AOS-W Instant 8.8.0.0

Alcatel·Lucent Enterprise

Release Notes

Copyright Information

Open Source Code

Revision History

The following table provides the revision history of this document.

Table 1: *Revision History*

Revision	Change Description
Revision 02	Air Slice support introduced on additional OAW-IAP platforms.
Revision 01	Initial release.

Chapter 1
Release Overview

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

- New Features and Enhancements on page 8
- Supported Hardware Platforms on page 14
- Regulatory Updates on page 16
- Resolved Issues on page 17
- Known Issues on page 24
- Upgrading an OAW-IAP on page 26

For the list of terms, refer to the Glossary.

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

Contacting Support

Table 2: *Contact Information*

Contact Center Online	
Main Site	https://www.al-enterprise.com
Support Site	https://businessportal.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

Terminology Change

As part of advancing Alcatel-Lucent Enterprise's commitment to racial justice, we are taking a much-needed step in overhauling ALE 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 ALE culture and moving forward, ALE 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

Usage	Old Language	New Language
Wireless LAN Controller	Mobility Master	Mobility Conductor
Firewall Configuration	Blacklist, Whitelist	Denylist, Allowlist
Types of Hackers	Black Hat, White Hat	Unethical, Ethical

Chapter 2
New Features and Enhancements

This chapter describes the features and enhancements introduced in Alcatel-Lucent AOS-W Instant 8.8.0.0.

ARM

Uplink MU-MIMO Transmission

AOS-W Instant 8.8.0.0 supports the uplink MU-MIMO transmission of 802.11ax protocol. Prior to AOS-W Instant 8.8.0.0, MU-MIMO allowed to send data frames from access points to clients. Now, the uplink MU-MIMO transmission allows to send data frames from clients to APs. It also helps in achieving throughput gains when applications need to upload large amount of data. It also enables the multiple spatially separated clients to access the channel at the same time and it is also useful in scenarios where stations have limited number of antennas. The uplink MU MIMO transmission is supported only in 5 GHz band. Only OAW-AP535 and OAW-AP535 access points support uplink MU MIMO transmission.

Support for Zero-Wait DFS

Dynamic Frequency Selection (DFS), a mandate for radio systems operating in the 5 GHz band to identify and avoid interference with Radar systems now supports the zero-wait feature. When an 802.11 radio detects radar, it vacates its channel and switches to another channel. This might result in a one minute outage. Starting from AOS-W Instant 8.8.0.0, the zero-wait DFS feature provides seamless change of channels and avoids the one minute outage. Hence, stations do not lose its connectivity when an AP moves to a DFS channel. This feature is enabled by default.

Authentication

Configuring a Timeout Duration for 802.1X Authentication

A new CLI command **ap1x-timeout** is added to configure a timeout duration for 802.1X authentication when the AP is used as a supplicant for 802.1X authentication

Configuring Ageout Time for PMK Cache Entries

A new setting, **delete-pmkcache**, is introduced in the WLAN SSID profile to delete client information in the PMK cache maintained for fast roaming. Configuring this setting deletes client information in the PMK cache immediately after a client disconnects or times out from the network as opposed to the default ageout time of 8 hours. This is configured using the CLI.

Support for New CoA Type

Aruba Instant supports a new CoA type for the radius attribute **Acct-Session-Id**.

Support for New Diffie-Hellman Groups for OWE

AOS-W Instant supports the Diffie-Hellman Groups 20 and 21 for Enhanced Open security.

Datapath

Enabling SFTP Transfers

AOS-W Instant now supports transfer of files using SFTP from the server to an AP. A new CLI command is introduced to support downloading and uploading of a configuration file using SFTP.

The following command restores the configuration through SFTP:

```
(Instant AP)# copy sftp <addr> <file> <username> system config
```

The following command is used to backup the configuration through SFTP:

```
(Instant AP)# copy config sftp <addr> <file> <username>
```

Parameter	Description
<addr>	Denotes the IP address of remote sftp server.
<file>	Denotes the configuration file's absolute path of the remote server.
<username>	Denotes the user name used to establish an ssh connection to the remote server.

Reboot the AP for the configuration changes to take effect.

Firewall

Increase in the Data Rate Range for Bandwidth Limit Contracts and Application Throttling

The upper limit for throttling application traffic and bandwidth limit contract for users is increased to 2 Gbps. This changes the range for **bandwidth-limit**, **throttle-upstream**, and **throttle-downstream** parameters in the **wlan access-rule** command. The new range for these parameters is 1-2147482 Kbps.

IoT

IoT Support for BLE Data forwarding for all Device Classes

AOS-W Instant now allows forwarding of BLE data for all device classes.

IoT Support for Coexistence

IoT Support for New Authentication Type

AOS-W Instant 8.8.0.0 introduces a new IoT authentication type, **Client Credentials**. The new authentication type can be configured in the IoT transport profile.

IoT Support for New BLE Sensors

AOS-W Instant now supports the following BLE vendors:

- Google
- Minew
- DirAct
- GwaHygiene
- Polestar
- Blyott

IoT Support for SES Imagotag

AOS-W Instant now allows an AP to authenticate with SES-Imagotag ESL server and verify the TLS FQDN. AOS-W Instant also supports channel 127 for SES Imagotag ESL.

IoT Support for Piera Sensor

AOS-W Instant now supports USB-based dongles from Piera.

IoT Support for SoluM ESL Gateway

AOS-W Instant now supports Solu M NEWTON USBG2 GW Zigbee-based USB gateway.

IoT Support for New USB-Based Sensors from EnOcean

AOS-W Instant now supports all sub-1-GHz USB-based sensors from EnOcean.

IoT Support for Per-Frame Filtering

AOS-W Instant now supports applying transport profile filters to each frame rather than on the device. This allows bleDataForwarding to treat payload content as packet filter.

IoT WebUI Enhancements

New parameters and fields have been added to configure radio profiles, zigbee profiles, include new vendors.

IoT Support for Zigbee Sniffer

AOS-W Instant supports IoT Zigbee sniffer to capture packets and debug zigbee messages. The internal radio and external USB dongle radio supported by the OAW-IAP can be used as zigbee sniffers. However, the internal or external radio type must be Nordic-based (AP-5xx access points or USB Zigbee radio) for this feature to work.

Support for New Endpoint Type

A new endpoint type Azure IoT Hub is introduced to allow secure, bi-directional communication between devices and the Azure cloud through a managed device that acts as a gateway.

WiFi Co-existence Support for OAW-AP534, OAW-AP535, and OAW-AP535 Access Points

AOS-W Instant now supports Wi-Fi and BLE coexistence on the radio of OAW-AP534, OAW-AP535, and OAW-AP535 access points. This prevent simultaneous transmissions on the radio of an AP. A new parameter called **iot-coexistence-disable** is added to the **rf dot11g-radio-profile** command to allow enabling or disabling of the BLE and Wi-Fi coexistence feature on the 802.11g radio.

Mesh

Enhancements to Topology Optimization Scanning

Topology optimization scanning, a scan performed by the AP to identify better links to the mesh portal, can now be configured on mesh point APs. This allows the mesh point APs to periodically scan the RF network and identify better connection to the mesh portals. The settings to configure the scan are available in the **wlan mesh-profile** command.

Platform

802.11mc Support

802.11mc standard (Wi-Fi Round Trip Time) is supported on OAW-AP500 Series, OAW-AP500H Series, OAW-AP510 Series, OAW-518 Series, OAW-AP530 Series, OAW-AP550 Series, 560 Series, and OAW-AP570 Series access points. This enables the AP to act as an Fine Timing Measurement (FTM) responder and send responses to time measurement queries from FTM capable clients.

Support for Air Slice on Additional OAW-IAP Platforms

Air Slice is now supported on OAW-AP500 Series, OAW-AP510 Series, OAW-AP530 Series, OAW-AP570 Series, and OAW-AP535 access points.

Discovering Disconnected Antennas

The **show ap antenna status** command has been introduced to display the operational antenna status of APs. This command helps in identifying broken or disconnected antennas and thus, helps in faster troubleshooting.

Enhancements to 530 Series and 550 Series Access Points

OAW-AP530 Series and OAW-AP550 Series access points are optimized for better power management in the following scenarios:

- For PoE 802.3at on E0 and PoE 802.3af on E1, the AP power changes to failover mode and gives priority to E0 port so that the overall power is IEEE 802.3at.
- For PoE 802.3bt on E0 and PoE 802.3af on E1, the AP power changes to failover mode and gives priority to E0 port so that the overall power is IEEE 802.3bt.

For more information, see *OAW-AP530 Series Access Point Installation Guide* and *OAW-AP550 Series Access Point Installation Guide*.

Fast Roaming with Mesh APs

The fast roaming feature in mesh deployments is now supported on 203H Series, 203R Series, 207 Series, OAW-AP340 Series, OAW-AP500 Series, OAW-AP500H Series, OAW-AP510 Series, OAW-AP530 Series, OAW-AP550 Series, 560 Series, and OAW-AP570 Series access points.

Dual Ethernet Uplink Support

Both Ethernet ports, Eth0 and Eth1, of OAW-AP318, OAW-AP320 Series, OAW-AP330 Series, OAW-AP370 Series, OAW-AP510 Series, OAW-AP530 Series, and OAW-AP570 Series access points operate as uplink ports by default. The Eth1 port of other APs with more than two Ethernet ports operate as downlink ports by default. The operation mode of the Ethernet ports can be configured using the webUI and the CLI.

Multiple Ethernet Uplink Support

OAW-IAPs enable the configuration of multiple Ethernet ports for uplink. This allows you to configure multiple Ethernet uplinks to function as active and backup uplink for the AP.

Single AP Mode

A new AP deployment mode, Single AP mode, is introduced. The Single AP mode is a type of standalone AP deployment that includes additional security features designed for AOS-W Instant deployments with only one AP in a site.

Support for New 4G Modem

AOS-W Instant supports GTC NETSTICK GLU-194ST 4G USB Modem for Sprint on OAW-IAPs except for OAW-AP303H.

Security

Enhancements to Fast BSS Transmission

Fast BSS transition is now operational with WPA3-Enterprise CNSA mode with GCM-256 encryption.

SNMP

Addition of SNMP traps for Association Failure on AP

Two new SNMP trap messages have been added:

- An SNMP trap is sent when PSK client authentication fails.
- An SNMP trap is sent when the client is rejected after reaching the maximum clients count.

To generate SNMP V3 traps, you need to first configure the SNMPV3 users, then configure the SNMP trap server details.

VPN

Increase in Number of Route Entries for IAP-VPN

The maximum number of static route entries has been increased from 32 to 160.

Support for Public Dynamic DNS

AOS-W Instant supports the configuration of Public Dynamic DNS for the OAW-IAP and its DL3 clients. This enables the AP to send its IP address updates and its clients IP address updates to public DDNS offered by ChangeiP, DynDNS, and No-IP.

Supported OAW-IAPs

The following table displays the OAW-IAP platforms supported in AOS-W Instant 8.8.0.0 release.

Table 3: *Supported OAW-IAP Platforms*

OAW-IAP Platform	Minimum Required AOS-W Instant Software Version
■ OAW-AP500H Series — AP-503H ■ 560 Series — AP-565 and AP-567	AOS-W Instant 8.7.1.0 or later
■ OAW-AP500H Series — OAW-AP505H ■ OAW-518 Series — OAW-AP518 ■ OAW-AP570 Series — OAW-AP574, OAW-AP575, and OAW-AP577 ■ OAW-AP570EX Series — OAW-AP575EX and OAW-AP577EX	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-AP387 Series — OAW-AP387 ■ 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 ■ OAW-AP370EX Series — OAW-AP375EX and OAW-AP377EX	AOS-W Instant 8.3.0.0 or later
■ 203H Series — OAW-AP203H	AOS-W Instant 6.5.3.0 or later

Table 3: *Supported OAW-IAP Platforms*

OAW-IAP Platform	Minimum Required AOS-W Instant Software Version
■ 203R Series — OAW-AP203R and OAW-AP203RP ■ OAW-AP303H Series — OAW-AP303H and OAW-AP303HR ■ 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

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 OAW-IAP CLI and execute the **show ap allowed-channels** 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 service.esd.alcatel-lucent.com.

The following DRT file version is part of this release:

- DRT-1.0_79479

Chapter 5
Resolved Issues

This release includes an update to JQuery, which has been upgraded to version 3.5.1 to address **CVE-2020-11022** and **CVE-2020-11023**.

Additionally, the following issues are resolved in this release.

Table 4: *Resolved Issues in AOS-W Instant 8.8.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-153932 AOS-211583	189128	A OAW-AP303H Series access point crashed and rebooted unexpectedly. The log file listed the reason for reboot as: **Reboot caused by kernel panic: Fatal exception**. The fix ensures that the AP works as expected. This issue was observed in APs using a 3G/4G USB modem for uplink. The crash was triggered when the USB modem lost WAN connectivity. This issue was observed in OAW-AP303H Series access points running AOS-W Instant 8.5.0.10 or later versions.	AOS-W Instant 8.5.0.10
AOS-178788 AOS-208860	181307	An AP crashed and rebooted unexpectedly. The log file lists the reason for the event as: **BadPtr:00000010 PC:wlc_scb_iternext+0x94/0xc0 [wl] Warm-reset.** The fix ensures that the AP works as expected. This issue was observed in APs running AOS-W Instant 8.3.0.6 or later versions.	AOS-W Instant 8.3.0.6
AOS-181197 AOS-208313	192623	An AP reloaded with a different subnet mask after a reboot. This issue occurred when the AP fails to find the DHCP server during AP boot. The fix ensures that the AP reboots with the correct subnet mask. This issue was observed in APs running AOS-W Instant 8.4.0.0 or later versions.	AOS-W Instant 8.6.0.4
AOS-186317 AOS-211873	—	Clients were unable to connect to an Instant AP. Enhancements to the wireless driver resolved this issue. This issue was observed in OAW-AP210 Series and OAW-AP 220 Series access points in a virtual controller role in an AOS-W Instant cluster running AOS-W Instant 8.3.0.0 or later versions.	AOS-W Instant 8.3.0.0
AOS-197400	—	An AP failed to switch uplink interfaces during an uplink failover event. This issue occurred when the AP was configured with two Ethernet uplinks. The fix ensures that the AP switches uplink interfaces during uplink failover. This issue was observed in APs running AOS-W Instant 8.6.0.1 or later versions.	AOS-W Instant 8.6.0.1
AOS-198417 AOS-209440	—	An OAW-AP387 access point reported high memory utilization. This issue occurred due to the large file size of a process log. The fix ensures that the size of the process log is regulated and the AP works as expected. This issue was observed in OAW-AP387 access points running AOS-W Instant 8.5.0.0 or later versions.	AOS-W Instant 8.5.0.0

Table 4: *Resolved Issues in AOS-W Instant 8.8.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-199744 AOS-209046	—	The output of **show iap table long** command did not display any values for **BID (Subnet Name)** column, when the command was executed on the Switch. This issue was observed in backup Switches when an OAW-IAP branch failed over from the primary Switch in an IAP-VPN deployment. Upgrade the Switch to AOS-W 8.7.1.1 to resolve the issue. This issue was observed in IAP-VPN deployments that had Switches running AOS-W 8.3.0.0 or later versions.	AOS-W Instant 8.5.0.7
AOS-200633	—	Users were unable to view the AOS-W Instant webUI in Internet Explorer browser. A **Certificate Invalid** error message was displayed. The fix ensures that the AOS-W Instant WebUI works as expected in Internet Explorer. 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-200816 AOS-210175 AOS-210892	—	Clients were unable to connect to OAW-IAPs due to over utilization of memory. The fix ensures that the Out of Memory issue is resolved. This issue was observed in OAW-AP305, OAW-AP315, and OAW-AP365 access points running AOS-W Instant 8.6.0.2 or later versions.	AOS-W Instant 8.6.0.2
AOS-205319 AOS-216577 AOS-218524	—	Some OAW-AP535 and OAW-AP535 access point crashed and rebooted unexpectedly. The log file listed the reason for reboot as: **Fatal exception in interrupt**. This fix ensures that the AP functions as expected. This issue was observed in OAW-AP535 and OAW-AP535 access points running AOS-W Instant 8.6.0.6 or later versions.	AOS-W Instant 8.7.0.0
AOS-205389	—	A few APs in an AOS-W Instant cluster intermittently reported **config checksum** errors and failed to sync configurations with the conductor AP. The fix ensures that member APs sync configurations from the conductor AP without any checksum errors. This issue occurred in OmniVista 3600 Air Manager managed AOS-W Instant networks. This issue was observed in APs running AOS-W Instant 8.5.0.7 or later versions.	AOS-W Instant 8.5.0.7
AOS-205932	—	Some client devices were disconnected from the network when roaming from one AP to another. This issue occurred when broadcast and multicast traffic for clients were blocked due to **Group Transient Key (GTK)** sync failure between the neighboring APs. The fix ensures that APs sync GTK successfully and clients can roam without any interruption in connection. This issue was observed in 802.11r enabled APs running AOS-W Instant 8.4.0.2 or later versions.	AOS-W Instant 8.4.0.2

Table 4: *Resolved Issues in AOS-W Instant 8.8.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-206840	—	The checksum ID and radio information of an AP were not updated on the Virtual Switch. This issue occurred in APs that are configured with a static channel. The fix ensures that the AP updates checksum ID and radio information on the Virtual Switch. This issue was observed in OAW-AP300 Series, OAW-AP315, OAW-AP320 Series, OAW-AP330 Series, OAW-AP360 Series, and OAW-AP370 Series access points running AOS-W Instant 8.4.0.6 or later versions.	AOS-W Instant 8.4.0.6
AOS-207070	—	Clients were unable to authenticate into the network using captive portal authentication when it was configured with an external RADIUS server. This issue occurred when the duration of TCP handshake process with the RADIUS server exceeded 400ms due to WAN issues. The fix ensures that clients can connect to networks using captive portal authentication configured with an external RADIUS server as expected. This issue was observed in APs running AOS-W Instant 8.5.0.0 or later versions.	AOS-W Instant 8.5.0.5
AOS-207415	—	The access request of some clients were rejected by the RADIUS server. This issue occurred when the access request sent from the AP to the RADIUS server was missing the **State** attribute. The fix ensures that clients can authenticate with the RADIUS server as expected. This issue was observed in APs running AOS-W Instant 8.4.0.0 or later versions.	AOS-W Instant 8.4.0.0
AOS-207599 AOS-207665	—	The local WebUI for some APs displayed the error message: **ERR_SSL_SERVER_CERT_BAD_FORMAT**. This issue occurred when the web browser used to access the local WebUI was Google Chrome, Microsoft Edge 79 and later versions, or Apple Safari. The fix ensures that the local webUI of the AP works as expected. This issue was observed in APs that were rebooted in the factory default state after upgrading to AOS-W Instant 8.7.0.0.	AOS-W Instant 8.7.0.0
AOS-207602	—	An OAW-IAP failed to complete 802.1X authentication when **Validate server** option was selected in the **Configuration** > **System** > **Show advanced options> Uplink** > **AP1X** section in the webUI. The debug log lists the reason for failure as: **Server validation failed**. The fix ensures that the AP completes 802.1X authentication and works as expected. This issue was observed in OAW-AP200 Series access points running AOS-W Instant 8.6.0.4 or later versions.	AOS-W Instant 8.6.0.4
AOS-207781 AOS-210105 AOS-211820	—	An OAW-IAP learned wrong IP addresses for certain domain names. The fix ensures that the AP learns the correct IP address. This issue was observed in APs running AOS-W Instant 8.5.0.0 or later versions.	AOS-W Instant 8.6.0.4
AOS-207893	—	Clients were unable to get an IP address. This occurred due to high memory utilization in the AP caused by the BLE daemon process. The fix ensures that memory utilization in the AP is regulated by the creation of a new boot log file at every restart instance of the BLE daemon process. This issue was observed in APs running AOS-W Instant 8.5.0.3 or later versions.	AOS-W Instant 8.5.0.3

Table 4: *Resolved Issues in AOS-W Instant 8.8.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-208330	—	OmniVista 3600 Air Manager reported incorrect client data transfer speeds in the RF dashboard. The fix ensures that OmniVista 3600 Air Manager reports the correct data transfer speeds in the RF dashboard. This issue was observed in OmniVista 3600 Air Manager managed APs running AOS-W Instant 8.6.0.2 or later versions.	AOS-W Instant 8.6.0.2
AOS-208474	—	An OAW-IAP disconnected itself from the cluster and then rejoined it. The log file lists the reason for the event as: **stm | PAPI_Send failed, send_papi_message_with_args, 1215: Resource temporarily unavailable**. The fix ensures that the AP stays connected to the cluster. 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-208648	—	The system log of an OAW-IAP randomly registered a lot of **Swarm quit factory default status by : ssid_config** messages. The fix ensures that the syslog of the AP does not generate random messages. This issue was observed in APs running AOS-W Instant 8.7.0.0 or later versions.	AOS-W Instant 8.7.0.0
AOS-208681	—	The AOS-W Instant webUI gets stuck on the uploading screen during firmware upgrade. This issue occurred when Internet Explorer was used to access the webUI. The fix ensures that the AOS-W Instant webUI works as expected when accessed using Internet Explorer. This issue was observed in access points running AOS-W Instant 8.6.0.5 or later versions.	AOS-W Instant 8.6.0.5
AOS-208783	—	Some GUI elements in the new webUI were not visible when accessed using Internet Explorer. This issue occurred when the system used to access the webUI had the font download option disabled in the firewall settings. The fix ensures that the new webUI is rendered as expected. This issue was observed in APs running AOS-W Instant 8.6.0.0 or later versions.	AOS-W Instant 8.6.0.5
AOS-209148	—	Clients were unable to reach the splash page for captive portal authentication. This issue occurred when the AP failed to process DNS queries from captive portal clients. The fix ensures that clients join the captive portal network as expected. This issue was observed in AOS-W Instant 8.6.0.0 or later versions.	AOS-W Instant 8.7.0.0
AOS-209239	—	An OAW-IAP operating as a DHCP server failed to serve IP addresses to clients connected to it. This issue occurred when the subnet for the DHCP scope was the same as the IP address of the AP. This fix ensures that the AP serves IP addresses to clients connected to it. 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 8.8.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-209306	—	Clients were either unable to connect to the AP or were getting disconnected from it. This issue occurred when the SAPD process over utilized CPU memory. The fix ensures that the memory usage of SAPD process is regulated and clients connect to the access point as expected. This issue was observed in OAW-APAP-324 access points running AOS-W Instant 8.4.0.0 or later versions.	AOS-W Instant 8.4.0.0
AOS-209855 AOS-210214 AOS-211809 AOS-212590 AOS-212823 AOS-214704		Some OAW-IAPs crashed and rebooted unexpectedly. The log file listed the reason for the event as: **Kernel panic - not syncing: Fatal exception in interrupt**. The fix ensures that the APs work as expected. This issue was observed in APs running AOS-W Instant 8.7.0.0 or later versions.	AOS-W Instant 8.7.0.0
AOS-210059	—	An OAW-IAP failed to install CA certificate for 802.1X authentication. The AP displayed the error message: **Validate certificate file failed**. The fix ensures that CA certificate is installed on the AP as expected. This issue was observed in APs running AOS-W Instant 8.5.0.9 or later versions.	AOS-W Instant 8.5.0.9
AOS-210141	—	An OAW-IAP sent RADIUS accounting messages with incorrect IP information. This issue occurred when the client moved from one user role to another after connecting to the network and the SSID had **Enforce DHCP** enabled. The fix ensures that the AP sends the correct IP information in RADIUS accounting messages when **Enforce DHCP** is enabled on the SSID. This issue was observed in APs running AOS-W Instant 8.6.0.2 or later versions.	AOS-W Instant 8.6.0.2
AOS-210224	—	Two member APs in a cluster were broadcasting on the same channel when other free channels were available. The fix ensures that the member APs broadcast on different channels to optimize bandwidth usage. This issue was observed in APs running AOS-W Instant 8.5.0.6 or later versions.	AOS-W Instant 8.5.0.6
AOS-210290	—	An OAW-IAP failed to update the service ID of AirGroup services when the service ID was configured through the AOS-W Instant WebUI. This issue occured when the name of the service ID contains a "." character. This issue was observed in APs running AOS-W Instant 8.7.0.0 or later versions.	AOS-W Instant 8.7.0.0
AOS-210338	—	OAW-IAPs scanned by Qualys server reported **QID:11827** indicating that theOAW-IAP HTTP POST operation missed one or more headers. The fix ensures that the headers are included in the HTTP POST operation. This issue was observed in AOS-W Instant 8.6.0.2 or later versions.	AOS-W Instant 8.6.0.2

Table 4: *Resolved Issues in AOS-W Instant 8.8.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-210440	—	Administrator authentication failed when accessing the OAW-IAP through the WebUI. This issue occured when the administrator password included special characters such as " or '. 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-210717 AOS-212956	—	The **Client-view heatmap** window in **Dashboard** > **Clients** page of the AOS-W Instant WebUI did not display any data. This issue occurred when the number of client match history record exceeds 300. This issue was observed in APs running AOS-W Instant 8.7.0.0 or later versions.	AOS-W Instant 8.7.0.0
AOS-210855 AOS-213801	—	The conductor AP in an AOS-W Instant cluster randomly encountered a CLI core crash and reset the Age for APs in the output of **show aps** command. The fix ensures that the AP works as expected. This issue was observed in APs running AOS-W Instant 8.5.0.0 or later versions.	AOS-W Instant 8.5.0.0
AOS-210903	—	Clients were getting de-authenticated from OAW-IAPs with a message: **No reason available**. The fix ensures that the clients do not get de-authenticated from the AP without reason. This issue was observed in OAW-AP535 access points running AOS-W Instant 8.7.0.0 or later versions.	AOS-W Instant 8.7.0.0
AOS-211407	—	Clients connected to an OAW-IAP were unable to send and receive traffic. This issue was observed in networks configured with Deny intra VLAN traffic and the client IP assignment was set to Virtual Controller managed. This issue occurred after a conductor AP failover event in the AOS-W Instant cluster. The fix ensures that clients can send and receive traffic in OAW-IAP clusters 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-211525 AOS-212652	—	An OAW-IAP inherits the gateway IP of the layer 2 switch in the event of a switch outage and causes an IP address conflict when the switch is back online. The fix ensures that the AP does not inherit the gateway IP of the layer 2 switch in the event of a switch outage. This issue was observed in APs running AOS-W Instant 8.5.0.5 or later versions.	AOS-W Instant 8.5.0.5
AOS-212238	—	An OAW-IAP failed to update device-owner and shared-user-list attributes sent from the ClearPass Policy Manager server in the AirGroup CPPM entries table. The fix ensures that the device owner, shared-user-list, and other shared attributes are displayed in the table.This issue was observed in APs running AOS-W Instant 8.7.0.0 or later versions.	AOS-W Instant 8.7.0.0

Table 4: *Resolved Issues in AOS-W Instant 8.8.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-213257	—	An OAW-IAP failed to remove the domain name suffix when logging username entries in the AirGroup users table. The fix ensures that the AP logs the username entry in the AirGroup table as expected. This issue occurred when **Enforce ClearPass registration** was enabled in the **Configuration** > **Services** > **AirGroup** section of the WebUI. 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-213941 AOS-215575	—	An OAW-IAP stopped broadcasting and rebooted unexpectedly. The log file lists the reason for reboot as: **Reboot due to trigger the cooldown event**. The fix ensures that the AP is able to pass traffic even at sub-zero temperatures. This issue is observed in APs running AOS-W Instant 8.7.1.0 or later versions.	AOS-W Instant 8.7.1.0
AOS-214199	—	An OAW-IAP failed to establish an SSL connection with OpenDNS servers. This issue occurred due to incompatibility with the content-header message sent by the OpenDNS server. The fix ensures that the SSL connection is successfully established with the OpenDNS server. This issue was observed in APs running AOS-W Instant 8.5.0.11 or later versions.	AOS-W Instant 8.5.0.11
AOS-214595	—	OAW-IAPs failed to respond to the **Alcatel-LucentPhyType** and Alcatel-Lucent**HTMode** MIB queries. This issue is resolved by: • Redefining the Alcatel-LucentHTMode and Alcatel-LucentPhyType labels and adding new mib OIDs aiClientPhyType and aiClientHtMode in the OAW-IAP MIB. • Redefining the labels SiemensHTMode and SiemensPhyType and adding new MIB OIDs sieClientPhyType and sieClientHtMode in the Siemens MIB. This issue was observed in OAW-IAPs running Alcatel-Lucent AOS-W Instant 8.6.0.6 or later versions.	AOS-W Instant 8.6.0.6
AOS-215475	—	The uplink preemption feature did not work on OAW-AP203R. This issue occurred as the Eth0 port status was not updated. The fix ensures that the uplink preemption feature works as expected. This issue was observed in APs running AOS-W Instant 8.6.0.0 or later versions.	AOS-W Instant 8.6.0.0
AOS-216793 AOS-217849	—	An AP crashed and rebooted unexpectedly. The log file listed the reason for reboot as: **Critical process /aruba/bin/stm [pid 26982] DIED, process marked as RESTART**. This fix ensures that the AP functions as expected. This issue was observed in APs running AOS-W Instant 8.6.0.0 or later versions.	AOS-W Instant 8.6.0.0
AOS-216834	—	Clients were unable to connect to some APs due to their high memory usage. This issue occured when DHCP or DNS events were subscribed and changes to the clarify configuration increased the process run time. The fix ensures that the clients are able to connect to the APs without issues. This issue was observed in APs running AOS-W Instant 8.6.0.7 or later versions.	AOS-W Instant 8.6.0.7

Chapter 6
Known Issues

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

Limitations

This section describes the limitations in Alcatel-Lucent AOS-W Instant 8.8.0.0.

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.

Known Issues

Following are the known issues observed in this release.

Table 5: *Known Issues in AOS-W Instant 8.8.0.0*

Bug ID	Description	Reported Version
AOS-203279	An AP-565 access point crashes and fails to reboot when software version prior to AOS-W Instant 8.7.1.0 is installed. This issue is observed in AP-565 access points running AOS-W Instant 8.7.1.0 or later versions.	AOS-W Instant 8.7.1.0
AOS-203311	An AP-565 access point reboots and disables FIPS mode. This issue is observed in AP-565 access points running AOS-W Instant 8.7.1.0 or later versions.	AOS-W Instant 8.7.1.0
AOS-208450	An AP-503H access point operating as a mesh point sends incorrect source MAC address in LLDP messages. This issue is observed in AP-503H access points running AOS-W Instant 8.7.1.0 or later versions.	AOS-W Instant 8.7.1.0
AOS-209405 AOS-212894 AOS-213220 AOS-214438	An OAW-IAP fails to block certain application and service traffic despite having ACLs configured to block them. This issue occurs with applications and services that use QUIC protocol, which is currently not supported by AppRF. This issue is observed in APs running AOS-W Instant 8.3.0.0 or later versions. **Workaround:** Add an ACL rule to deny traffic in UDP ports **443** and **80**. This configures the AP to deny traffic when the ACL is applied and forces the application to use TLS instead of QUIC protocol.	AOS-W Instant 8.6.0.9
AOS-214157	When multiple DL3 clients with the same host name connect to the same AP, the AP updates the IP address of the most recently connected client. This issue is observed in networks configured with public DDNS. This issue is observed in APs running AOS-W Instant 8.8.0.0.	AOS-W Instant 8.8.0.0
AOS-214948	Some mesh APs display incorrect mesh link information in the output of **show ap mesh link** command. This issue is observed in APs running AOS-W Instant 8.7.1.0 or later versions.	AOS-W Instant 8.8.0.0
AOS-215513	An OAW-IAP fails to resolve DNS when the following configurations are applied: • Uplink VLAN configured is not 1. • Primary VPN is configured and the default gateway is the IPSec tunnel. This issue is observed in APs running AOS-W Instant 8.8.0.0.	AOS-W Instant 8.8.0.0
AOS-218747	The OAW-IAP database in the Switch is not populated with DL3 entries. This issue occurs when an apostrophe (') character is used in the OAW-IAP branch name. This issue is observed in APs running AOS-W Instant 8.6.0.9 or later versions.	AOS-W Instant 8.6.0.9

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.

Topics in this chapter include:

- Upgrading an OAW-IAP Using OmniVista 3600 Air Manager Management Platform on page 26
- Upgrading an OAW-IAP Image Manually Using WebUI on page 27
- Upgrading an OAW-IAP Image Manually Using CLI on page 30
- Upgrade from AOS-W Instant 6.4.x.x-4.2.x.x to AOS-W Instant 8.8.0.x on page 30

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.

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 Alcatel-Lucent 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 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.

In the Old WebUI

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 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, OAW-AP575EX, OAW-AP577, and OAW-AP577EX	AlcatelInstant_Draco_8.8.0.x_xxxx
OAW-AP504, OAW-AP505, OAW-AP500H Series, and 560 Series	AlcatelInstant_Gemini_8.8.0.x_xxxx
OAW-IAP314, OAW-IAP315, OAW-IAP324, OAW-IAP325, OAW-AP374, OAW-AP375, OAW-AP377, OAW-AP318, and OAW-AP387	AlcatelInstant_Hercules_8.8.0.x_xxxx
OAW-IAP334 and OAW-IAP335	AlcatelInstant_Lupus_8.8.0.x_xxxx

Access Points	Image File Format
OAW-AP534, OAW-AP535, and OAW-AP535	AlcatelInstant_Scorpio_8.8.0.x_xxxx
OAW-AP303, OAW-AP303H, 303P Series, OAW-IAP304, OAW-IAP305, OAW-AP365, and OAW-AP367	AlcatelInstant_Ursa_8.8.0.x_xxxx
OAW-AP203H, OAW-AP203R, OAW-AP203RP, and OAW-IAP207	AlcatelInstant_Vela_8.8.0.x_xxxx

- Select the **Image URL** option. Select this option to obtain an image file from a HTTP, TFTP, or FTP URL.
  - HTTP - http://<IP-address>/<image-file>. For example, http://<IP-address>/AlcatelInstant_Hercules_8.8.0.x_xxxx
  - TFTP - tftp://<IP-address>/<image-file>. For example, tftp://<IP-address>/AlcatelInstant_Hercules_8.8.0.x_xxxx
  - FTP - ftp://<IP-address>/<image-file>. For example, ftp://<IP-address>/AlcatelInstant_Hercules_8.8.0.x_xxxx
  - FTP - ftp://<user name:password>@<IP-address>/<image-file>. For example, ftp://<alcatel:123456>@<IP-address>/AlcatelInstant_Hercules_8.8.0.x_xxxx

NOTE

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.

3. Clear the **Reboot all APs after upgrade** check box if required. This 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.

In the New WebUI (AOS-W Instant 8.4.0.0 or later versions)

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 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, OAW-AP575EX, OAW-AP577, and OAW-AP577EX	AlcatelInstant_Draco_8.8.0.x_xxxx
OAW-AP504, OAW-AP505, OAW-AP500H Series, and 560 Series	AlcatelInstant_Gemini_8.8.0.x_xxxx
OAW-IAP314, OAW-IAP315, OAW-IAP324, OAW-IAP325, OAW-AP374, OAW-AP375, OAW-AP377, OAW-AP318, and OAW-AP387	AlcatelInstant_Hercules_8.8.0.x_xxxx
OAW-IAP334 and OAW-IAP335	AlcatelInstant_Lupus_8.8.0.x_xxxx
OAW-AP534, OAW-AP535, and OAW-AP535	AlcatelInstant_Scorpio_8.8.0.x_xxxx
OAW-AP303, OAW-AP303H, 303P Series, OAW-IAP304, OAW-IAP305, OAW-AP365, and OAW-AP367	AlcatelInstant_Ursa_8.8.0.x_xxxx
OAW-AP203H, OAW-AP203R, OAW-AP203RP, and OAW-IAP207	AlcatelInstant_Vela_8.8.0.x_xxxx

- Select the **Image URL** option. Select this option to obtain an image file from a HTTP, TFTP, or FTP URL.
  - HTTP - http://<IP-address>/<image-file>. For example, http://<IP-address>/AlcatelInstant_Hercules_8.8.0.x_xxxx
  - TFTP - tftp://<IP-address>/<image-file>. For example, tftp://<IP-address>/AlcatelInstant_Hercules_8.8.0.x_xxxx
  - FTP - ftp://<IP-address>/<image-file>. For example, ftp://<IP-address>/AlcatelInstant_Hercules_8.8.0.x_xxxx
  - FTP - ftp://<user name:password>@<IP-address>/<image-file>. For example, ftp://<alcatel:123456>@<IP-address>/AlcatelInstant_Hercules_8.8.0.x_xxxx

NOTE

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.

3. 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.
4. Click **Upgrade Now** to upgrade the OAW-IAP to the newer version.
5. Click **Save**.

Upgrading an OAW-IAP Image Manually Using CLI

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_8.8.0.x_xxxx
```

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_8.8.0.x_xxxx
```

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 8.8.0.x

Before you upgrade an OAW-IAP running AOS-W Instant 6.5.4.0 or earlier versions to AOS-W Instant 8.8.0.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 https://businessportal2.alcatel-lucent.com.
3. Verify the affected serial numbers of the OAW-IAP units.