AOS-W Instant 8.9.0.0

Release Notes

Contents

The following table provides the revision history of this document.

Table 1: *Revision History*

Revision	Change Description
Revision 03	AOS-225120 was added to the list of Known Issues.
Revision 02	Added an important update regarding the encryption and decryption process of custom certificates in AOS-W Instant 8.9.0.0.
Revision 01	Initial release.

Chapter 1
Release Overview

This AOS-W Instant release notes includes the following topics:

For the list of terms, refer to the Glossary.

Related Documents

The following guides are part of the complete documentation for the Alcatel-Lucent user-centric network:

- *Alcatel-Lucent AP Software Quick Start Guide*
- *AOS-W Instant User Guide*
- *AOS-W Instant CLI Reference Guide*
- *AOS-W Instant REST API Guide*
- *AOS-W Instant Syslog Messages Reference Guide*
- *Alcatel-Lucent OAW-IAP Troubleshooting Guide*

Supported Browsers

The following browsers are officially supported for use with the AOS-W Instant WebUI:

- Microsoft Internet Explorer 11 on Windows 7 and Windows 8
- Microsoft Edge (Microsoft Edge 38.14393.0.0 and Microsoft EdgeHTML 14.14393) on Windows 10
- Mozilla Firefox 48 or later on Windows 7, Windows 8, Windows 10, and macOS
- Apple Safari 8.0 or later on macOS
- Google Chrome 67 or later on Windows 7, Windows 8, Windows 10, and macOS

Terminology Change

As part of advancing Alcatel-Lucent's commitment to racial justice, we are taking a much-needed step in overhauling Alcatel-Lucent engineering terminology to reflect our belief system of diversity and inclusion. Some legacy products and publications may continue to include terminology that seemingly evokes bias against specific groups of people. Such content is not representative of our Alcatel-Lucent culture and moving forward, Alcatel-Lucent will replace racially insensitive terms and instead use the following new language:

Usage	Old Language	New Language
Campus Access Points + Controllers	Master-Slave	Conductor-Member
Instant Access Points	Master-Slave	Conductor-Member
Switch Stack	Master-Slave	Conductor-Member
Wireless LAN Controller	Mobility Master	Mobility Conductor
Firewall Configuration	Blacklist, Whitelist	Denylist, Allowlist
Types of Hackers	Black Hat, White Hat	Unethical, Ethical

Contacting Support

Table 2: *Contact Information*

Contact Center Online	
Main Site	https://www.al-enterprise.com
Support Site	https://myportal.al-enterprise.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
EMEA	+800 00200100 (Toll Free) or +1(650)385-2193
Asia Pacific	+65 6240 8484
Worldwide	1-818-878-4507

Chapter 2
New Features and Enhancements

This chapter describes the features and enhancements introduced in this release.

Important Update on Encryption and Decryption of Custom Certificates

Starting from AOS-W Instant 8.9.0.0, the private key or the passphrase used in custom certificates will be encrypted in flash. If you choose to downgrade the Instant AP from 8.9.0.0 to 8.8.0.x or an earlier version, ensure that you remove all custom certificates before downgrade, as the older versions would not be able to decrypt the private key or the passphrase of the custom certificates. Once the OAW-IAP version is downgraded to 8.8.0.x or an earlier version, you are required to re-upload the custom certificates.

Recovery Procedure

- If you have accidentally downgraded the OAW-IAP software image from 8.9.0.0 to 8.8.0.x without removing all the custom certificates, follow the below instructions:
- For OmniVista 3600 Air Manager Managed OAW-IAPs – The downgrade would detect a certificate mismatch. If auto commit function is enabled, the certificates will be automatically recovered when OmniVista 3600 Air Manager completes the push cert operation. Else, you are required to manually push the certificates from OmniVista 3600 Air Manager to the OAW-IAPs. Also ensure that the auto commit setting is enabled on OmniVista 3600 Air Manager.
- For locally managed OAW-IAPs – Execute the clear-cert command on the OAW-IAP and then manually re-upload the custom certificates.

ARM

Configure Beacon Rates in WLAN SSID Settings

Two new parameters **a-beacon-rate** and **g-beacon-rate** are introduced in the WLAN SSID profile configuration to allow control of the beacon rates independently of the basic rates configured on the profile.

Authentication

Fall Back to Internal Authentication Only During Authentication Server Timeout

A new option to configure the OAW-IAP to fallback to internal authentication only when the response from the authentication server times out is introduced. When enabled, the OAW-IAP uses the internal authentication server to authenticate management users only when the response from the authentication server times out. This can be configured through the CLI and the command to enable this is **mgmt-auth-server-timeout-local-backup**.

Managing Authentication Certificates

Before downgrading an OAW-IAP to an earlier version, clear the certificate assignment for all applications in the OAW-IAP. If OmniVista 3600 Air Manager is used for managing certificates on an OAW-IAP, clear the certificates using the OmniVista 3600 Air Manager UI, or the OAW-IAP CLI.

Support for Using EST Certificate with AP1X Authentication

A new parameter **ap1x tls est** is introduced to allow EST certificates to be used for AP1X authentication.

Support for Using EST Certificate with RADSEC

A new CLI command **radsec-use-est-certificate** is introduced to allow RADSEC to use EST certificates instead of custom or default certificates.

In a scenario where a configuration sync error is observed on a member AP in an AOS-W Instant cluster, or a new member AP joins the cluster, a checksum error is generated. This checksum error is now reported to Central???, in order to determine whether to collect the configuration audit from the member AP.

CLI

Report Crash Information for Conductor and Member APs

A new entry called **Crash Info** is added to the output of the **show aps** command, to indicate if a crash has occurred on a conductor or a member AP.

Change in the Denotation of Radio Bands in Show Commands

The denotation of radio bands in the output of the following commands were changed from **802.11a** and **802.11b/g** to **5 GHz** and **2.4 GHz** respectively:

- show ap monitor
- show ap debug received-reg-table
- show ap bss-table
- show ap allowed-channels

Change in Default SSL Protocol Used for Web Server Connections

The default SSL protocol used for web server connections has been changed to TLS v1.2. This change in default SSL protocol is only applicable to factory default APs running AOS-W Instant 8.9.0.0 and later versions. APs that are upgraded to AOS-W Instant 8.9.0.0 or later versions from earlier versions will continue to use the pre-existing SSL protocol configuration for web server connections.

Datapath / Firewall

Enhancement to Ethernet and Wi-Fi Uplink Preemption

AOS-W Instant now supports configuring two layer-3 wired uplinks. However, only one uplink can remain active at a time, while the other uplink server as a backup in case a failover is initiated.

DHCP

DHCP Information Reporting

OAW-IAPs can now forward DHCP information of clients to a server in Local, Local L3, Centralized L3, Distributed L3, and Virtual Switch assigned networks. This allows the AP to forward the DHCP information of clients to servers for client profiling.

DNS

Support for Including Pointer Records in Updates Sent by DDNS Clients to the DDNS Server

AOS-W Instant now supports including pointer records along with A (host) records in the updates sent by the DDNS clients to the DDNS server. PTR resolves an IP address to a fully-qualified domain name (FQDN) and maps the IP address to a hostname, ensuring that the IP address of the AP is officially connected to the host. The following CLI changes are introduced in this release:

- A new CLI configuration command called **dynamic-dns-ap-ptr** is introduced to enable the DDNS clients to include pointer records in the updates sent to the DDNS server.
- A second CLI command **dynamic-dns-ptr** is introduced in the Distributed, L3 DHCP profile configuration, to allow DHCP L3 clients to send PTR updates to the DDNS server.
- A new parameter called **DHCP PTR DDNS** is introduced in the output of the **show dhcps config** command.
- The **DDNS Client List for PTR records** section is added in the output of the **show ddns clients** command.
- A new parameter called **DDNS PTR Enabled** is added in the output of **show ddns** command.
- The **show log system** command can be used to view the logs related to the DDNS updates.

IoT

Configuring Customizable Payload for APB Beacons

A new CLI command **ble-configure** is introduced to allow configuring a customized payload for APB Beacons. The **show ap debug ble-advertisement-info** command is introduced to show the advertisement information on the OAW-IAP Virtual Switch.

Displaying the Name for Assa Abloy Door Locks

The Assa Abloy door locks will now be displayed using a name in the output of the show ap debug zigbee client-table command. This enhancement is helpful in identifying and debugging issues related to a specific Assa Abloy door lock connected to the system.

Enhancement to Serial Data Transport Profiles

A new CLI parameter **usbSerialDeviceTypeFilter <filter>** is added to the IoT transport profile configuration to allow users to filter serial data based on the USB dongle type. You can also select the **Serial Data** checkbox in Transport services when configuring an IoT transport profile to filter serial data based on one of the following USB dongle types:

- EnOcean
- Piera
- OSU

Enhancement to Tx Power Value for IoT BLE or Zigbee Radio Profile

The maximum configurable value of **Tx power** for BLE and Zigbee based radio profiles is increased to 20.

New IoT Generic Filtering options

The following generic filtering parameters are introduced in the IoT Transport Profile configuration:

- **usbSerialDeviceTypeFilter <filter>**
- **companyIdentifierFilter <filter>**
- **serviceUUIDFilter <filter>**
- **macOuiFilter <filter>**
- **localNameFilter <filter>**

Support for Azure Southbound Action for BLE Devices

The Asynchronous Cloud to Device (C2D) messages are added to support Azure southbound action on BLE devices.

Support Removed for ZF Openmatics Server Type

The **ZF Openmatics** server type is no longer available in the webUI and CLI as part of the IoT transport profile configuration. However, the ZF devices and ZF device class is still available to support ZF sensors through the HTTPS-Websocket server type.

WebUI Enhancements in the IoT Transport Profile

A new field called **Transport services** is added in the IoT transport profile configuration that allows users to filter data based on the following device class filters:

- BLE Telemetry
- BLE Data
- Wi-Fi Data
- Serial Data
- Zigbee Data

Selecting each of these options displays a corresponding **Filters** menu in the webUI, to allow users to choose various IoT device types currently supported by AOS-W Instant.

Platform

Support for New AP Platform

The Alcatel-Lucent 630 Series access points (AP-635) are high performance, tri-radio, indoor access points that can be deployed in either controller-based (AOS-W) or controller-less (AOS-W Instant) network environments. These APs deliver high performance concurrent 2.4 GHz, 5 GHz, and 6 GHz 802.11ax Wi-Fi (Wi-Fi 6E) functionality with MIMO radios (2x2 in 2.4 GHz, 5 GHz, and 6 GHz), while also supporting 802.11a, 802.11b, 802.11g, 802.11n, and 802.11ac wireless services.

Additional features include:

- IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac, and IEEE 802.11ax operation as a wireless access point.

- IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac, and IEEE 802.11ax spectrum monitor.
- Two Ethernet ports, ENET0 and ENET1, capable of data rates up to 2.5 Gbps.
- Compatible with IEEE 802.3bt, IEEE 802.3at, and IEEE 802.3af PoE standards on both Ethernet ports.
- Thermal management.

- Support for OFDMA.

For complete technical details and installation instructions, see Alcatel-Lucent 630 Series Access Points Installation Guide.

Wi-Fi 6 E Support for OAW-AP635 Access Points

OAW-AP635 access points are Wi-Fi 6E capable access points that are equipped with a 6 GHz radio. These APs can operate in the 6 GHz radio band in addition to 2.4 GHz and 5 GHz radio bands. To support the new 6 GHz radio, updates were made to the following AOS-W Instant features:

- New options to configure 6 GHz Wi-Fi networks are introduced in the SSID profile settings.
- New options to configure the 6 GHz radio are introduced in the radio settings of the AP.
- New options to configure ARM features such as band steering, customizing valid channels, and wide bands for the 6 GHz radio are introduced.
- A new radio profile for 6 GHz is introduced.

The above configuration options are only available in OAW-AP635 access points.

VPN

New Parameters Added to IAP-VPN Telemetry Messages

The following parameters will now be included in the IAP-VPN telemetry reporting messages for AOS-W Instant 8.9.0.0 and later versions:

- optional MacAddress dst_mac = 11;
- optional string down_reason = 13;
- optional string link_tag = 15;
- optional string alias_map_name = 17;
- optional IpAddress src_ip = 18;
- optional DeviceType peer_device_type = 20;
- optional ManagedBy managed_by = 24;
- optional IpAddress responder = 29;
- optional string peer_host_name = 30;
- optional string map_name = 31;

Schedule for VPN Preemption

A new setting is added to VPN preemption that enables the configuration of a schedule for preemption to occur. When enabled, the switch from the backup tunnel to the primary tunnel occurs only during the scheduled period. This allows you control the preemption action and reduce preemption switches during the active hours of the network.

Chapter 3
Supported Hardware Platforms

The following table displays the OAW-IAP platforms supported in AOS-W Instant 8.9.0.x release.

Table 3: *Supported OAW-IAP Platforms*

OAW-IAP Platform	Minimum Required AOS-W Instant Software Version
630 Series — OAW-AP635	AOS-W Instant 8.9.0.0 or later
500H Series — AP-503H 560 Series — AP-565 and AP-567	AOS-W Instant 8.7.1.0 or later
500H Series — OAW-AP505H OAW-AP518 — OAW-AP518 OAW-AP570 Series — OAW-AP574, OAW-AP575, and OAW-AP577 570EX Series — AP-575EX and AP-577EX	AOS-W Instant 8.7.0.0 or later
OAW-AP500 Series — OAW-AP504 and OAW-AP505	AOS-W Instant 8.6.0.0 or later
OAW-AP530 Series — OAW-AP534 and OAW-AP535 OAW-AP550 Series — OAW-AP535	AOS-W Instant 8.5.0.0 or later
OAW-AP303 Series — OAW-AP303P OAW-AP510 Series — OAW-AP514 and OAW-AP515	AOS-W Instant 8.4.0.0 or later
OAW-AP303 Series — OAW-AP303 OAW-AP318 Series — OAW-AP318 OAW-AP340 Series — OAW-AP344 and OAW-AP345 OAW-AP370 Series — OAW-AP374, OAW-AP375, and OAW-AP377	AOS-W Instant 8.3.0.0 or later
203H Series — OAW-AP203H	AOS-W Instant 6.5.3.0 or later
203R Series — OAW-AP203R and OAW-AP203RP OAW-AP360 Series — OAW-AP365 and OAW-AP367	AOS-W Instant 6.5.2.0 or later
207 Series — OAW-IAP207 OAW-AP300 Series — OAW-IAP304 and OAW-IAP305	AOS-W Instant 6.5.1.0-4.3.1.0 or later
OAW-AP310 Series — OAW-IAP314 and OAW-IAP315 OAW-AP330 Series — OAW-IAP334 and OAW-IAP335	AOS-W Instant 6.5.0.0-4.3.0.0 or later
OAW-AP320 Series — OAW-IAP324 and OAW-IAP325	AOS-W Instant 6.4.4.3-4.2.2.0 or later

Chapter 4
Regulatory Updates

This chapter contains the Downloadable Regulatory Table (DRT) file version introduced in this release.

Periodic regulatory changes may require modifications to the list of channels supported by an AP. For a complete list of channels supported by an AP using a specific country domain, access the Switch Command Line Interface (CLI) and execute the **show ap allowed-channels country-code <country-code> ap-type <ap-model>** command.

For a complete list of countries and the regulatory domains in which the APs are certified for operation, refer to the Downloadable Regulatory Table or the DRT Release Notes at myportal.al-enterprise.com.

The following DRT file version is part of this release:

- DRT-1.0_80922

Chapter 5
Resolved Issues

The following issues are resolved in this release.

Table 4: *Resolved Issues in AOS-W Instant 8.9.0.0*

New Bug ID	Description	Reported Version
AOS-210688	Apple devices were unable to connect to OAW-AP225 access points operating as Virutal Switches in mesh deployments. This issue occurred when the AP advertised a Channel Switch Announcement but remained in the same channel. The fix ensures that Apple devices can connect to the OAW-AP225 access points operating as Virtual Switches as expected. This issue was observed in OAW-AP225 access points running AOS-W Instant 8.6.0.5 or later versions.	AOS-W Instant 8.6.0.5
AOS-211630	Session ACL configured on an OAW-IAP was not enforced when DPI was disabled. This issue occurred in SSIDs in which client IP assignment was set to **Network Assigned**. The fix ensures that the session ACL takes effect as expected. This issue was observed in APs running AOS-W Instant 8.5.0.0 or later versions.	AOS-W Instant 8.6.0.6
AOS-213613	Clients were unable to stay connected to a wireless network. This issue occurred when: ■ the SSID was configured with MPSK security. ■ the OAW-IAP was assigned only IPv6 addresses. The fix ensures that clients stay connected to SSIDs configured with MPSK security on IPv6-only APs. This issue was observed in APs running AOS-W Instant 8.7.1.0 or later versions.	AOS-W Instant 8.7.1.0
AOS-214836	Clients authenticating using a RADIUS server experienced delay in the authentication process and sometimes required multiple retries before a successful authentication. This issue occurred when the RADIUS server was configured as an FQDN address. The fix ensures that clients authenticate as expected when RADIUS server is configured as FQDN address. This issue was observed in APs running AOS-W Instant 8.6.0.5 or later versions.	AOS-W Instant 8.6.0.5
AOS-214877	The uplink port of an OAW-IAP was disabled by the Switch because of loop protection when the AP switched from mesh mode to Ethernet uplink. The fix ensures that the AP can sucessfully switch from mesh mode to Ethernet uplink. This issue was observed in APs running AOS-W Instant 8.3.0.0 or later versions.	AOS-W Instant 8.3.0.0
AOS-217185	Clients connected to a member AP were unable to pass IP traffic and new clients connecting to the same AP were unable to receive IP addresses.This issue occurred in member APs in an IAP-VPN cluster when the per-AP GRE tunnel connection between the AP and the Switch failed. The fix ensures that the per-AP GRE tunnel stays connected as expected and clients connected to the member AP are able to pass and receive IP traffic as expected. This issue was observed in APs running AOS-W Instant 8.3.0.0 or later versions.	AOS-W Instant 8.3.0.0

Table 4: *Resolved Issues in AOS-W Instant 8.9.0.0*

New Bug ID	Description	Reported Version
AOS-217468	The webUI of an OAW-IAP froze when a new configuration change was applied through the webUI or the CLI. When this issue occurred, the CLI of the conductor AP and the member APs became inaccessible. The fix ensures that the AOS-W Instant webUI reponds as expected after a configuration change is applied through the webUI and the CLI. This issue was observed in APs running AOS-W Instant 8.7.1.1 or later versions.	AOS-W Instant 8.7.1.1
AOS-217829	The new webUI in OAW-IAPs did not update the status of member APs when they were disconnected from the network. The fix ensures that the status of member APs are reflected in the AOS-W Instant webUI as expected. This issue was observed in APs running AOS-W Instant 8.6.0.4 or later versions.	AOS-W Instant 8.6.0.4
AOS-218235	The Switch logged random IP and MAC pairing information in its user table in an IAP-VPN deployment. This issue occurred when clients roamed to a different AP in the cluster before completing the DNS process with the source OAW-IAP. The fix ensures that random IP and MAC pairings are not sent to the Switch. This issue was observed in APs running AOS-W Instant 8.3.0.0 or later versions.	AOS-W Instant 8.3.0.0
AOS-218761 AOS-224026	The webUI of the OAW-IAP failed to sort APs according to client count when clicking on the **Clients** column label in the **Dashboard > Access Points** page of the AOS-W Instant webUI. The fix ensures that OAW-IAPs are sorted according to their client count when the **Clients** column label is clicked in the **Dashboard > Access Points** page of the AOS-W Instant webUI. This issue was observed in APs running AOS-W Instant 8.7.1.1 or later version.	AOS-W Instant 8.7.1.1
AOS-218807	Clients connected to OAW-IAP207 access points were randomly disconnected from the network. The AP reported high CPU and memory utilization during this period. The fix ensures that OAW-IAP207 access points work as expected. This issue was observed in OAW-IAP207 access points running AOS-W Instant 8.5.0.0 or later versions.	AOS-W Instant 8.6.0.7
AOS-218974	iPhone clients running iOS 14 or later versions were unable to connect to SSIDs when a HotSpot2.0 profile was mapped to it. This issue occurred when a HotSpot 2.0 profile was not configured on the iOS device. The fix ensures that iPhone clients running iOS 14 or later versions are able to connect to SSIDs with a HotSpot 2.0 profile as expected. This issue was observed in APs running AOS-W Instant 8.6.0.4 or later versions.	AOS-W Instant 8.6.0.4
AOS-219592	Clients received router advertisement packets from VLANs other than the assigned VLAN. This issue was observed in SSIDs configured with Dynamic VLAN assignment. The fix ensures that clients only receive router advertisement packets from their assigned VLAN. This issue was observed in APs running AOS-W Instant 8.6.0.7 or later versions.	AOS-W Instant 8.6.0.7
AOS-219705	Clients were unable to pass traffic after they disconnect and rejoin an SSID network. This issue occurred when ClearPass Policy Manager was used for authentication. The fix ensures that clients are able to pass traffic as expected after disconnecting and rejoining the network. This issue was observed in APs running AOS-W Instant 8.6.0.7 or later versions.	AOS-W Instant 8.6.0.7

Table 4: *Resolved Issues in AOS-W Instant 8.9.0.0*

New Bug ID	Description	Reported Version
AOS-220622	An OAW-IAP randomly generated **mini_httpd error** messages. These messages were displayed in the output of **show log debug** command and were also sent to the syslog server. Teh fix ensures that the OAW-IAP does not generate random **mini_httpd error** messages. This issue was observed in APs running AOS-W Instant 8.7.1.3 or later versions.	AOS-W Instant 8.7.1.3
AOS-221524	Clients connected to an OAW-IAP were unable to access the Internet. This issue occurred when the MAC address of a member OAW-IAP was mistakenly cached as the DNS server IP. The fix ensures that the correct DNS server IP is cached by the conductor AP and clients are serviced as expected. This issue was observed in APs running AOS-W Instant 8.6.0.8 or later versions.	AOS-W Instant 8.6.0.8
AOS-221532	Clients connected to an OAW-IAP were unable to establish an SSH connection with the VPN concentrator. This issue occurred because the OAW-IAP applied a source NAT rule to traffic destined to the VPNC IP. The fix ensures that the AP establishes SSH connection with the VPN concentrator as expected. This issue was observed in APs running AOS-W Instant 8.8.0.0 or later versions.	AOS-W Instant 8.8.0.0
AOS-221595	The DNS requests of clients were dropped by the OAW-IAP. The debug log listed the reason for DNS packet drop as: **route lookup failure**. The fix ensures that the OAW-IAP processes DNS requests of clients as expected. This issue was observed in APs running AOS-W Instant 8.6.0.0 or later versions.	AOS-W Instant 8.6.0.8
AOS-222127	The first client connecting to an SSID configured with **download-role** was assigned the default role instead of the role received from the ClearPass Policy Manager server. The fix ensures that the first client connecting to an SSID configured with **download-role** is assigned the role received from the ClearPass Policy Manager server. This issue was observed in APs running AOS-W Instant 8.6.0.8 or later versions.	AOS-W Instant 8.6.0.8
AOS-222562	An OAW-IAP generated random station management errors when operating in standalone mode. The fix ensures that the AP does not generate station management error messages in standalone mode. This issue was observed in APs running AOS-W Instant 8.8.0.0 or later versions.	AOS-W Instant 8.8.0.0
AOS-222909	The **show usb-enet** command failed to display the list of all USB devices connected to an OAW-IAP cluster. The fix ensures that the **show usb-enet** command displays the list of all USB devices connected to an OAW-IAP cluster. This issue was observed in OAW-IAP clusters running AOS-W Instant 8.6.0.6 or later versions.	AOS-W Instant 8.6.0.6

Chapter 6
Known Issues and Limitations

This chapter describes the known issues and limitations observed in this release.

Limitations

This section describes the limitations in AOS-W Instant 8.9.0.0.

OAW-AP635 Access Points

OAW-AP635 access points do not support Wi-Fi uplink.

AP Hostname Character Limit Extension

The number of ASCII characters allowed in the OAW-IAP hostname is increased from 32 to 128 characters. The following configuration settings do not support the new limit of 128 ASCII characters in AOS-W Instant 8.8.0.0:

- The AP Name field in Role Derivation or VLAN Derivation.
- The AP Name field in beacon and probe response frames.
- The AP Name field in the **show ap mesh link** and **ap mesh neighbor** commands.

Dynamic Multicast Optimization Unsupported with VLAN Derivation

AOS-W Instant does not support Dynamic Multicast Optimization when the SSID is configured with VLAN derivation.

Inbound Firewall

The **apip-all** configuration is not supported by the **inbound-firewall** command in OAW-IAP cluster deployments. It is only supported in standalone or single-AP modes of deployment.

Uplink Failover Limitation

Uplink failover or pre-emption between eth0 and Wi-Fi uplink is currently not supported.

Unified Communications Manager

UCM does not prioritize NAT traffic.

Zigbee Devices Need to be Re-Paired After Upgrade to AOS-W Instant 8.9.0.0

After upgrading to AOS-W Instant 8.9.0.0 or a later release, you are required to re-pair your Zigbee devices. This limitation is due to upgrades to the Zigbee software stack required to support changing the default link key feature. The default link key is a 16 octet key defined by Zigbee specification and is known as ZigBeeAlliance09. It can be used to decrypt packets exchanged between two devices, if all packets are

captured by Zigbee sniffer from the time a connection is established. The new upgrade allows users to change the default link key.

Known Issues

Following are the known issues observed in this release.

Table 5: *Known Issues in AOS-W Instant 8.9.0.0*

Bug ID	Description	Reported Version
AOS-224500	An OAW-IAP is unable to pass traffic and service clients when both dual Ethernet uplink and Wi-Fi uplink are configured. This issue is observed in APs running AOS-W Instant 8.9.0.0.	AOS-W Instant 8.9.0.0
AOS-224517	An OAW-AP635 access point fails to update DRT when the update process is carried out locally through the WebUI. The WebUI returns the error message: **drt_grade_drt_file_error**. This issue is observed in OAW-AP635 access points running AOS-W Instant 8.9.0.0. **Workaround:** Update the DRT file using a webserver.	AOS-W Instant 8.9.0.0
AOS-225120	Some OAW-IAPs fail to communicate with the Switch in IAP-VPN deployments. This occurs when the AP includes the following configuration: ▪ **vpn gre-outside** is enabled on the AP. ▪ **per-ap-tunnel** is enabled in the VPN tunnel profile. This issue is observed in OAW-AP340 Series, AP-503H, OAW-AP505H, and OAW-AP510 Series access points running AOS-W Instant 8.8.0.0 or later versions.	AOS-W Instant 8.9.0.0

Chapter 7
Upgrading an OAW-IAP

This chapter describes the AOS-W Instant software upgrade procedures and the different methods for upgrading the image on the OAW-IAP.

While upgrading anOAW-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.

Topics in this chapter include:

Upgrading an OAW-IAP Using OmniVista 3600 Air Manager Management Platform

If the multi-class OAW-IAP network is managed by OmniVista 3600 Air Manager, image upgrades can only be done through the OmniVista 3600 Air Manager WebUI. The OAW-IAP images for different classes must be uploaded on the AMP server. If new OAW-IAPs joining the network need to synchronize their software with the version running on the virtual Switch, and if the new OAW-IAP belongs to a different class, the image file for the new OAW-IAP is provided by OmniVista 3600 Air Manager. If OmniVista 3600 Air Manager does not have the appropriate image file, the new OAW-IAP will not be able to join the network.

The virtual Switch communicates with the OmniVista 3600 Air Manager server if OmniVista 3600 Air Manager is configured. If OmniVista 3600 Air Manager is not configured on the OAW-IAP, the image is requested from the Image server.

HTTP Proxy Support through Zero Touch Provisioning

OAW-IAPs experience issues when connecting to OmniVista 3600 Air Manager, or Activate through the HTTP proxy server which requires a user name and password. The ideal way to provide seamless connectivity for these cloud platforms is to supply the proxy information to the OAW-IAP through a DHCP server.

Starting with AOS-W Instant 8.4.0.0, besides being able to authenticate to the HTTP proxy server, the factory default OAW-IAPs can also communicate with the server through a HTTP proxy server DHCP which does not require authentication.

In order for the factory default OAW-IAP to automatically discover the proxy server, you need to configure the HTTP proxy information in the DHCP server option. The OAW-IAP will receive the proxy information and store it in a temporary file.

To retrieve the port and the proxy server information, you need to first configure the DHCP **option 60** to **ArubaInstantAP** as shown below:

```
(Instant AP)(config)# ip dhcp <profile_name>
(Instant AP)("IP DHCP profile-name")# option 60 ArubaInstantAP
```

Secondly, use the following command to configure the proxy server:

```
(Instant AP)(config)# proxy server <host> <port> [<username> <password>]
```

Use the text string **option 148 text server=host_ip,port=PORT,username=USERNAME,password=PASSWORD** to retrieve the details of the proxy server.

Rolling Upgrade on OAW-IAPs with OmniVista 3600 Air Manager

Starting from AOS-W Instant 8.4.0.0, Rolling Upgrade for OAW-IAPs in standalone mode is supported with OmniVista 3600 Air Manager. The upgrade is orchestrated through NMS and allows the OAW-IAPs deployed in standalone mode to be sequentially upgraded such that the APs upgrade and reboot one at a time. With Rolling Upgrade, the impact of upgrading a site is reduced to a single AP at any given point in time. This enhances the overall availability of the wireless network. For more information, see *OmniVista 3600 Air Manager 8.2.8.2 AOS-W Instant Deployment Guide* and *OmniVista 3600 Air Manager 8.2.8.2 Release Notes*.

Upgrading an OAW-IAP Image Manually Using the WebUI

You can manually obtain an image file from a local file system or from a remote server accessed using a TFTP, FTP or HTTP URL.

The following procedure describes how to manually check for a new firmware image version and obtain an image file using the webUI:

1. Navigate to **Maintenance** > **Firmware**.
2. Expand **Manual** section.
3. The firmware can be upgraded using a downloaded image file or a URL of an image file.
   a. To update firmware using a downloaded image file:
      i. Select the **Image file** option. This method is only available for single-class OAW-IAPs.
      ii. Click on **Browse** and select the image file from your local system. The following table describes the supported image file format for different OAW-IAP models:

Access Points	Image File Format
OAW-AP344, OAW-AP345, OAW-AP514, OAW-AP515, OAW-AP518, OAW-AP574, OAW-AP575, AP-575EX, OAW-AP577, and AP-577EX	AlcatelInstant_Draco_8.9.0.x_xxxx
AP-503H, OAW-AP504, OAW-AP505, OAW-AP505H, AP-565, and AP-567.	AlcatelInstant_Gemini_8.9.0.x_xxxx

Access Points	Image File Format
OAW-IAP314, OAW-IAP315, OAW-IAP324, OAW-IAP325, OAW-AP374, OAW-AP375, OAW-AP377, OAW-AP318, and OAW-AP387	AlcatelInstant_Hercules_8.9.0.x_xxxx
OAW-IAP334 and OAW-IAP335	AlcatelInstant_Lupus_8.9.0.x_xxxx
OAW-AP534, OAW-AP535, and OAW-AP535	AlcatelInstant_Scorpio_8.9.0.x_xxxx
OAW-AP303, OAW-AP303H, 303P Series, OAW-IAP304, OAW-IAP305, OAW-AP365, and OAW-AP367	AlcatelInstant_Ursa_8.9.0.x_xxxx
OAW-AP203H, OAW-AP203R, OAW-AP203RP, and OAW-IAP207	AlcatelInstant_Vela_8.9.0.x_xxxx

b. To upgrade firmware using the URL of an image file:

   i. Select the **Image URL** option to obtain an image file from a HTTP, TFTP, or FTP URL.

   ii. Enter the image URL in the **URL** text field. The syntax to enter the URL is as follows:
   - HTTP - http://<IP-address>/<image-file>. For example, http://<IP-address>/AlcatelInstant_Hercules_8.9.0.x_xxxx
   - TFTP - tftp://<IP-address>/<image-file>. For example, tftp://<IP-address>/AlcatelInstant_Hercules_8.9.0.x_xxxx
   - FTP - ftp://<IP-address>/<image-file>. For example, ftp://<IP-address>/AlcatelInstant_Hercules_8.9.0.x_xxxx
   - FTP - ftp://<user name:password>@<IP-address>/<image-file>. For example, ftp://<alcatel:123456>@<IP-address>/AlcatelInstant_Hercules_8.9.0.x_xxxx

The FTP server supports both **anonymous** and **username:password** login methods.

Multiclass OAW-IAPs can be upgraded only in the URL format, not in the local image file format.

4. Disable the **Reboot all APs after upgrade** toggle switch if required. This option is enabled 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.
5. Click **Upgrade Now** to upgrade the OAW-IAP to the newer version.
6. Click **Save**.

Upgrading an OAW-IAP Image Manually Using CLI

The following procedure describes how to upgrade an image using a HTTP, TFTP, or FTP URL:

```
(Instant AP)# upgrade-image <ftp/tftp/http-URL>
```

The following is an example to upgrade an image by using the FTP URL :

```
(Instant AP)# upgrade-image ftp://192.0.2.7/AlcatelInstant_Hercules_8.9.0.x_xxxx
```

The following procedure describes how to upgrade an image without rebooting the OAW-IAP:

```
(Instant AP)# upgrade-image2-no-reboot <ftp/tftp/http-URL>
```

The following is an example to upgrade an image without rebooting the OAW-IAP:

```
(Instant AP)# upgrade-image2-no-reboot ftp://192.0.2.7/AlcatelInstant_Hercules_
8.9.0.x_xxxx
```

The following command describes how 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
```

Upgrade from AOS-W Instant 6.4.x.x-4.2.x.x to AOS-W Instant 8.9.0.x

Before you upgrade an OAW-IAP running AOS-W Instant 6.5.4.0 or earlier versions to AOS-W Instant 8.9.0.x, follow the procedures mentioned below:

1. Upgrade from AOS-W Instant 6.4.x.x-4.2.x.x or any version prior to AOS-W Instant 6.5.4.0 to AOS-W Instant 6.5.4.0.
2. Refer to the *Field Bulletin AP1804-1* at myportal.al-enterprise.com.
3. Verify the affected serial numbers of the OAW-IAP units.