1")# p2p-cross-connect
(Instant AP) (Hotspot2.0 "hs1")# end
(Instant AP) # commit apply

```

Step 3: Associating advertisement profiles with the hotspot profile

```

(Instant AP) # configure terminal
(Instant AP) (config)# hotspot hs-profile hs1
(Instant AP) (Hotspot2.0 "hs1")# advertisement-profile anqp-nai-realm nr1
(Instant AP) (Hotspot2.0 "hs1")# advertisement-profile anqp-venue-name vn1
(Instant AP) (Hotspot2.0 "hs1")# advertisement-profile anqp-nwk-auth na1
(Instant AP) (Hotspot2.0 "hs1")# advertisement-profile anqp-roam-cons rc1
(Instant AP) (Hotspot2.0 "hs1")# advertisement-profile anqp-3gpp 3g1
(Instant AP) (Hotspot2.0 "hs1")# advertisement-profile anqp-ip-addr-avail ip1
(Instant AP) (Hotspot2.0 "hs1")# advertisement-profile anqp-domain-name dn1
(Instant AP) (Hotspot2.0 "hs1")# advertisement-profile h2qp-oper-name on1
(Instant AP) (Hotspot2.0 "hs1")# advertisement-profile h2qp-wan-metrics wm1
(Instant AP) (Hotspot2.0 "hs1")# advertisement-profile h2qp-conn-cap cc1
(Instant AP) (Hotspot2.0 "hs1")# advertisement-profile h2qp-oper-class oc1
(Instant AP) (Hotspot2.0 "hs1")# end
(Instant AP) # commit apply

```

Step 4: Associating the hotspot profile with WLAN SSID:

```

(Instant AP) # configure terminal
(Instant AP) # wlan ssid-profile ssidProfile1
(Instant AP) (SSID Profile "ssidProfile1")# essid hsProf

```

```
(Instant AP) (SSID Profile "ssidProfile1")# type employee
(Instant AP) (SSID Profile "ssidProfile1")# vlan 200
(Instant AP) (SSID Profile "ssidProfile1")# opmode wpa2-aes
(Instant AP) (SSID Profile "ssidProfile1")# blacklist
(Instant AP) (SSID Profile "ssidProfile1")# mac-authentication
(Instant AP) (SSID Profile "ssidProfile1")# l2-auth-failthrough
(Instant AP) (SSID Profile "ssidProfile1")# radius-accounting
(Instant AP) (SSID Profile "ssidProfile1")# radius-accounting-mode user-association
(Instant AP) (SSID Profile "ssidProfile1")# radius-interim-accounting-interval 10
(Instant AP) (SSID Profile "ssidProfile1")# radius-reauth-interval 20
(Instant AP) (SSID Profile "ssidProfile1")# max-authentication-failures 2
(Instant AP) (SSID Profile "ssidProfile1")# set-role-by-ssid
(Instant AP) (SSID Profile "ssidProfile1")# hotspot-profile hsl
(Instant AP) (SSID Profile "ssidProfile1")# end
(Instant AP)# commit apply
```

This chapter consists of the following topics:

[Configuring ClearPass Guest on page 390](#)

[Verifying ClearPass Guest Setup on page 393](#)

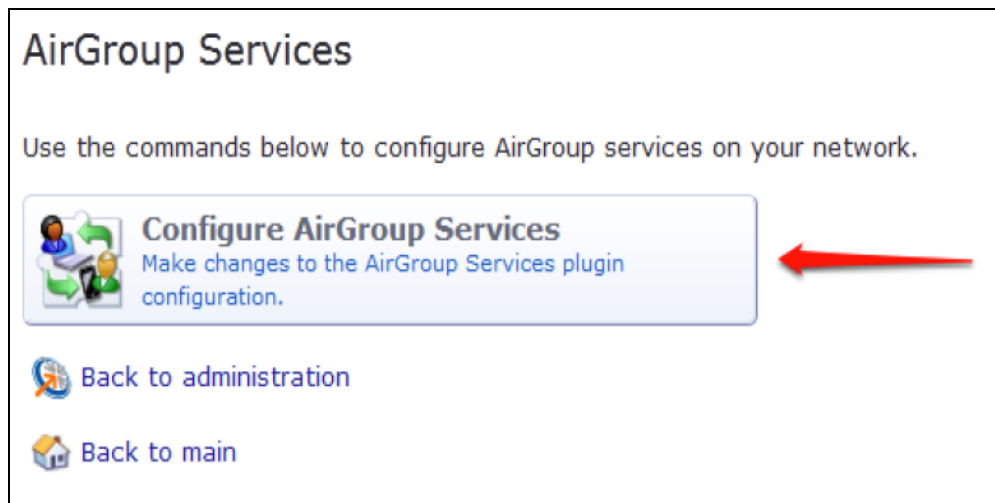
[Troubleshooting on page 393](#)

Configuring ClearPass Guest

To configure ClearPass Guest:

1. From the ClearPass Guest UI, navigate to **Administration > AirGroup Services**.
2. Click **Configure AirGroup Services**.

Figure 113 *Configure AirGroup Services*



3. Click **Add a new controller**.
4. Update the parameters with appropriate values.



Ensure that the port configured matches the CoA port ([RFC 3576](#)) set on the OAW-IAP configuration.

5. Click **Save Configuration**.

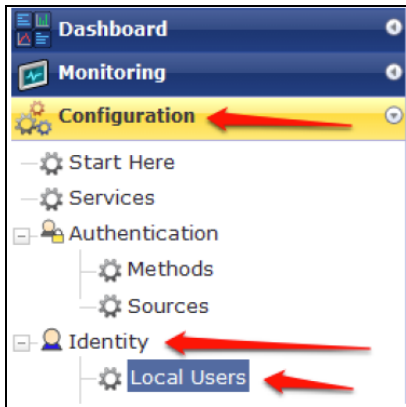
In order to demonstrate AirGroup, either an AirGroup Administrator or an AirGroup Operator account must be created.

Creating AirGroup Administrator and Operator Account

To create a AirGroup administrator and AirGroup operator account using the ClearPass Policy Manager UI:

1. Navigate to the ClearPass Policy Manager UI, and navigate to **Configuration > Identity > Local Users**.

Figure 114 Configuration > Identity > Local Users Selection



2. Click **Add User**.
3. Create an **AirGroup Administrator** by entering the required values.

Figure 115 Create an AirGroup Administrator

A screenshot of the 'Add Local User' form. The form contains the following fields:

- User ID: airgroup-admin
- Name: AirGroup Admin
- Password: masked with dots
- Verify Password: masked with dots
- Enable User: (Check to enable local user)
- Role: [AirGroup Administrator] (dropdown menu)

Below the fields is an 'Attributes' section with a table:

Attribute	Value
1. Click to add...	

At the bottom right of the form are 'Add' and 'Cancel' buttons. A red arrow points to the Role dropdown menu.

4. Click **Add**.
5. Now click **Add User** to create an **AirGroup Operator**.

Figure 116 Create an AirGroup Operator

The 'Add Local User' dialog box contains the following fields:

- User ID: airgroup-oper
- Name: AirGroup Operator
- Password: [masked]
- Verify Password: [masked]
- Enable User: (Check to enable local user)
- Role: [AirGroup Operator] (indicated by a red arrow)

Below the fields is an 'Attributes' table with columns 'Attribute' and 'Value'. The first row contains '1. Click to add...'. At the bottom right are 'Add' and 'Cancel' buttons.

6. Click **Add** to save the user with an **AirGroup Operator** role. The **AirGroup Administrator** and **AirGroup Operator** IDs will be displayed in the **Local Users** UI screen.

Figure 117 Local Users UI Screen

ClearPass Policy Manager
admin (Super Administrator)

Configuration > Identity > Local Users

Local Users

User deleted successfully

Filter: User ID contains [] Go Clear Filter Show 10 records

#	<input type="checkbox"/>	User ID	Name	Role	Status
1.	<input type="checkbox"/>	airgroup-admin	AirGroup Admin	[AirGroup Administrator]	Enabled
2.	<input type="checkbox"/>	airgroup-oper	AirGroup Operator	[AirGroup Operator]	Enabled
3.	<input type="checkbox"/>	test	test	TestRole	Enabled

Showing 1-3 of 3

Buttons: Add User, Import Users, Export Users, Export, Delete

7. Navigate to the ClearPass Guest UI and click **Logout**. The **ClearPass Guest Login** page is displayed. Use the AirGroup admin credentials to log in.
8. After logging in, click **Create Device**.

Figure 118 Create a Device



The **Register Shared Device** page is displayed.

Figure 119 ClearPass Guest- Register Shared Device

Register Shared Device	
* Device Name:	<input type="text"/> Enter a name to identify the device.
* MAC Address:	<input type="text"/> Enter the MAC address of the device.
Shared Locations:	<input type="text"/> Enter a list of location IDs where this device will be shared. Use a comma-separated list of tag=value pairs; tag may be AP-Name, AP-Group, or FQLN. A fully qualified location name is '<ap-name>.floor<N>.<building-name>.<campus>'. Leave blank to share with all locations.
Shared With:	<input type="text"/> Enter up to 10 usernames that will be able to use this device. Use a comma-separated list, e.g. user1,user2,user3, or blank for all users.
Shared Roles:	<input type="text"/> List the user roles that will be able to use this device. Use a comma-separated list, e.g. role1,role2,role3, or blank for all roles.
	

For this test, add your AppleTV device name and MAC address but leave all other boxes empty.

9. Click **Register Shared Device**.

Verifying ClearPass Guest Setup

To verify the setup:

1. Disconnect your AppleTV and OSX Mountain Lion/iOS 6 devices if they were previously connected to the wireless network. Remove their entries from the switch's user table using these commands:
 - Find the MAC address—**show user table**
 - Delete the address from the table—**aaa user delete mac 00:aa:22:bb:33:cc**
2. Reconnect both devices. To limit access to the AppleTV, access the ClearPass Guest UI using either the AirGroup admin or the AirGroup operator credentials. Next, navigate to **List Devices > Test Apple TV > Edit**. Add a username that is not used to log in to the Apple devices in the **Shared With** box.
3. Disconnect and remove the OSX Mountain Lion/iOS 6 device from the switch's user table. Reconnect the device by not using the username that you added to the **Shared With** box. The AppleTV should not be available to this device.
4. Disconnect the OSX Mountain Lion/iOS 6 device and delete it from the switch's user table. Reconnect using the username that was added to the **Shared With** box. The OSX Mountain Lion/iOS 6 device should once again have access to the AppleTV.

Troubleshooting

Table 83: *Troubleshooting*

Problem	Solution
Limiting devices has no effect.	Ensure IPv6 is disabled.
Apple Macintosh running Mountain Lion can use AirPlay but iOS devices cannot.	Ensure IPv6 is disabled.

This section describes the most common IAP-VPN deployment models and provides information to carry out the necessary configuration procedures. The examples in this section refer to more than one DHCP profile and wired port configuration in addition to wireless SSID configuration. All these are optional. In most networks, a single DHCP profile and wireless SSID configuration referring to a DHCP profile is sufficient.

The following scenarios are described in this section:

- [Scenario 1—IPsec: Single Datacenter Deployment with No Redundancy on page 396](#)
- [Scenario 2—IPsec: Single Datacenter with Multiple Switches for Redundancy on page 400](#)
- [Scenario 3—IPsec: Multiple Datacenter Deployment with Primary and Backup Switches for Redundancy on page 404](#)
- [Scenario 4—GRE: Single Datacenter Deployment with No Redundancy on page 409](#)

Scenario 1—IPsec: Single Datacenter Deployment with No Redundancy

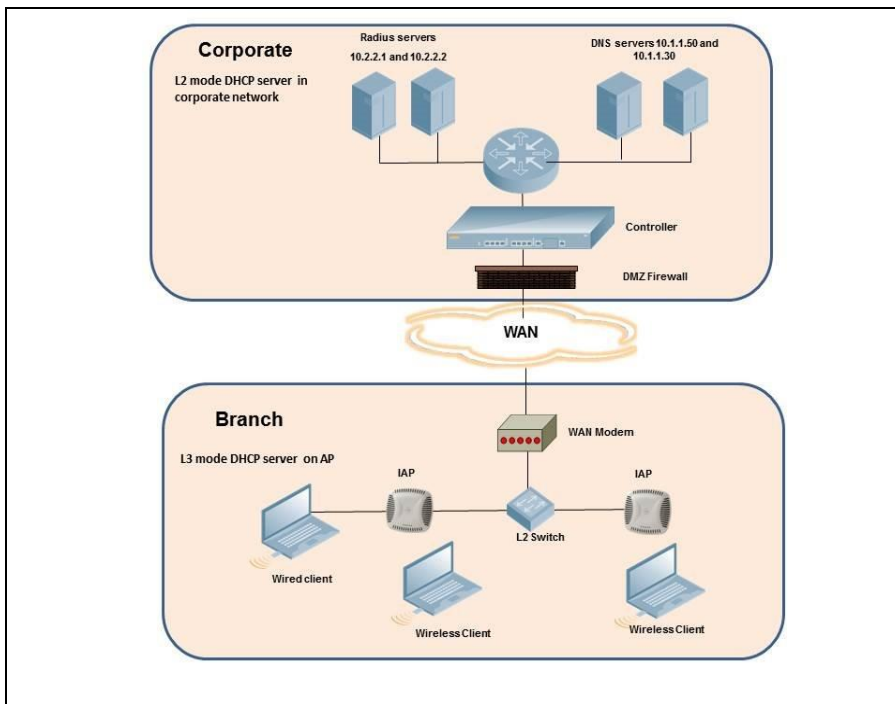
This scenario includes the following configuration elements:

1. Single VPN primary configuration using IPsec.
2. Split-tunneling of client traffic.
3. Split-tunneling of DNS traffic from clients.
4. Distributed, L3 and Centralized, L2 mode DHCP.
5. RADIUS server within corporate network and authentication survivability for branch survivability.
6. Wired and wireless users in L2 and L3 modes, respectively.
7. Access rules defined for wired and wireless networks to permit all traffic.

Topology

Figure 120 shows the topology and the IP addressing scheme used in this scenario.

Figure 120 Scenario 1—IPsec: Single datacenter Deployment with No Redundancy



The following IP addresses are used in the examples for this scenario:

- 10.0.0.0/8 is the corporate network
- 10.20.0.0/16 subnet is reserved for L2 mode
- 10.30.0.0/16 subnet is reserved for L3 mode
- Client count in each branch is 200

OAW-IAP Configuration

The following table provides information on the configuration steps performed through the CLI with example values. For information on the UI procedures, see the topics referenced in the *UI Procedure* column.

Table 84: OAW-IAP Configuration for Scenario 1—IPsec: Single Datacenter Deployment with No Redundancy

Configuration Steps	CLI Commands	UI Procedure
1. Configure the primary host for VPN with the Public VRRP IP address of the switch.	<pre>(Instant AP) (config)# vpn primary <public VRRP IP of switch></pre>	See Configuring an IPsec Tunnel
2. Configure a routing profile to tunnel all 10.0.0.0/8 subnet traffic to switch.	<pre>(Instant AP) (config)# routing-profile (Instant AP) (routing-profile)# route 10.0.0.0 255.0.0.0 <public VRRP IP of switch></pre>	See Configuring Routing Profiles
3. Configure Enterprise DNS for split DNS. The example in the next column uses a specific enterprise domain to only tunnel all DNS queries matching that domain to corporate.	<pre>(Instant AP) (config)# internal-domains (Instant AP) (domains)# domain-name corpdomain.com</pre>	See Configuring Enterprise Domains
4. Configure Centralized, L2 and Distributed, L3 with VLAN 20 and VLAN 30, respectively.	<p>Centralized, L2 profile</p> <pre>(Instant AP) (config)# ip dhcp l2-dhcp (Instant AP) (DHCP Profile "l2-dhcp")# server-type Centralized,L2 (Instant AP) (DHCP Profile "l2-dhcp")# server-vlan 20</pre> <p>Distributed, L3 profile</p> <pre>(Instant AP) (config)# ip dhcp l3-dhcp (Instant AP) (DHCP Profile "l3-dhcp")# server-type Distributed,L3 (Instant AP) (DHCP Profile "l3-dhcp")# server-vlan 30 (Instant AP) (DHCP Profile "l3-dhcp")# ip-range 10.30.0.0 10.30.255.255 (Instant AP) (DHCP Profile "l3-dhcp")# dns-server 10.1.1.50,10.1.1.30 (Instant AP) (DHCP Profile "l3-dhcp")# domain-name corpdomain.com (Instant AP) (DHCP Profile "l3-dhcp")# client-count 200</pre> <p>NOTE: The IP range configuration on each branch will be the same. Each OAW-IAP will derive a smaller subnet based on the client count scope using the Branch ID (BID) allocated by switch.</p>	See Configuring Centralized DHCP Scopes and Configuring Distributed DHCP Scopes
5. Create authentication servers for user authentication. The example in the next column assumes 802.1X SSID.	<pre>(Instant AP) (config)# wlan auth-server server1 (Instant AP) (Auth Server "server1")# ip 10.2.2.1 (Instant AP) (Auth Server "server1")# port 1812 (Instant AP) (Auth Server "server1")# acctport 1813 (Instant AP) (Auth Server "server1")# key "presharedkey" (Instant AP) (Auth Server "server1")# exit</pre> <pre>(Instant AP) (config)# wlan auth-server server2 (Instant AP) (Auth Server "server2")# ip 10.2.2.2 (Instant AP) (Auth Server "server2")# port 1812</pre>	See Configuring an External Server for Authentication

Table 84: OAW-IAP Configuration for Scenario 1—IPsec: Single Datacenter Deployment with No Redundancy

Configuration Steps	CLI Commands	UI Procedure
	<pre>(Instant AP) (Auth Server "server2") # acctport 1813 (Instant AP) (Auth Server "server2") # key "presharedkey"</pre>	
<p>6. Configure wired port and wireless SSIDs using the authentication servers.</p>	<p>Configure wired ports to operate in L2 mode and associate Centralized, L2 mode VLAN 20 to the wired port profile.</p> <pre>(Instant AP) (config) # wired-port-profile wired-port (Instant AP) (wired-port-profile "wired-port") # switchport-mode access (Instant AP) (wired-port-profile "wired-port") # allowed-vlan all (Instant AP) (wired-port-profile "wired-port") # native-vlan 20 (Instant AP) (wired-port-profile "wired-port") # no shutdown (Instant AP) (wired-port-profile "wired-port") # access-rule-name wired-port (Instant AP) (wired-port-profile "wired-port") # type employee (Instant AP) (wired-port-profile "wired-port") # auth- server server1 (Instant AP) (wired-port-profile "wired-port") # auth- server server2 (Instant AP) (wired-port-profile "wired-port") # dot1x (Instant AP) (wired-port-profile "wired-port") # exit (Instant AP) (config) # enet1-port-profile wired-port</pre> <p>Configure a wireless SSID to operate in L3 mode and associate Distributed, L3 mode VLAN 30 to the WLAN SSID profile.</p> <pre>(Instant AP) (config) # wlan ssid-profile wireless- ssid (Instant AP) (SSID Profile "wireless-ssid") # enable (Instant AP) (SSID Profile "wireless-ssid") # type employee (Instant AP) (SSID Profile "wireless-ssid") # essid wireless-ssid (Instant AP) (SSID Profile "wireless-ssid") # opmode wpa2-aes (Instant AP) (SSID Profile "wireless-ssid") # vlan 30 (Instant AP) (SSID Profile "wireless-ssid") # auth- server server1 (Instant AP) (SSID Profile "wireless-ssid") # auth- server server2 (Instant AP) (SSID Profile "wireless-ssid") # auth- survivability</pre>	<p>See Configuring a Wired Profile and Wireless Network Profiles</p>
<p>7. Create access rule for wired and wireless authentication. In this example, the rule permits all traffic.</p>	<p>For wired profile:</p> <pre>(Instant AP) (config) # wlan access-rule wired-port (Instant AP) (Access Rule "wired-port") # rule any any match any any permit</pre> <p>For WLAN SSID:</p> <pre>(Instant AP) (config) # wlan access-rule wireless-ssid</pre>	<p>See Configuring ACL Rules for Network Services</p>

Table 84: OAW-IAP Configuration for Scenario 1—IPsec: Single Datacenter Deployment with No Redundancy

Configuration Steps	CLI Commands	UI Procedure
	<pre>(Instant AP) (Access Rule "wireless-ssid")# rule any any match any any any permit</pre>	
NOTE: Ensure that you execute the commit apply command in the AOS-W Instant CLI before saving the configuration and propagating changes across the OAW-IAP cluster.		

OAW-IAP-Connected Switch Configuration

Client VLANs defined in this example must be opened on the upstream switches in multiple OAW-IAP deployments, as client traffic from the slave to the master is tagged with the client VLAN.

Datacenter Configuration

For information on switch configuration, see [Configuring a Switch for IAP-VPN Operations on page 245](#). Ensure that the upstream router is configured with a static route pointing to the switch for the L3 VLAN.

Scenario 2—IPsec: Single Datacenter with Multiple Switches for Redundancy

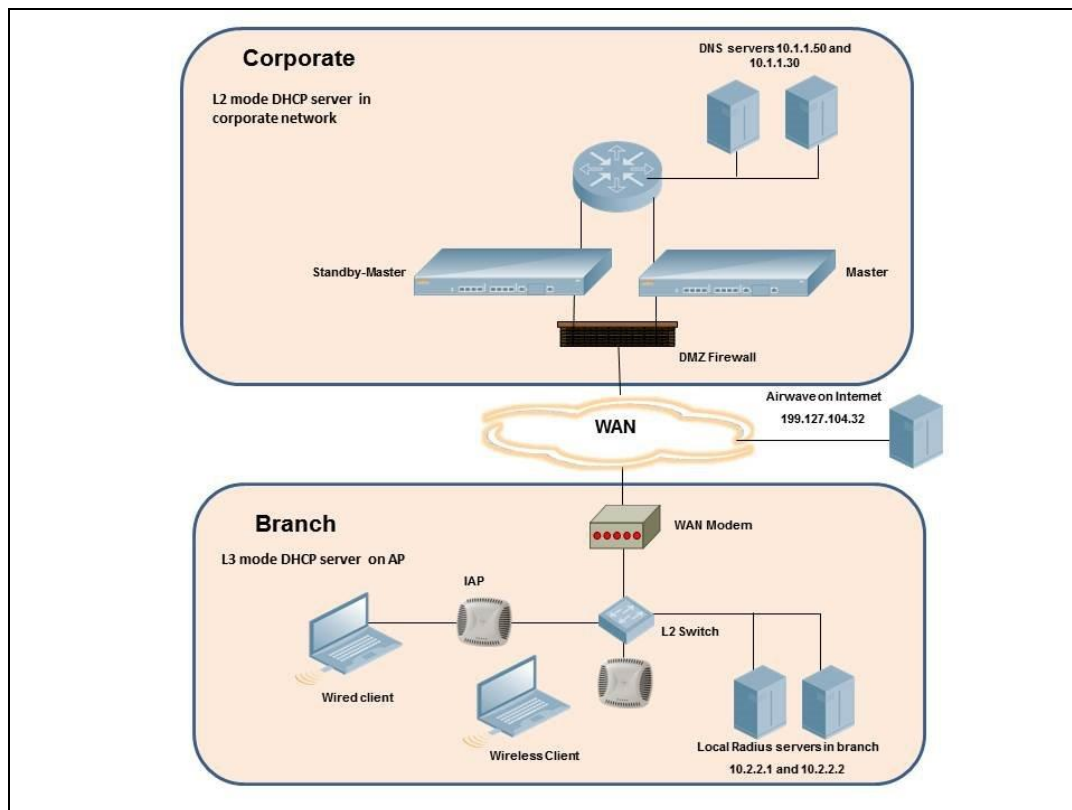
This scenario includes the following configuration elements:

- A VRRP instance between the master/standby-master pair, which is configured as the primary VPN IP address.
- Tunneling of all traffic to datacenter.
- Exception route to bypass tunneling of RADIUS and OmniVista traffic, which are locally reachable in the branch and the Internet, respectively.
- All client DNS queries are tunneled to the switch.
- Distributed, L3 and Centralized, L2 mode DHCP on all branches. L3 is used by the employee network and L2 is used by the guest network with captive portal.
- Wired and wireless users in L2 and L3 modes.
- Access rules defined for wired and wireless networks.

Topology

Figure 121 shows the topology and the IP addressing scheme used in this scenario.

Figure 121 Scenario 2—IPsec: Single Datacenter with Multiple switches for Redundancy



The following IP addresses are used in the examples for this scenario:

- 10.0.0.0/8 is the corporate network
- 10.20.0.0/16 subnet is reserved for L2 mode – used for guest network
- 10.30.0.0/16 subnet is reserved for L3 mode
- Client count in each branch is 200

- 10.2.2.0/24 is a branch-owned subnet, which needs to override global routing profile
- 199.127.104.32 is used an example IP address of the OmniVista server in the Internet

OAW-IAP Configuration

The following table provides information on the configuration steps performed through the CLI with example values. For information on the UI procedures, see the topics referenced in the *UI Procedure* column.

Table 85: OAW-IAP Configuration for Scenario 2—IPsec: Single Datacenter with Multiple switches for Redundancy

Configuration Steps	CLI Commands	UI Procedure
1. Configure the primary host for VPN with the Public VRRP IP address of the switch.	<pre>(Instant AP) (config)# vpn primary <public VRRP IP of switch></pre>	See Configuring an IPsec Tunnel
2. Configure routing profiles to tunnel traffic through IPsec.	<pre>(Instant AP) (config)# routing-profile (Instant AP) (routing-profile)# route 0.0.0.0 0.0.0.0 <public VRRP IP of switch></pre>	See Configuring Routing Profiles
3. Define routing profile exception RADIUS server and OmniVista IPs, since the design requirement for this solution requires local RADIUS authentication, even though the IP matches the routing profile destination.	<pre>(Instant AP) (config)# routing-profile (Instant AP) (routing-profile)# route 10.2.2.1 255.255.255.255 0.0.0.0 (Instant AP) (routing-profile)# route 10.2.2.2 255.255.255.255 0.0.0.0 (Instant AP) (routing-profile)# route 199.127.104.32 255.255.255.255 0.0.0.0</pre>	See Configuring Routing Profiles
4. Configure Enterprise DNS. The configuration example in the next column tunnels all DNS queries to the original DNS server of clients without proxying on OAW-IAP.	<pre>(Instant AP) (config)# internal-domains (Instant AP) (domains)# domain-name *</pre>	See Configuring Enterprise Domains
5. Configure Centralized, L2 and Distributed, L3 with VLAN 20 and VLAN 30, respectively.	<p>Centralized, L2 profile</p> <pre>(Instant AP) (config)# ip dhcp l2-dhcp (Instant AP) (DHCP Profile "l2-dhcp")# server-type Centralized,L2 (Instant AP) (DHCP Profile "l2-dhcp")# server-vlan 20</pre> <p>Distributed, L3 profile</p> <pre>(Instant AP) (config)# ip dhcp l3-dhcp (Instant AP) (DHCP Profile "l3-dhcp")# server-type Distributed,L3 (Instant AP) (DHCP Profile "l3-dhcp")# server-vlan 30 (Instant AP) (DHCP Profile "l3-dhcp")# ip-range 10.30.0.0 10.30.255.255 (Instant AP) (DHCP Profile "l3-dhcp")# dns-server 10.1.1.50,10.1.1.30 (Instant AP) (DHCP Profile "l3-dhcp")# domain-name corpdomain.com</pre>	See Configuring Centralized DHCP Scopes and Configuring Distributed DHCP Scopes

Table 85: OAW-IAP Configuration for Scenario 2—IPsec: Single Datacenter with Multiple switches for Redundancy

Configuration Steps	CLI Commands	UI Procedure
	<pre>(Instant AP) (DHCP Profile "l3-dhcp")# client-count 200</pre> <p>NOTE: The IP range configuration on each branch will be the same. Each OAW-IAP will derive a smaller subnet based on the client count scope using the Branch ID (BID) allocated by switch.</p>	
<p>6. Create authentication servers for user authentication. The example in the next column assumes 802.1X SSID.</p>	<pre>(Instant AP) (config)# wlan auth-server server1 (Instant AP) (Auth Server "server1")# ip 10.2.2.1 (Instant AP) (Auth Server "server1")# port 1812 (Instant AP) (Auth Server "server1")# acctport 1813 (Instant AP) (Auth Server "server1")# key "presharedkey" (Instant AP) (Auth Server "server1")# exit (Instant AP) (config)# wlan auth-server server2 (Instant AP) (Auth Server "server2")# ip 10.2.2.2 (Instant AP) (Auth Server "server2")# port 1812 (Instant AP) (Auth Server "server2")# acctport 1813 (Instant AP) (Auth Server "server2")# key "presharedkey"</pre>	<p>See Configuring an External Server for Authentication</p>
<p>7. Configure wired port and wireless SSIDs using the authentication servers.</p>	<p>Configure wired ports to operate in L3 mode and associate Distributed, L3 mode VLAN 30 to the wired port profile.</p> <pre>(Instant AP) (config) # wired-port-profile wired-port (Instant AP) (wired-port-profile "wired-port")# switchport-mode access (Instant AP) (wired-port-profile "wired-port")# allowed-vlan all (Instant AP) (wired-port-profile "wired-port")# native-vlan 30 (Instant AP) (wired-port-profile "wired-port")# no shutdown (Instant AP) (wired-port-profile "wired-port")# access-rule-name wired-port (Instant AP) (wired-port-profile "wired-port")# type employee (Instant AP) (wired-port-profile "wired-port")# auth-server server1 (Instant AP) (wired-port-profile "wired-port")# auth-server server2 (Instant AP) (wired-port-profile "wired-port")# dot1x (Instant AP) (wired-port-profile "wired-port")# exit (Instant AP) (config)# enet1-port-profile wired-port</pre> <p>Configure a wireless SSID to operate in L2 mode and associate Centralized, L2 mode VLAN 20 to the WLAN SSID profile.</p> <pre>(Instant AP) (config) # wlan ssid-profile guest (Instant AP) (SSID Profile "guest")# enable (Instant AP) (SSID Profile "guest")# type guest (Instant AP) (SSID Profile "guest")# essid guest (Instant AP) (SSID Profile "guest")# opmode opensystem (Instant AP) (SSID Profile "guest")# vlan 20</pre>	<p>See Configuring a Wired Profile and Wireless Network Profiles</p>

Table 85: OAW-IAP Configuration for Scenario 2—IPsec: Single Datacenter with Multiple switches for Redundancy

Configuration Steps	CLI Commands	UI Procedure
	<pre>(Instant AP) (SSID Profile "guest") # auth-server server1 (Instant AP) (SSID Profile "guest") # auth-server server2 (Instant AP) (SSID Profile "guest") # captive-portal internal</pre> <p>NOTE: This example uses internal captive portal use case using external authentication server. You can also use an external captive portal example.</p> <p>NOTE: The SSID type guest is used in this example to enable configuration of captive portal. However, corporate access through VPN tunnel is still allowed for this SSID because the VLAN associated to this SSID is a VPN-enabled VLAN (20 in this example).</p>	
<p>8. Create access rule for wired and wireless authentication. In this example, the rule permits all traffic.</p>	<p>For wired profile:</p> <pre>(Instant AP) (config) # wlan access-rule wired-port (Instant AP) (Access Rule "wired-port") # rule any any match any any any permit</pre> <p>For WLAN SSID:</p> <pre>(Instant AP) (config) # wlan access-rule guest (Instant AP) (Access Rule "guest") # rule any any match any any any permit</pre>	<p>See Configuring ACL Rules for Network Services</p>
<p>NOTE: Ensure that you execute the commit apply command in the AOS-W Instant CLI before saving the configuration and propagating changes across the OAW-IAP cluster.</p>		

OAW-IAP-Connected Switch Configuration

Client VLANs defined in this example must be opened on the upstream switches in multiple OAW-IAP deployments, as client traffic from the slave to the master is tagged with the client VLAN.

Datacenter Configuration

For information on switch configuration, see [Configuring a Switch for IAP-VPN Operations on page 245](#). Ensure that the upstream router is configured with a static route pointing to the switch for the L3 VLAN.

Scenario 3—IPsec: Multiple Datacenter Deployment with Primary and Backup Switches for Redundancy

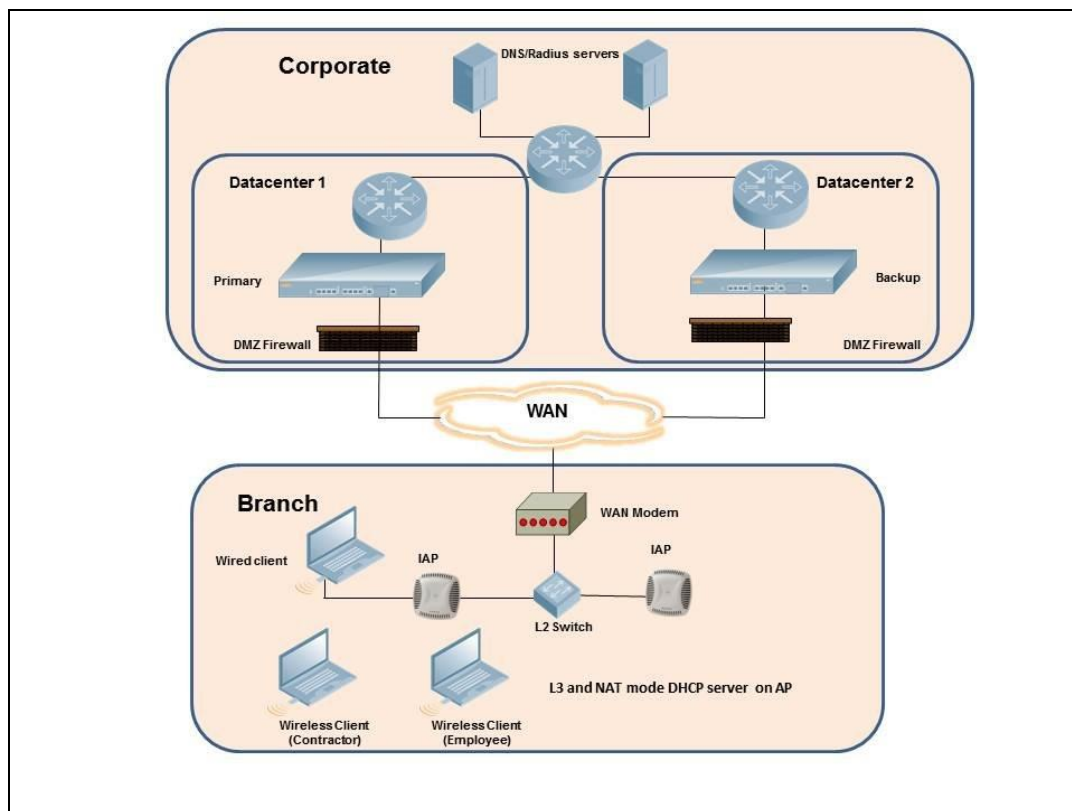
This scenario includes the following configuration elements:

- Multiple switch deployment model with switches in different data centers operating as primary/backup VPN with **Fast Failover** and preemption enabled.
- Split-tunneling of traffic.
- Split-tunneling of client DNS traffic.
- Two Distributed, L3 mode DHCPs, one each for employee and contractors; and one Local mode DHCP server.
- RADIUS server within corporate network and authentication survivability enabled for branch survivability.
- Wired and wireless users in L3 and NAT modes, respectively.
- Access rules for wired and wireless users with source-NAT-based rule for contractor roles to bypass global routing profile.
- OSPF based route propagation on switch.

Topology

Figure 122 shows the topology and the IP addressing scheme used in this scenario.

Figure 122 Scenario 3—IPsec: Multiple Datacenter Deployment with Primary and Backup Switches for Redundancy



The IP addressing scheme used in this example is as follows:

- 10.0.0.0/8 is the corporate network.
- 10.30.0.0/16 subnet is reserved for L3 mode –used by Employee SSID.

- 10.40.0.0/16 subnet is reserved for L3 mode –used by Contractor SSID.
- 172.16.20.0/24 subnet is used for NAT mode – used for wired network.
- Client count in each branch is 200.
- Contractors are only permitted to reach 10.16.0.0/16 network.

OAW-IAP Configuration

This section provides information on configuration steps performed through the CLI and the UI.

Table 86: OAW-IAP Configuration for Scenario 3—IPsec: Multiple Datacenter Deployment

Configuration Steps	CLI Commands	UI Procedure
1. Configure the primary IP address. This IP address is the Public IP address of the switch. Fast Failover is enabled for fast convergence.	<pre>(Instant AP) (config)# vpn primary <public IP of primary switch> (Instant AP) (config)# vpn backup <public IP of backup switches> (Instant AP) (config)# vpn preemption (Instant AP) (config)# vpn fast-failover</pre>	See Configuring an IPsec Tunnel
2. Configure routing profiles to tunnel traffic through IPsec.	<pre>(Instant AP) (config)# routing-profile (Instant AP) (routing-profile)# route 0.0.0.0 0.0.0.0 <public IP of primary switch> (Instant AP) (routing-profile)# route 10.0.0.0 255.0.0.0 <public IP of backup switch></pre>	See Configuring Routing Profiles
3. Configure Enterprise DNS for split DNS. The example in the next column uses a specific enterprise domain to tunnel all DNS queries matching that domain to corporate.	<pre>(Instant AP) (config)# internal-domains (Instant AP) (domains)# domain-name corpdomain.com</pre>	See Configuring Enterprise Domains
4. Configure Distributed, L3 DHCP profiles with VLAN 30 and VLAN 40.	<p>Distributed, L3 profile with VLAN 30</p> <pre>(Instant AP) (config)# ip dhcp l3-dhcp (Instant AP) (DHCP profile "l3-dhcp")# server-type Distributed,L3 (Instant AP) (DHCP profile "l3-dhcp")# server-vlan 30 (Instant AP) (DHCP profile "l3-dhcp")# ip-range 10.30.0.0 10.30.255.255 (Instant AP) (DHCP profile "l3-dhcp")# dns-server 10.1.1.50,10.1.1.30 (Instant AP) (DHCP profile "l3-dhcp")# domain-name corpdomain.com (Instant AP) (DHCP profile "l3-dhcp")# client-count 200</pre> <p>Distributed, L3 profile with VLAN 40</p> <pre>(Instant AP) (config)# ip dhcp l3-dhcp (Instant AP) (DHCP profile "l3-dhcp")# server-type Distributed,L3 (Instant AP) (DHCP profile "l3-dhcp")# server-vlan 40 (Instant AP) (DHCP profile "l3-dhcp")# ip-range 10.40.0.0 10.40.255.255 (Instant AP) (DHCP profile "l3-dhcp")# dns-server 10.1.1.50,10.1.1.30</pre>	See Configuring Distributed DHCP Scopes and Configuring Local DHCP Scopes

Table 86: OAW-IAP Configuration for Scenario 3—IPsec: Multiple Datacenter Deployment

Configuration Steps	CLI Commands	UI Procedure
	<pre>(Instant AP) (DHCP profile "l3-dhcp")# domain-name corpdomain.com (Instant AP) (DHCP profile "l3-dhcp")# client-count 200</pre> <p>Local profile with VLAN 20</p> <pre>(Instant AP) (config)# ip dhcp local (Instant AP) (DHCP profile "local")# server-type Local (Instant AP) (DHCP profile "local")# server-vlan 20 (Instant AP) (DHCP profile "local")# subnet 172.16.20.1 (Instant AP) (DHCP profile "local")# subnet-mask 255.255.255.0 (Instant AP) (DHCP profile "local")# lease-time 86400 (Instant AP) (DHCP profile "local")# dns-server 10.1.1.30,10.1.1.50 (Instant AP) (DHCP profile "local")# domain-name arubanetworks.com</pre> <p>NOTE: The IP range configuration on each branch will be the same. Each OAW-IAP will derive a smaller subnet based on the client count scope using the Branch ID (BID) allocated by the switch.</p>	
<p>5. Create authentication servers for user authentication. The example in the next column assumes 802.1X SSID.</p>	<pre>(Instant AP) (config)# wlan auth-server server1 (Instant AP) (Auth Server "server1")# ip 10.2.2.1 (Instant AP) (Auth Server "server1")# port 1812 (Instant AP) (Auth Server "server1")# acctport 1813 (Instant AP) (Auth Server "server1")# key "presharedkey" (Instant AP) (Auth Server "server1")# exit</pre> <pre>(Instant AP) (config)# wlan auth-server server2 (Instant AP) (Auth Server "server1")# ip 10.2.2.2 (Instant AP) (Auth Server "server1")# port 1812 (Instant AP) (Auth Server "server1")# acctport 1813 (Instant AP) (Auth Server "server1")# key "presharedkey"</pre>	<p>See Configuring an External Server for Authentication</p>
<p>6. Configure wired port and wireless SSIDs using the authentication servers and access rules; enable authentication survivability.</p>	<p>Configure wired ports to operate in NAT mode and associate VLAN 20 to the wired port profile.</p> <pre>(Instant AP) (config) # wired-port-profile wired-port (Instant AP) (wired-port-profile "wired-port")# switchport-mode access (Instant AP) (wired-port-profile "wired-port")# allowed-vlan all (Instant AP) (wired-port-profile "wired-port")# native-vlan 20 (Instant AP) (wired-port-profile "wired-port")# no shutdown (Instant AP) (wired-port-profile "wired-port")# access-rule-name wired-port (Instant AP) (wired-port-profile "wired-port")# type employee</pre>	<p>See Configuring a Wired Profile and Wireless Network Profiles</p>

Table 86: OAW-IAP Configuration for Scenario 3—IPsec: Multiple Datacenter Deployment

Configuration Steps	CLI Commands	UI Procedure
	<pre>(Instant AP) (wired-port-profile "wired-port")# auth-server server1 (Instant AP) (wired-port-profile "wired-port")# auth-server server2 (Instant AP) (wired-port-profile "wired-port")# dot1x (Instant AP) (wired-port-profile "wired-port")# exit (Instant AP) (config)# enet1-port-profile wired-port</pre> <p>Configure a wireless SSID to operate in L3 mode for employee and associate Distributed, L3 mode VLAN 30 to the WLAN SSID profile.</p> <pre>(Instant AP) (config) # wlan ssid-profile wireless-ssid (Instant AP) (SSID Profile "wireless-ssid")# enable (Instant AP) (SSID Profile "wireless-ssid")# type employee (Instant AP) (SSID Profile "wireless-ssid")# essid wireless-ssid (Instant AP) (SSID Profile "wireless-ssid")# opmode wpa2-aes (Instant AP) (SSID Profile "wireless-ssid")# vlan 30 (Instant AP) (SSID Profile "wireless-ssid")# auth-server server1 (Instant AP) (SSID Profile "wireless-ssid")# auth-server server2 (Instant AP) (SSID Profile "wireless-ssid")# auth-survivability</pre> <p>Configure a wireless SSID to operate in L3 mode for contractor and associate Distributed, L3 mode VLAN 40 to the WLAN SSID profile.</p> <pre>(Instant AP) (config) # wlan ssid-profile wireless-ssid-contractor (Instant AP) (SSID Profile "wireless-ssid-contractor")# enable (Instant AP) (SSID Profile "wireless-ssid-contractor")# type contractor (Instant AP) (SSID Profile "wireless-ssid-contractor")# essid wireless-ssid-contractor (Instant AP) (SSID Profile "wireless-ssid-contractor")# opmode wpa2-aes (Instant AP) (SSID Profile "wireless-ssid-contractor")# vlan 40 (Instant AP) (SSID Profile "wireless-ssid-contractor")# auth-server server1 (Instant AP) (SSID Profile "wireless-ssid-contractor")# auth-server server2 (Instant AP) (SSID Profile "wireless-ssid-contractor")# auth-survivability</pre>	
<p>7. Create access rule for wired and wireless authentication. In this example, the rule</p>	<p>For wired profile:</p> <pre>(Instant AP) (config)# wlan access-rule wired-port (Instant AP) (Access Rule "wired-port")# rule any any match any any permit</pre>	<p>See Configuring ACL Rules for Network</p>

Table 86: OAW-IAP Configuration for Scenario 3—IPsec: Multiple Datacenter Deployment

Configuration Steps	CLI Commands	UI Procedure
permits all traffic. For contractor SSID role, the rule allows only 10.16.0.0/16 network and all other traffic address is translated at the source and the global routing profile definition is bypassed.	<p>For WLAN SSID employee roles:</p> <pre>(Instant AP) (config) # wlan access-rule wireless-ssid (Instant AP) (Access Rule "wireless-ssid") # rule any any match any any any permit</pre> <p>For WLAN SSID contractor roles:</p> <pre>(Instant AP) (config) # wlan access-rule wireless-ssid-contractor (Instant AP) (Access Rule "wireless-ssid-contractor") # rule 10.16.0.0 255.255.0.0 match any any any permit (Instant AP) (Access Rule "wireless-ssid-contractor") # rule any any match any any any src-nat</pre>	Services
<p>NOTE: Ensure that you execute the commit apply command in the AOS-W Instant CLI before saving the configuration and propagating changes across the OAW-IAP cluster.</p>		

OAW-IAP-Connected Switch Configuration

Client VLANs defined in this example must be opened on the upstream switches in multiple OAW-IAP deployments, as client traffic from the slave to the master is tagged with the client VLAN.

Datacenter Configuration

For information on switch configuration, see [Configuring a Switch for IAP-VPN Operations on page 245](#).

The following OSPF configuration is required on the switch to redistribute IAP-VPN routes to upstream routers:

```
(host) (config) # router ospf
(host) (config) # router ospf router-id <ID>
(host) (config) # router ospf area 0.0.0.0
(host) (config) # router ospf redistribute rapng-vpn
```


Scenario 4—GRE: Single Datacenter Deployment with No Redundancy

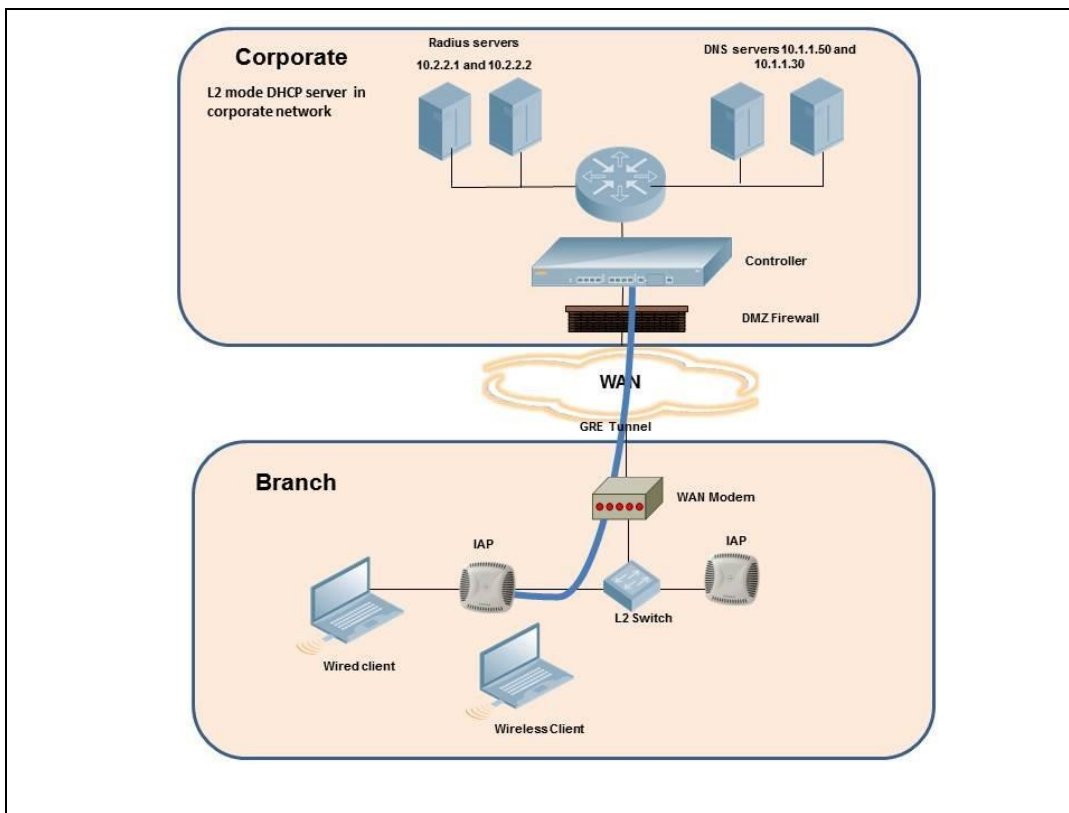
This scenario includes the following configuration elements:

- Single VPN primary configuration using GRE
 - **Aruba GRE**, does not require any configuration on the Alcatel-Lucent OmniAccess WLAN Switch that acts as a GRE endpoint.
 - **Manual GRE**, which requires GRE tunnels to be explicitly configured on the GRE endpoint that can be an Alcatel-Lucent OmniAccess WLAN Switch or any device that supports GRE termination.
- Tunneling of all traffic to datacenter
- Centralized, L2 mode DHCP profile
- RADIUS server within corporate network and authentication survivability for branch survivability.
- Wired and wireless users in L2 mode
- Access rules defined for wired and wireless networks to permit all traffic

Topology

Figure 123 shows the topology and the IP addressing scheme used in this scenario:

Figure 123 Scenario 4—GRE: Single Datacenter Deployment with No Redundancy



The following IP addresses are used in the examples for this scenario:

- 10.0.0.0/8 is the corporate network.
- 10.20.0.0/16 subnet is reserved for L2 mode.

OAW-IAP Configuration

This section provides information on configuration steps performed by using the CLI and the UI.

Table 87: OAW-IAP Configuration for Scenario—GRE: Single Datacenter Deployment with No Redundancy

Configuration Steps	CLI Commands	UI Procedure
<p>1. Configure Aruba GRE or manual GRE</p> <ul style="list-style-type: none"> Aruba GRE uses an IPsec tunnel to facilitate switch configuration and requires VPN to be configured. This VPN tunnel is not used for any client traffic. Manual GRE uses standard GRE tunnel configuration and requires switch configuration to complete the GRE tunnel. 	<p>Aruba GRE configuration</p> <pre>(Instant AP) (config)# vpn primary <switch-IP> (Instant AP) (config)# vpn gre-outside</pre> <p>Manual GRE configuration</p> <pre>(Instant AP) (config)# gre primary <switch-IP> (Instant AP) (config)# gre type 80</pre> <p>Per-AP GRE tunnel configuration</p> <p>Optionally, per-AP GRE tunnel can also be enabled, which causes each OAW-IAP to form an independent GRE tunnel to the GRE end-point. Aruba GRE requires each OAW-IAP MAC to be present in the switch whitelist. Manual GRE requires GRE configuration for the IP of each OAW-IAP on the switch.</p> <pre>(Instant AP) (config)# gre per-ap-tunnel</pre> <p>NOTE: Starting with AOS-W Instant 6.5.1.0-4.3.1.0, if VC IP is configured and per-AP GRE tunnel is disabled, OAW-IAP uses VC IP as the GRE source IP. For Manual GRE, this simplifies configuration on switch, since only the VC IP destined GRE tunnel interface configuration is required.</p>	<p>See Configuring Aruba GRE Parameters and Configuring Manual GRE Parameters</p>
<p>2. Configure routing profiles to tunnel traffic through GRE.</p>	<pre>(Instant AP) (config)# routing-profile (Instant AP) (routing-profile)# route 0.0.0.0 0.0.0.0 <IP of GRE-endpoint></pre>	<p>See Configuring Routing Profiles</p>
<p>3. Configure Enterprise DNS. The example in the next column tunnels all DNS queries to the client's original DNS server without proxying on OAW-IAP.</p>	<pre>(Instant AP) (config)# internal-domains (Instant AP) (domains)# domain-name *</pre>	<p>See Configuring Enterprise Domains</p>
<p>4. Configure Centralized, L2 DHCP profile with VLAN 20.</p>	<p>Centralized, L2 DHCP profile VLAN 20</p> <pre>(Instant AP) (config)# ip dhcp l2-dhcp (Instant AP) (DHCP profile "l2-dhcp")# server-type Centralized,L2 (Instant AP) (DHCP profile "l2-dhcp")# server-vlan 20</pre>	<p>See Configuring Centralized DHCP Scopes</p>

Table 87: OAW-IAP Configuration for Scenario—GRE: Single Datacenter Deployment with No Redundancy

Configuration Steps	CLI Commands	UI Procedure
<p>5. Create authentication servers for user authentication. The example in the next column assumes 802.1X SSID.</p>	<pre>(Instant AP) (config)# wlan auth-server server1 (Instant AP) (Auth Server "server1")# ip 10.2.2.1 (Instant AP) (Auth Server "server1")# port 1812 (Instant AP) (Auth Server "server1")# acctport 1813 (Instant AP) (Auth Server "server1")# key "presharedkey" (Instant AP) (Auth Server "server1")# exit (Instant AP) (config)# wlan auth-server server2 (Instant AP) (Auth Server "server1")# ip 10.2.2.2 (Instant AP) (Auth Server "server1")# port 1812 (Instant AP) (Auth Server "server1")# acctport 1813 (Instant AP) (Auth Server "server1")# key "presharedkey"</pre>	<p>See Configuring an External Server for Authentication</p>
<p>6. Configure wired and wireless SSIDs using the authentication servers and access rules; enable authentication survivability.</p>	<p>Configure wired ports to operate in Centralized, L2 mode and associate VLAN 20 to the wired port profile.</p> <pre>(Instant AP) (config) # wired-port-profile wired-port (Instant AP) (wired-port-profile "wired-port")# switchport-mode access (Instant AP) (wired-port-profile "wired-port")# allowed-vlan all (Instant AP) (wired-port-profile "wired-port")# native-vlan 20 (Instant AP) (wired-port-profile "wired-port")# no shutdown (Instant AP) (wired-port-profile "wired-port")# access-rule-name wired-port (Instant AP) (wired-port-profile "wired-port")# type employee (Instant AP) (wired-port-profile "wired-port")# auth-server server1 (Instant AP) (wired-port-profile "wired-port")# auth-server server2 (Instant AP) (wired-port-profile "wired-port")# dot1x (Instant AP) (wired-port-profile "wired-port")# exit (Instant AP) (config)# enet1-port-profile wired-port</pre> <p>Configure a wireless SSID to operate in Centralized, L2 mode and associate VLAN 20 to the WLAN SSID profile.</p> <pre>(Instant AP) (config) # wlan ssid-profile wireless-ssid (Instant AP) (SSID Profile "wireless-ssid")# enable (Instant AP) (SSID Profile "wireless-ssid")# type employee (Instant AP) (SSID Profile "wireless-ssid")# essid wireless-ssid (Instant AP) (SSID Profile "wireless-ssid")# opmode wpa2-aes (Instant AP) (SSID Profile "wireless-ssid")# vlan 20 (Instant AP) (SSID Profile "wireless-ssid")# auth- server server1 (Instant AP) (SSID Profile "wireless-ssid")# auth- server server2</pre>	<p>See Configuring a Wired Profile and Wireless Network Profiles</p>

Table 87: OAW-IAP Configuration for Scenario—GRE: Single Datacenter Deployment with No Redundancy

Configuration Steps	CLI Commands	UI Procedure
	(Instant AP) (SSID Profile "wireless-ssid") # auth-survivability	
7. Create access rule for wired and wireless authentication.	<p>For wired profile:</p> <pre>(Instant AP) (config) # wlan access-rule wired-port (Instant AP) (Access Rule "wired-port") # rule any any match any any any permit</pre> <p>For WLAN SSID employee roles:</p> <pre>(Instant AP) (config) # wlan access-rule wireless-ssid (Instant AP) (Access Rule "wireless-ssid") # rule any any match any any any permit</pre>	See Configuring ACL Rules for Network Services
<p>NOTE: Ensure that you execute the commit apply command in the AOS-W Instant CLI before saving the configuration and propagating changes across the OAW-IAP cluster.</p>		

OAW-IAP-Connected Switch Configuration

Client VLANs defined in this example must be opened on the upstream switches in multiple OAW-IAP deployments, as client traffic from the slave to the master is tagged with the client VLAN.

Datacenter Configuration

For information on switch configuration, see [Configuring a Switch for IAP-VPN Operations on page 245](#).

The following GRE configuration is required on the switch:

```
(host) (config) # interface tunnel <Number>
(host) (config-tunnel) # description <Description>
(host) (config-tunnel) # tunnel mode gre <ID>
(host) (config-tunnel) # tunnel source <switch-IP>
(host) (config-tunnel) # tunnel destination <AP-IP>
(host) (config-tunnel) # trusted
(host) (config-tunnel) # tunnel vlan <allowed-VLAN>
```

Glossary

The following table lists the terms and their definitions used in this document.

Table 88: List of Terms

Term	Definition
802.11	An evolving family of specifications for wireless LANs developed by a working group of the Institute of Electrical and Electronics Engineers (IEEE). 802.11 standards use the Ethernet protocol and CSMA/CA (carrier sense multiple access with collision avoidance) for path sharing.
802.11a	Provides specifications for wireless systems. Networks using 802.11a operate at radio frequencies in the 5GHz band. The specification uses a modulation scheme known as orthogonal frequency-division multiplexing (OFDM) that is especially well suited to use in office settings. The maximum data transfer rate is 54 Mbps.
802.11b	WLAN standard often called Wi-Fi; backward compatible with 802.11. Instead of the phase-shift keying (PSK) modulation method historically used in 802.11 standards, 802.11b uses complementary code keying (CCK), which allows higher data speeds and is less susceptible to multipath-propagation interference. 802.11b operates in the 2.4 GHz band and the maximum data transfer rate is 11 Mbps.
802.11g	Offers transmission over relatively short distances at up to 54 Mbps, compared with the 11 Mbps theoretical maximum of 802.11b. 802.11g operates in the 2.4 GHz band and employs orthogonal frequency division multiplexing (OFDM), the modulation scheme used in 802.11a, to obtain higher data speed. Computers or terminals set up for 802.11g can fall back to speeds of 11 Mbps, so that 802.11b and 802.11g devices can be compatible within a single network.
802.11n	Wireless networking standard to improve network throughput over the two previous standards 802.11a and 802.11g with a significant increase in the maximum raw data rate from 54 Mbps to 600 Mbps with the use of four spatial streams at a channel width of 40 MHz. 802.11n operates in the 2.4 and 5.0 bands.
AP	An access point (AP) connects users to other users within the network and also can serve as the point of interconnection between the WLAN and a fixed wire network. The number of access points a WLAN needs is determined by the number of users and the size of the network.
access point mapping	The act of locating and possibly exploiting connections to WLANs while driving around a city or elsewhere. To do war driving, you need a vehicle, a computer (which can be a laptop), a wireless Ethernet card set to work in promiscuous mode, and some kind of an antenna which can be mounted on top of or positioned inside the car. Because a WLAN may have a range that extends beyond an office building, an outside user may be able to intrude into the network, obtain a free Internet connection, and possibly gain access to company records and other resources.

Table 88: List of Terms

Term	Definition
ad-hoc network	A LAN or other small network, especially one with wireless or temporary plug-in connections, in which some of the network devices are part of the network only for the duration of a communications session or, in the case of mobile or portable devices, while in some close proximity to the rest of the network.
band	A specified range of frequencies of electromagnetic radiation.
DHCP	The Dynamic Host Configuration Protocol (DHCP) is an auto-configuration protocol used on IP networks. Computers or any network peripherals that are connected to IP networks must be configured, before they can communicate with other computers on the network. DHCP allows a computer to be configured automatically, eliminating the need for a network administrator. DHCP also provides a central database to keep track of computers connected to the network. This database helps in preventing any two computers from being configured with the same IP address.
DNS Server	<p>A Domain Name System (DNS) server functions as a phonebook for the Internet and Internet users. It converts human readable computer hostnames into IP addresses and vice-versa.</p> <p>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.</p>
DST	Daylight saving time (DST), also known as summer time, is the practice of advancing clocks, so that evenings have more daylight and mornings have less. Typically clocks are adjusted forward one hour near the start of spring and are adjusted backward in autumn.
EAP	Extensible authentication protocol (EAP) refers to the authentication protocol in wireless networks that expands on methods used by the point-to-point protocol (PPP), a protocol often used when connecting a computer to the Internet. EAP can support multiple authentication mechanisms, such as token cards, smart cards, certificates, one-time passwords, and public key encryption authentication.
fixed wireless	Wireless devices or systems in fixed locations such as homes and offices. Fixed wireless devices usually derive their electrical power from the utility mains, unlike mobile wireless or portable wireless which tend to be battery-powered. Although mobile and portable systems can be used in fixed locations, efficiency and bandwidth are compromised compared with fixed systems.
frequency allocation	Use of radio frequency spectrum regulated by governments.
frequency spectrum	Part of the electromagnetic spectrum.

Table 88: *List of Terms*

Term	Definition
hotspot	A WLAN node that provides Internet connection and virtual private network (VPN) access from a given location. A business traveler, for example, with a laptop equipped for Wi-Fi can look up a local hot spot, contact it, and get connected through its network to reach the Internet and their own company remotely with a secure connection. Increasingly, public places, such as airports, hotels, and coffee shops are providing free wireless access for customers.
IEEE 802.11 standards	The IEEE 802.11 is a set of standards that are categorized based on the radio wave frequency and the data transfer rate.
POE	<p>Power over Ethernet (PoE) is a method of delivering power on the same physical Ethernet wire used for data communication. Power for devices is provided in one of the following two ways:</p> <ul style="list-style-type: none">• Endspan— The switch that an AP is connected for power supply.• Midspan— A device can sit between the switch and APs <p>The choice of endspan or midspan depends on the capabilities of the switch to which the OAW-IAP is connected. Typically if a switch is in place and does not support PoE, midspan power injectors are used.</p>
PPPoE	Point-to-Point Protocol over Ethernet (PPPoE) is a method of connecting to the Internet typically used with DSL services where the client connects to the DSL modem.
QoS	Quality of Service (QoS) refers to the capability of a network to provide better service to a specific network traffic over various technologies.
RF	Radio Frequency (RF) refers to the portion of electromagnetic spectrum in which electromagnetic waves are generated by feeding alternating current to an antenna.
TACACS	Family of protocols that handle remote authentication and related services for network access control through a centralized server.
TACACS+	Derived from TACACS but an entirely new and separate protocol to handle AAA services. TACACS+ uses TCP and is not compatible with TACACS. Because it encrypts password, username, authorization, and accounting, it is less vulnerable than RADIUS.
VPN	A Virtual Private Network (VPN) network that uses a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network. A VPN ensures privacy through security procedures and tunneling protocols such as the Layer Two Tunneling Protocol (L2TP). Data is encrypted at the sending end and decrypted at the receiving end.

Table 88: List of Terms

Term	Definition
W-CDMA	Officially known as IMT-2000 direct spread; ITU standard derived from Code-Division Multiple Access (CDMA). Wideband code-division multiple access (W-CDMA) is a third-generation (3G) mobile wireless technology that promises much higher data speeds to mobile and portable wireless devices than commonly offered in today's market.
Wi-Fi	A term for certain types of WLANs. Wi-Fi can apply to products that use any 802.11 standard. Wi-Fi has gained acceptance in many businesses, agencies, schools, and homes as an alternative to a wired LAN. Many airports, hotels, and fast-food facilities offer public access to Wi-Fi networks.
WEP	Wired equivalent privacy (WEP) is a security protocol specified in 802.11b, designed to provide a WLAN with a level of security and privacy comparable to what is usually expected of a wired LAN. Data encryption protects the vulnerable wireless link between clients and access points; once this measure has been taken, other typical LAN security mechanisms such as password protection, end-to-end encryption, virtual private networks (VPNs), and authentication can be put in place to ensure privacy.
wireless	Describes telecommunications in which electromagnetic waves (rather than some form of wire) carry the signal over part or all of the communication path.
wireless network	In a Wireless LAN (WLAN), laptops, desktops, PDAs, and other computer peripherals are connected to each other without any network cables. These network elements or clients use radio signals to communicate with each other. Wireless networks are set up based on the IEEE 802.11 standards.
WISP	Wireless ISP (WISP) refers to an internet service provider (ISP) that allows subscribers to connect to a server at designated hot spots (access points) using a wireless connection such as Wi-Fi. This type of ISP offers broadband service and allows subscriber computers, called stations, to access the Internet and the web from anywhere within the zone of coverage provided by the server antenna, usually a region with a radius of several kilometers.
wireless service provider	A company that offers transmission services to users of wireless devices through radio frequency (RF) signals rather than through end-to-end wire communication.
WLAN	Wireless local area network (WLAN) is a local area network (LAN) that the users access through a wireless connection.

The following table lists the acronyms and abbreviations used in Aruba documents.

Table 89: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
3G	Third Generation of Wireless Mobile Telecommunications Technology
4G	Fourth Generation of Wireless Mobile Telecommunications Technology
AAA	Authentication, Authorization, and Accounting
ABR	Area Border Router
AC	Access Category
ACC	Advanced Cellular Coexistence
ACE	Access Control Entry
ACI	Adjacent Channel interference
ACL	Access Control List
AD	Active Directory
ADO	Active X Data Objects
ADP	Aruba Discovery Protocol
AES	Advanced Encryption Standard
AIFSN	Arbitrary Inter-frame Space Number
ALE	Analytics and Location Engine
ALG	Application Layer Gateway
AM	Air Monitor
AMON	Advanced Monitoring
AMP	AirWave Management Platform
A-MPDU	Aggregate MAC Protocol Data Unit
A-MSDU	Aggregate MAC Service Data Unit
ANQP	Access Network Query Protocol

Table 89: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
ANSI	American National Standards Institute
AP	Access Point
API	Application Programming Interface
ARM	Adaptive Radio Management
ARP	Address Resolution Protocol
AVF	AntiVirus Firewall
BCMC	Broadcast-Multicast
BGP	Border Gateway protocol
BLE	Bluetooth Low Energy
BMC	Beacon Management Console
BPDU	Bridge Protocol Data Unit
BRAS	Broadband Remote Access Server
BRE	Basic Regular Expression
BSS	Basic Service Set
BSSID	Basic Service Set Identifier
BYOD	Bring Your Own Device
CA	Certification Authority
CAC	Call Admission Control
CALEA	Communications Assistance for Law Enforcement Act
CAP	Campus AP
CCA	Clear Channel Assessment
CDP	Cisco Discovery Protocol
CDR	Call Detail Records
CEF	Common Event Format
CGI	Common Gateway Interface

Table 89: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
CHAP	Challenge Handshake Authentication Protocol
CIDR	Classless Inter-Domain Routing
CLI	Command-Line Interface
CN	Common Name
CoA	Change of Authorization
CoS	Class of Service
CPE	Customer Premises Equipment
CPsec	Control Plane Security
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
CRL	Certificate Revocation List
CSA	Channel Switch Announcement
CSMA/CA	Carrier Sense Multiple Access / Collision Avoidance
CSR	Certificate Signing Request
CSV	Comma Separated Values
CTS	Clear to Send
CW	Contention Window
DAS	Distributed Antenna System
dB	Decibel
dBm	Decibel Milliwatt
DCB	Data Center Bridging
DCE	Data Communication Equipment
DCF	Distributed Coordination Function
DDMO	Distributed Dynamic Multicast Optimization
DES	Data Encryption Standard

Table 89: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
DFS	Dynamic Frequency Selection
DFT	Discreet Fourier Transform
DHCP	Dynamic Host Configuration Protocol
DLNA	Digital Living Network Alliance
DMO	Dynamic Multicast optimization
DN	Distinguished Name
DNS	Domain Name System
DOCSIS	Data over Cable Service Interface Specification
DoS	Denial of Service
DPD	Dead Peer Detection
DPI	Deep Packet Inspection
DR	Designated Router
DRT	Downloadable Regulatory Table
DS	Differentiated Services
DSCP	Differentiated Services Code Point
DSSS	Direct Sequence Spread Spectrum
DST	Daylight Saving Time
DTE	Data Terminal Equipment
DTIM	Delivery Traffic Indication Message
DTLS	Datagram Transport Layer Security
DU	Data Unit
EAP	Extensible Authentication Protocol
EAP-FAST	EAP-Flexible Authentication Secure Tunnel
EAP-GTC	EAP-Generic Token Card
EAP-MD5	EAP-Method Digest 5

Table 89: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
EAP-MSCHAP EAP-MSCHAPv2	EAP-Microsoft Challenge Handshake Authentication Protocol
EAPoL	EAP over LAN
EAPoUDP	EAP over UDP
EAP-PEAP	EAP-Protected EAP
EAP-PWD	EAP-Password
EAP-TLS	EAP-Transport Layer Security
EAP-TTLS	EAP-Tunneled Transport Layer Security
ECC	Elliptical Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
EIGRP	Enhanced Interior Gateway Routing Protocol
EIRP	Effective Isotropic Radiated Power
EMM	Enterprise Mobility Management
ESI	External Services Interface
ESS	Extended Service Set
ESSID	Extended Service Set Identifier
EULA	End User License Agreement
FCC	Federal Communications Commission
FFT	Fast Fourier Transform
FHSS	Frequency Hopping Spread Spectrum
FIB	Forwarding Information Base
FIPS	Federal Information Processing Standards
FQDN	Fully Qualified Domain Name
FQLN	Fully Qualified Location Name
FRER	Frame Receive Error Rate

Table 89: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
FRR	Frame Retry Rate
FSPL	Free Space Path Loss
FTP	File Transfer Protocol
GBps	Gigabytes per second
Gbps	Gigabits per second
GHz	Gigahertz
GIS	Generic Interface Specification
GMT	Greenwich Mean Time
GPP	Guest Provisioning Page
GPS	Global Positioning System
GRE	Generic Routing Encapsulation
GUI	Graphical User Interface
GVRP	GARP or Generic VLAN Registration Protocol
H2QP	Hotspot 2.0 Query Protocol
HA	High Availability
HMD	High Mobility Device
HSPA	High-Speed Packet Access
HT	High Throughput
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IAS	Internet Authentication Service
ICMP	Internet Control Message Protocol
IdP	Identity Provider
IDS	Intrusion Detection System
IE	Information Element

Table 89: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
IEEE	Institute of Electrical and Electronics Engineers
IGMP	Internet Group Management Protocol
IGP	Interior Gateway Protocol
IGRP	Interior Gateway Routing Protocol
IKE PSK	Internet Key Exchange Pre-shared Key
IoT	Internet of Things
IP	Internet Protocol
IPM	Intelligent Power Monitoring
IPS	Intrusion Prevention System
IPsec	IP Security
ISAKMP	Internet Security Association and Key Management Protocol
ISP	Internet Service Provider
JSON	JavaScript Object Notation
KBps	Kilobytes per second
Kbps	Kilobits per second
L2TP	Layer-2 Tunneling Protocol
LACP	Link Aggregation Control Protocol
LAG	Link Aggregation Group
LAN	Local Area Network
LCD	Liquid Crystal Display
LDAP	Lightweight Directory Access Protocol
LDPC	Low-Density Parity-Check
LEA	Law Enforcement Agency
LEAP	Lightweight Extensible Authentication Protocol
LED	Light Emitting Diode

Table 89: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
LEEF	Long Event Extended Format
LI	Lawful Interception
LLDP	Link Layer Discovery Protocol
LLDP-MED	LLDP–Media Endpoint Discovery
LMS	Local Management Switch
LNS	L2TP Network Server
LTE	Long Term Evolution
MAB	MAC Authentication Bypass
MAC	Media Access Control
MAM	Mobile Application Management
MBps	Megabytes per second
Mbps	Megabits per second
MCS	Modulation and Coding Scheme
MD5	Message Digest 5
MDM	Mobile Device Management
mDNS	Multicast Domain Name System
MFA	Multi-factor Authentication
MHz	Megahertz
MIB	Management Information Base
MIMO	Multiple-Input Multiple-Output
MLD	Multicast Listener Discovery
MPDU	MAC Protocol Data Unit
MPLS	Multiprotocol Label Switching
MPPE	Microsoft Point-to-Point Encryption
MSCHAP	Microsoft Challenge Handshake Authentication Protocol

Table 89: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
MSS	Maximum Segment Size
MSSID	Mesh Service Set Identifier
MSTP	Multiple Spanning Tree Protocol
MTU	Maximum Transmission Unit
MU-MIMO	Multi-User Multiple-Input Multiple-Output
MVRP	Multiple VLAN Registration Protocol
NAC	Network Access Control
NAD	Network Access Device
NAK	Negative Acknowledgment Code
NAP	Network Access Protection
NAS	Network Access Server Network-attached Storage
NAT	Network Address Translation
NetBIOS	Network Basic Input/Output System
NIC	Network Interface Card
Nmap	Network Mapper
NMI	Non-Maskable Interrupt
NMS	Network Management Server
NOE	New Office Environment
NTP	Network Time Protocol
OAuth	Open Authentication
OCSP	Online Certificate Status Protocol
OFA	OpenFlow Agent
OFDM	Orthogonal Frequency Division Multiplexing
OID	Object Identifier

Table 89: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
OKC	Opportunistic Key Caching
OS	Operating System
OSPF	Open Shortest Path First
OUI	Organizationally Unique Identifier
OVA	Open Virtual Appliance
OVF	Open Virtualization Format
PAC	Protected Access Credential
PAP	Password Authentication Protocol
PAPI	Proprietary Access Protocol Interface
PCI	Peripheral Component Interconnect
PDU	Power Distribution Unit
PEAP	Protected Extensible Authentication Protocol
PEAP-GTC	Protected Extensible Authentication Protocol-Generic Token Card
PEF	Policy Enforcement Firewall
PFS	Perfect Forward Secrecy
PHB	Per-hop behavior
PIM	Protocol-Independent Multicast
PIN	Personal Identification Number
PKCS	Public Key Cryptography Standard
PKI	Public Key Infrastructure
PLMN	Public Land Mobile Network
PMK	Pairwise Master Key
PoE	Power over Ethernet
POST	Power On Self Test
PPP	Point-to-Point Protocol

Table 89: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
PPPoE	PPP over Ethernet
PPTP	PPP Tunneling Protocol
PRNG	Pseudo-Random Number Generator
PSK	Pre-Shared Key
PSU	Power Supply Unit
PVST	Per VLAN Spanning Tree
QoS	Quality of Service
RA	Router Advertisement
RADAR	Radio Detection and Ranging
RADIUS	Remote Authentication Dial-In User Service
RAM	Random Access Memory
RAP	Remote AP
RAPIDS	Rogue Access Point and Intrusion Detection System
RARP	Reverse ARP
REGEX	Regular Expression
REST	Representational State Transfer
RF	Radio Frequency
RFC	Request for Comments
RFID	Radio Frequency Identification
RIP	Routing Information Protocol
RRD	Round Robin Database
RSA	Rivest, Shamir, Adleman
RSSI	Received Signal Strength Indicator
RSTP	Rapid Spanning Tree Protocol
RTCP	RTP Control Protocol

Table 89: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
RTLS	Real-Time Location Systems
RTP	Real-Time Transport Protocol
RTS	Request to Send
RTSP	Real Time Streaming Protocol
RVI	Routed VLAN Interface
RW RoW	Rest of World
SA	Security Association
SAML	Security Assertion Markup Language
SAN	Subject Alternative Name
SCB	Station Control Block
SCEP	Simple Certificate Enrollment Protocol
SCP	Secure Copy Protocol
SCSI	Small Computer System Interface
SDN	Software Defined Networking
SDR	Software-Defined Radio
SDU	Service Data Unit
SD-WAN	Software-Defined Wide Area Network
SFTP	Secure File Transfer Protocol
SHA	Secure Hash Algorithm
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SIRT	Security Incident Response Team
SKU	Stock Keeping Unit
SLAAC	Stateless Address Autoconfiguration

Table 89: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
SMB	Small and Medium Business
SMB	Server Message Block
SMS	Short Message Service
SMTP	Simple Mail Transport Protocol
SNIR	Signal-to-Noise-Plus-Interference Ratio
SNMP	Simple Network Management Protocol
SNR	Signal-to-Noise Ratio
SNTP	Simple Network Time Protocol
SOAP	Simple Object Access Protocol
SoC	System on a Chip
SoH	Statement of Health
SSH	Secure Shell
SSID	Service Set Identifier
SSL	Secure Sockets Layer
SSO	Single Sign-On
STBC	Space-Time Block Coding
STM	Station Management
STP	Spanning Tree Protocol
STRAP	Secure Thin RAP
SU-MIMO	Single-User Multiple-Input Multiple-Output
SVP	SpectraLink Voice Priority
TAC	Technical Assistance Center
TACACS	Terminal Access Controller Access Control System
TCP/IP	Transmission Control Protocol/ Internet Protocol
TFTP	Trivial File Transfer Protocol

Table 89: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
TIM	Traffic Indication Map
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TLV	Type-length-value
ToS	Type of Service
TPC	Transmit Power Control
TPM	Trusted Platform Module
TSF	Timing Synchronization Function
TSPEC	Traffic Specification
TTL	Time to Live
TTLS	Tunneled Transport Layer Security
TXOP	Transmission Opportunity
U-APSD	Unscheduled Automatic Power Save Delivery
UCC	Unified Communications and Collaboration
UDID	Unique Device Identifier
UDP	User Datagram Protocol
UI	User Interface
UMTS	Universal Mobile Telecommunication System
UPnP	Universal Plug and Play
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
USB	Universal Serial Bus
UTC	Coordinated Universal Time
VA	Virtual Appliance
VBN	Virtual Branch Networking

Table 89: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
VBR	Virtual Beacon Report
VHT	Very High Throughput
VIA	Virtual Intranet Access
VIP	Virtual IP Address
VLAN	Virtual Local Area Network
VM	Virtual Machine
VoIP	Voice over IP
VoWLAN	Voice over Wireless Local Area Network
VPN	Virtual Private Network
VRD	Validated Reference Design
VRF	Visual RF
VRRP	Virtual Router Redundancy Protocol
VSA	Vendor-Specific Attributes
VTP	VLAN Trunking Protocol
WAN	Wide Area Network
WebUI	Web browser User Interface
WEP	Wired Equivalent Privacy
WFA	Wi-Fi Alliance
WIDS	Wireless Intrusion Detection System
WINS	Windows Internet Naming Service
WIPS	Wireless Intrusion Prevention System
WISPr	Wireless Internet Service Provider Roaming
WLAN	Wireless Local Area Network
WME	Wireless Multimedia Extensions
WMI	Windows Management Instrumentation

Table 89: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
WMM	Wi-Fi Multimedia
WMS	WLAN Management System
WPA	Wi-Fi Protected Access
WSDL	Web Service Description Language
WWW	World Wide Web
WZC	Wireless Zero Configuration
XAuth	Extended Authentication
XML	Extensible Markup Language
XML-RPC	XML Remote Procedure Call
ZTP	Zero Touch Provisioning

Glossary

The following table lists the terms and their definitions used in this document.

Table 90: *List of Terms*

Term	Definition
802.11	An evolving family of specifications for wireless LANs developed by a working group of the Institute of Electrical and Electronics Engineers (IEEE). 802.11 standards use the Ethernet protocol and CSMA/CA (carrier sense multiple access with collision avoidance) for path sharing.
802.11a	Provides specifications for wireless systems. Networks using 802.11a operate at radio frequencies in the 5GHz band. The specification uses a modulation scheme known as orthogonal frequency-division multiplexing (OFDM) that is especially well suited to use in office settings. The maximum data transfer rate is 54 Mbps.
802.11b	WLAN standard often called Wi-Fi; backward compatible with 802.11. Instead of the phase-shift keying (PSK) modulation method historically used in 802.11 standards, 802.11b uses complementary code keying (CCK), which allows higher data speeds and is less susceptible to multipath-propagation interference. 802.11b operates in the 2.4 GHz band and the maximum data transfer rate is 11 Mbps.

Table 90: *List of Terms*

Term	Definition
802.11g	Offers transmission over relatively short distances at up to 54 Mbps, compared with the 11 Mbps theoretical maximum of 802.11b. 802.11g operates in the 2.4 GHz band and employs orthogonal frequency division multiplexing (OFDM), the modulation scheme used in 802.11a, to obtain higher data speed. Computers or terminals set up for 802.11g can fall back to speeds of 11 Mbps, so that 802.11b and 802.11g devices can be compatible within a single network.
802.11n	Wireless networking standard to improve network throughput over the two previous standards 802.11a and 802.11g with a significant increase in the maximum raw data rate from 54 Mbps to 600 Mbps with the use of four spatial streams at a channel width of 40 MHz. 802.11n operates in the 2.4 and 5.0 bands.
AP	An access point (AP) connects users to other users within the network and also can serve as the point of interconnection between the WLAN and a fixed wire network. The number of access points a WLAN needs is determined by the number of users and the size of the network.
access point mapping	The act of locating and possibly exploiting connections to WLANs while driving around a city or elsewhere. To do war driving, you need a vehicle, a computer (which can be a laptop), a wireless Ethernet card set to work in promiscuous mode, and some kind of an antenna which can be mounted on top of or positioned inside the car. Because a WLAN may have a range that extends beyond an office building, an outside user may be able to intrude into the network, obtain a free Internet connection, and possibly gain access to company records and other resources.
ad-hoc network	A LAN or other small network, especially one with wireless or temporary plug-in connections, in which some of the network devices are part of the network only for the duration of a communications session or, in the case of mobile or portable devices, while in some close proximity to the rest of the network.
band	A specified range of frequencies of electromagnetic radiation.
DHCP	The Dynamic Host Configuration Protocol (DHCP) is an auto-configuration protocol used on IP networks. Computers or any network peripherals that are connected to IP networks must be configured, before they can communicate with other computers on the network. DHCP allows a computer to be configured automatically, eliminating the need for a network administrator. DHCP also provides a central database to keep track of computers connected to the network. This database helps in preventing any two computers from being configured with the same IP address.

Table 90: List of Terms

Term	Definition
DNS Server	<p>A Domain Name System (DNS) server functions as a phonebook for the Internet and Internet users. It converts human readable computer hostnames into IP addresses and vice-versa.</p> <p>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.</p>
DST	<p>Daylight saving time (DST), also known as summer time, is the practice of advancing clocks, so that evenings have more daylight and mornings have less. Typically clocks are adjusted forward one hour near the start of spring and are adjusted backward in autumn.</p>
EAP	<p>Extensible authentication protocol (EAP) refers to the authentication protocol in wireless networks that expands on methods used by the point-to-point protocol (PPP), a protocol often used when connecting a computer to the Internet. EAP can support multiple authentication mechanisms, such as token cards, smart cards, certificates, one-time passwords, and public key encryption authentication.</p>
fixed wireless	<p>Wireless devices or systems in fixed locations such as homes and offices. Fixed wireless devices usually derive their electrical power from the utility mains, unlike mobile wireless or portable wireless which tend to be battery-powered. Although mobile and portable systems can be used in fixed locations, efficiency and bandwidth are compromised compared with fixed systems.</p>
frequency allocation	<p>Use of radio frequency spectrum regulated by governments.</p>
frequency spectrum	<p>Part of the electromagnetic spectrum.</p>
hotspot	<p>A WLAN node that provides Internet connection and virtual private network (VPN) access from a given location. A business traveler, for example, with a laptop equipped for Wi-Fi can look up a local hot spot, contact it, and get connected through its network to reach the Internet and their own company remotely with a secure connection. Increasingly, public places, such as airports, hotels, and coffee shops are providing free wireless access for customers.</p>
IEEE 802.11 standards	<p>The IEEE 802.11 is a set of standards that are categorized based on the radio wave frequency and the data transfer rate.</p>
POE	<p>Power over Ethernet (PoE) is a method of delivering power on the same physical Ethernet wire used for data communication. Power for devices is provided in one of the following two ways:</p> <ul style="list-style-type: none">● Endspan— The switch that an AP is connected for power supply.● Midspan— A device can sit between the switch and APs

Table 90: List of Terms

Term	Definition
	The choice of endspan or midspan depends on the capabilities of the switch to which the OAW-IAP is connected. Typically if a switch is in place and does not support PoE, midspan power injectors are used.
PPPoE	Point-to-Point Protocol over Ethernet (PPPoE) is a method of connecting to the Internet typically used with DSL services where the client connects to the DSL modem.
QoS	Quality of Service (QoS) refers to the capability of a network to provide better service to a specific network traffic over various technologies.
RF	Radio Frequency (RF) refers to the portion of electromagnetic spectrum in which electromagnetic waves are generated by feeding alternating current to an antenna.
TACACS	Family of protocols that handle remote authentication and related services for network access control through a centralized server.
TACACS+	Derived from TACACS but an entirely new and separate protocol to handle AAA services. TACACS+ uses TCP and is not compatible with TACACS. Because it encrypts password, username, authorization, and accounting, it is less vulnerable than RADIUS.
VPN	A Virtual Private Network (VPN) network that uses a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network. A VPN ensures privacy through security procedures and tunneling protocols such as the Layer Two Tunneling Protocol (L2TP). Data is encrypted at the sending end and decrypted at the receiving end.
W-CDMA	Officially known as IMT-2000 direct spread; ITU standard derived from Code-Division Multiple Access (CDMA). Wideband code-division multiple access (W-CDMA) is a third-generation (3G) mobile wireless technology that promises much higher data speeds to mobile and portable wireless devices than commonly offered in today's market.
Wi-Fi	A term for certain types of WLANs. Wi-Fi can apply to products that use any 802.11 standard. Wi-Fi has gained acceptance in many businesses, agencies, schools, and homes as an alternative to a wired LAN. Many airports, hotels, and fast-food facilities offer public access to Wi-Fi networks.

Table 90: *List of Terms*

Term	Definition
WEP	Wired equivalent privacy (WEP) is a security protocol specified in 802.11b, designed to provide a WLAN with a level of security and privacy comparable to what is usually expected of a wired LAN. Data encryption protects the vulnerable wireless link between clients and access points; once this measure has been taken, other typical LAN security mechanisms such as password protection, end-to-end encryption, virtual private networks (VPNs), and authentication can be put in place to ensure privacy.
wireless	Describes telecommunications in which electromagnetic waves (rather than some form of wire) carry the signal over part or all of the communication path.
wireless network	In a Wireless LAN (WLAN), laptops, desktops, PDAs, and other computer peripherals are connected to each other without any network cables. These network elements or clients use radio signals to communicate with each other. Wireless networks are set up based on the IEEE 802.11 standards.
WISP	Wireless ISP (WISP) refers to an internet service provider (ISP) that allows subscribers to connect to a server at designated hot spots (access points) using a wireless connection such as Wi-Fi. This type of ISP offers broadband service and allows subscriber computers, called stations, to access the Internet and the web from anywhere within the zone of coverage provided by the server antenna, usually a region with a radius of several kilometers.
wireless service provider	A company that offers transmission services to users of wireless devices through radio frequency (RF) signals rather than through end-to-end wire communication.
WLAN	Wireless local area network (WLAN) is a local area network (LAN) that the users access through a wireless connection.