AOS-W Instant 8.7.0.0

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 04	The description of AOS-197800 was modified.
Revision 03	Added AOS-207599 and AOS-207665 to the list of Known Issues in 8.7.0.0.
Revision 02	Removed instances of Fremont Sensors.
Revision 01	Initial release.

Chapter 1
Release Overview

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

For the list of terms, refer 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://businessportal2.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
EMEA	+800 00200100 (Toll Free) or +1(650)385-2193
Asia Pacific	+65 6240 8484
Worldwide	1-818-878-4507

This chapter describes the features and enhancements introduced in Alcatel-Lucent AOS-W Instant 8.7.0.0.

ARM

802.11ax Aware Client Match

The **client-match he-min-snr** parameter is introduced to configure the minimum SNR value required for the targeted HE (802.11ax) steering. The default value of this parameter is 40.

The following show commands have been enhanced to display the HE related information of the APs in the output:

- show arm config
- show ap client-view
- show ap client-match-ssid-table
- show ap client-probe-report <radio id>
- show ap virtual-beacon-report
- show ap client-match-history client-mac <client>
- show ap client-match-triggers

ARM Settings in Radio Profiles

ARM settings for individual radios can be configured in their respective radio profiles in addition to the ARM profile. This feature allows you to maximize network efficiency in dense RF environments by customizing ARM settings for individual radios. These ARM configurations are available under **rf dot11a-radio-profile**, **rf dot11a-secondary-radio-profile**, and **rf dot11g-radio-profile** commands.

Authentication

Enhancement to EAP Fragments

A new CLI command **dot1x eap-frag-mtu <mtu>** is added to configure the IP MTU to be considered for EAP fragmentation.

Datapath / Firewall

Adding a Comment in Access Rules

A new parameter **rule desc <description>** is introduced in the **wlan access-rule** command. This parameter allows you to insert a comment in the access rule, to help identify its purpose.

Unified Communications Manager

Unified Communications Manager is a new service module that manages voice and video calls in OAW-IAPs. UCM identifies voice and video call sessions through SIP control packets and prioritizes them in the datapath for better end user experience. The call records and UCM processes are logged in the AP for monitoring.

OAW-IAP Management

Certificate Enrollment Using EST

Customized certificates can now be enrolled or re-enrolled automatically on the OAW-IAP by creating an EST profile.

Support for Low Power Mode

A new CLI command **ap-poe-power-optimization** is introduced in the privileged execution mode, to enable or disable low power mode on an OAW-IAP. Enabling this feature results in the USB and POE-PSE capabilities, if applicable, on the AP to be disabled, and the requested POE draw is reduced accordingly.

IDS

Enhancements to Control Ageout of Valid APs and Interfering APs

Two new CLI parameters, **valid-ap-max-unseen-timeout** and **ap-max-unseen-timeout**, are introduced in the **ids** command to control the ageout duration of valid and interfering APs. These parameters enable you to effectively control the RF environment.

IoT

IoT Endpoint Configuration Update

When the **meridian-asset-tracking** endpoint is configured and the firmware is upgraded to AOS-W Instant 8.7.0.0, the CA certificate should be uploaded in order to connect to the meridian server.

Support for Data Filter

AOS-W Instant supports IoT data filter that reduces the traffic on the telemetry interfaces.

Support for Exposure Notification

AOS-W Instant now supports a IoT device payload content called **Exposure Notification** based on the presence of service UUID 0xFD6F and service data 0xFD6F.

Support for Input-Filter on BLE Devices

AOS-W Instant now supports a input-filter for BLE devices. When IoT transport profiles are configured, BLE-devices are filtered based on the IoT transport profiles which may include device class, UUID, or vendor filters. Only BLE devices that should be reported are stored in the BLE-table and data loss is avoided.

Support for IoT Southbound API RT-4894-SAM

AOS-W Instant now supports an IoT Southbound API that allows interaction with IoT devices and does not require any knowledge of the device by Alcatel-Lucent infrastructure.

Support for Wiliot Sensor

AOS-W Instant now supports Wiliot sensors. Wiliot is a leading provider of battery-free BLE tags. An AP streams the BLE data received from a Wiliot sensor over Telemetry-Websocket.

Zigbee Socket Device

ZigBee Socket Device (ZSD) can be configured and applied as a filter in IoT transport. With ZSD, specify the source endpoint, destination endpoint, destination profile ID, or destination cluster ID and the packets between the ZigBee devices and server are transmitted through the Alcatel-Lucent Telemetry Websocket.

Mesh

Configuring Multiple Mesh Cluster Profiles

Previously, users could only configure **mesh-cluster-name** and **mesh-cluster-key** in AP-ENV, and only one command could be configured, Starting from AOS-W Instant 8.7.0.0, a new command **mesh-cluster** is introduced to configure more than one mesh cluster profile on an OAW-IAP and assign a priority to each profile. This allows the users to configure a primary mesh cluster and also keep a backup mesh cluster in case the primary mesh cluster goes down. The mesh points connected to the primary cluster would then attempt to connect to the mesh cluster with the next highest priority. This command currently allows users to configure a maximum of 16 mesh cluster profiles on an OAW-IAP and assign a priority between 1 to 16 for each profile.

Mesh Link Radio Selection for OAW-AP340 Series and OAW-AP550 Series Access Points

The 5 GHz radio used for mesh link in OAW-AP340 Series and OAW-AP550 Series access points can now be configured. This feature is supported in dual 5 GHz and split 5 GHz radio enabled APs. Show commands related to mesh cluster are also enhanced to display the operating radio information of mesh APs. This feature is designed to offer better control of the RF environment in mesh networks.

Platform

OAW-AP570 Series Access Points

The Alcatel-Lucent OAW-AP570 Series access points (OAW-AP574, OAW-AP575, and OAW-AP577) are high performance, multi-radio, outdoor 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 and 5 GHz 802.11ax Wi-Fi (Wi-Fi 6) functionality with MIMO radios (2x2 in 2.4 GHz, 4x4 in 5 GHz), while also supporting 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac, and 802.11ax wireless services.

The APs provide the following functionality:

- 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.
- Mesh mode.
- Two Ethernet ports, ENET0 and ENET1, capable of data rates up to 2.5 Gbps and 1 Gbps respectively.
- Compatible with IEEE 802.3bt, IEEE 802.3at, and IEEE 802.3af PoE standards on both Ethernet ports.
- Intelligent Thermal Management.

For complete technical details and installation instructions, see *Alcatel-Lucent OAW-AP570 Series Access Points Installation Guide*.

OAW-AP570EX Series Access Points

The Alcatel-Lucent OAW-AP570EX Series access points (OAW-AP575EX and OAW-AP577EX) are high performance, multi-radio access points suitable for harsh and hazardous outdoor locations. They 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 and 5 GHz 802.11ax Wi-Fi (Wi-Fi 6) functionality with MIMO radios (2x2 in 2.4 GHz, 4x4 in 5 GHz), while also supporting 802.11a, 802.11b, 802.11g, 802.11n, and 802.11ac wireless services.

The APs provide the following functionality:

- 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.
- Mesh mode.
- Two Ethernet ports, ENET0 and ENET1, capable of data rates up to 2.5 Gbps and 1 Gbps respectively.
- Compatible with IEEE 802.3bt, IEEE 802.3at, and IEEE 802.3af PoE standards on both Ethernet ports.
- Thermal Management.

For complete technical details and installation instructions, see *Alcatel-Lucent OAW-AP570EX Series Access Points Installation Guide*.

OAW-AP505H Access Points

The Alcatel-Lucent OAW-AP505H access points are entry-level, dual-radio wireless AP that can be deployed in either controller-based (AOS-W) or controller-less (AOS-W Instant) network environments. These APs delivers high performance concurrent 2.4 GHz and 5 GHz 802.11ax Wi-Fi (Wi-Fi 6) functionality with 2x2 MU-MIMO radios, while also supporting 802.11a, 802.11b, 802.11g, 802.11n, and 802.11ac wireless services.

The APs provide the following functionality:

- 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.
- Mesh mode.
- Compatible with IEEE 802.3bt, IEEE 802.3at, and IEEE 802.3af PoE standards.
- One uplink Ethernet port capable of data rates up to 2.5 Gbps.
- Four downlink Ethernet ports capable of data rates up to 1 Gbps, including two 802.3at PoE PSE ports for supplying power to downlink devices.
- Integrated BLE and Zigbee radios.
- Flexible USB host interface with 5W power sourcing capability.

For complete technical details and installation instructions, see *Alcatel-Lucent OAW-AP505H Access Point Installation Guide*.

OAW-AP518 Access Points

The Alcatel-Lucent OAW-AP518 access points are high performance, multi-radio, outdoor access point 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 and 5 GHz 802.11ax Wi-Fi (Wi-Fi 6) functionality with MIMO radios (2x2 in 2.4 GHz, 4x4 in 5 GHz), while also supporting 802.11a, 802.11b, 802.11g, 802.11n, and 802.11ac wireless services.

The APs provide the following functionality:

- 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 and 1 Gbps respectively.
- Compatible with IEEE 802.3bt, IEEE 802.3at, and IEEE 802.3af PoE standards on both Ethernet ports.
- Mesh mode.
- Thermal Management.

For complete technical details and installation instructions, see*Alcatel-Lucent OAW-AP518 Access Point Installation Guide*.

Air Slice

Alcatel-Lucent's key RF differentiation, Air Slice, designed for 11ax APs optimizes user experience and assures QoA to enterprise applications. Air Slice combines AppRF and UCC for classifying applications and it also supports custom flow definitions. Air Slice uses a combination of priority queuing, dynamic WMM boosting, and 11ax based radio resource scheduling to prioritize enterprise applications in the presence of competing background traffic flows to meet latency and bandwidth requirements.

Air Slice is supported only on OAW-AP530 Series and OAW-AP535 access points. It is mandatory to enable DPI on the AP before configuring Air Slice, else an error will be reported.

The **wlan access-list session <acl>** list and **wlan access-rule <access_list>** list commands are modified based on the network configuration. When rule **action** is permitted, the rule can configure the new option **markapp** with **custom appid**.

AP Name Broadcast in Probe Responses

The **advertise ap-name** parameter in the **wlan ssid-profile** command will broadcast the AP name in probe responses. The existing functionality broadcasted the AP name only in beacon responses. This feature is supported on OAW-AP300 Series and OAW-AP500 Series access points running AOS-W Instant 8.7.0.0.

AP USB Management

AOS-W Instant supports new infrastructure to manage any USB device that is plugged to an AP. The infrastructure allows describing a USB device through either CLI configuration or by using predefined descriptors, USB device management through USB ACLs, and supports plugins for USB devices. The infrastructure supports sending notification to other processes and script-based notifications.

Automatic Update of CA Certificate Bundle

The OAW-IAP automatically checks for CA certificate bundle updates and installs the new version when it is available on Activate.

Disable Factory Reset When AP is Operational

A new CLI command **disable-factory-reset** is introduced to disable the factory reset feature when the AP is operational.

Enhancements for Wi-Fi Uplink Troubleshooting

The IP address, subnet mask, and gateway information of the layer 3 network are added to the output of **show wifi-uplink status** command. These information will enable you to easily troubleshoot issues with the Wi-Fi uplink.

Enhancements to the OAW-IAP Hostname

The number of ASCII characters allowed in the OAW-IAP hostname is increased from 32 to 128 characters. As a best practice, It is recommended to configure the hostname by using only **a**-**z**, **A**-**Z**, **0**-**9**, ‘**.**’, ‘**-**‘, ‘**:**’, ‘_’ , and not special characters such as '**#$%**'.

The following configuration settings do not support the new limit of 128 ASCII characters in AOS-W Instant 8.7.0.0:

- 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.

Intelligent Thermal Management

Intelligent Thermal Management dynamically adapts operations of the AP to reduce the internal temperature if it exceeds the maximum threshold. This feature is supported in OAW-AP570 Series, OAW-AP570EX Series, and OAW-AP518 access points.

Third Party Certificate Support for OAW-IAP Applications

A new certificate management method is introduced that enables installation and use of third party certificates for OAW-IAP applications. This feature is currently supported only in locally managed AOS-W Instant networks. This feature can be configured using the new WebUI and the CLI.

Security

Fast BSS Transition Support for WPA3

AOS-W Instant now supports Fast BSS Transition (802.1r) for the WPA3 modes in both tunnel-forwarding and decrypt-tunnel modes for all APs which support WPA3.

Local Multiple PSK Operating Mode

In the Local MPSK operating mode, you can define up to 24 pre-shared keys per SSID on the OAW-IAP without actually requiring an external policy engine like ClearPass Policy Manager. The PSKs may be assigned to different client devices to connect to the SSID with Local MPSK configured. These local PSKs would serve as an extension of the base pre-shared key functionality. Local MPSK only supports passphrases in the form of strings. It does not support passphrases in the form of hexa-decimal characters. The local MPSK mode is currently supported only on a **employee** type and **personal** sercurity level SSID.

A new CLI command **wlan-mpsk-local** is introduced to allow SSIDs to operate in the local MPSK mode.

Support for Diffie-Hellman Groups in Enhanced Open Security

AOS-W Instant now supports Diffie-Hellman Groups 20 and 21 in Enhanced Open Security.

Supported OAW-IAPs

The following table displays the OAW-IAP platforms supported in AOS-W Instant 8.7.0.0 release.

Table 3: *Supported OAW-IAP Platforms*

OAW-IAP Platform	Minimum Required AOS-W Instant Software Version
■ 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
■ 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

Table 3: *Supported OAW-IAP Platforms*

OAW-IAP Platform	Minimum Required AOS-W Instant Software Version
■ 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

Deprecated Instant APs

The following Instant APs are no longer supported from AOS-W Instant 8.7.0.0 onwards:

- OAW-AP210 Series — OAW-IAP214 and OAW-IAP215
- OAW-AP 220 Series — OAW-IAP224, OAW-IAP225, and OAW-IAP228
- OAW-AP270 Series — OAW-IAP274, OAW-IAP275, and OAW-IAP277
- RAP 155 Series — OAW-RAP155 and OAW-RAP155P

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_75772

Chapter 5
Resolved Issues

This chapter describes the issues resolved in this release.

Table 4: *Resolved Issues in AOS-W Instant 8.7.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-175124 AOS-175157 AOS-175158 AOS-177320 AOS-204018	—	The IAPmgr process crashed when the branch name was updated. The fix ensures that the IAPmgr process does not crash. 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-183995 AOS-198632	—	Clients connected to a guest WLAN SSID could not access the Internet. The fix ensures that clients can access the Internet as expected. This issue was observed in slave APs in AOS-W Instant clusters running AOS-W Instant 8.3.0.0 or later versions.	AOS-W Instant 8.3.0.0
AOS-184474 AOS-186793 AOS-186872 AOS-186971 AOS-189390 AOS-190362 AOS-192337 AOS-194239 AOS-194677 AOS-195037 AOS-195056 AOS-196378 AOS-197722 AOS-200468 AOS-201008 AOS-202766 AOS-205672	—	An AP crashed and rebooted unexpectedly. The log file listed the reason for this event as: **kernel panic: Rebooting the AP because of FW ASSERT**. Enhancements to the wireless driver resolved this issue. This issue was observed in OAW-AP300 Series access points running AOS-W Instant 8.3.0.6 or later versions.	AOS-W Instant 8.3.0.6

Table 4: *Resolved Issues in AOS-W Instant 8.7.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-186723 AOS-199062	—	The Ethernet link between the AP and the Switch went down when the **speed/duplex** configuration for the link was set to **100/full**. The fix ensures that the AP works as expected. This issue was observed in OAW-AP303H and OAW-AP365 access points running AOS-W Instant 8.3.0.0 or later versions.	AOS-W Instant 8.3.0.0
AOS-187847 AOS-203188	—	Some OAW-IAPs were broadcasting an SSID even though the AP was connected to a POE AF injector. The fix ensures that the AP does not broadcast the SSID. This issue was observed in OAW-AP365 and OAW-AP515 access points, running AOS-W Instant 8.5.0.0 or later versions.	AOS-W Instant 8.5.0.0
AOS-188123 AOS-202924	—	An OAW-IAP lost connectivity to the ALE server and failed to reconnect. The **show log system** command displayed the following error messages: ■ **ale: Warning: ale temp file reach the limit.** ■ **ale: ERROR! ale post timeout, delete last send temp file.** The fix ensures that the AP remains connected to the ALE server. This issue was observed in AOS-W Instant clusters running AOS-W Instant 8.6.0.0 or later versions.	AOS-W Instant 8.6.0.0
AOS-195046 AOS-201014 AOS-202245 AOS-203671 AOS-204328	—	An OAW-IAP crashed and rebooted unexpectedly. The log file listed the reason for the event as: AP **Reboot reason: External-WDT-reset.**The fix ensures that the AP does not crash and reboot unexpectedly. This issue was observed in OAW-AP510 Series access points, running AOS-W Instant 8.5.0.0 or later versions.	AOS-W Instant 8.5.0.0.
AOS-195564 AOS-196892 AOS-198878	—	A client lost its IP address when roaming. This issue occurred under the following scenarios: ■ When the client switched from the mesh portal AP to a mesh point AP, when no other client was connected to the mesh portal AP. ■ AOS-W Instant networks in which Client VLAN Assignment was set to **Dynamic** in the **Network > VLAN** tab of the webUI. The fix ensures that clients retain their IP address when roaming between APs. 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 8.7.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-196869 AOS-199431 AOS-199587 AOS-199592 AOS-201056 AOS-201192 AOS-201589 AOS-201803 AOS-201638 AOS-203260 AOS-203650	—	A OAW-AP510 Series access point crashed and rebooted unexpectedly. The log file listed the reason for the reboot as: **BadAddr:64690a3b303db3 PC:wlc_ mutx_bw_policy_update+0x408/0x28b8 [wl_v6] Warm-reset.** The fix ensures that AP works as expected. This issue was observed in OAW-AP510 Series access points running AOS-W Instant 8.6.0.0 or later versions.	AOS-W Instant 8.6.0.0
AOS-197715	—	RADIUS packets sent from the AP to the server exceeded the MTU limit and caused RADIUS timeout failure. The fix ensures that the RADIUS packets sent from the AP do not exceed the MTU limit. 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-197800 AOS-199464	—	Clients were unable to connect to an 802.1X enabled SSID when the software version was upgraded to AOS-W Instant 8.3.0.0 or later versions. This issue occurred when the external RADIUS server rejected the client's authentication request because of a service-type mismatch. The mismatch occurred because the AP sent RADIUS requests with service-type value of framed instead of login by default. The fix ensures that the default service-type for 802.1X RADIUS authentication is login. This issue was observed in APs running AOS-W Instant 8.3.0.0 or later versions. **NOTE:** For APs running AOS-W Instant 8.7.0.0 or later versions, the service-type of 802.1X RADIUS authentication can be changed back to framed using the **service-type-framed-user 1x** parameter in the **wlan auth-server <profile name>** command.	AOS-W Instant 8.6.0.0
AOS-198275	—	Clients were not redirected to the captive portal page for authentication when the **radius-reauth-interval** defined in the network profile expired. This issue occurred when both 802.1X authentication and captive portal authentication were enabled in the AOS-W Instant network. The fix ensures that clients are redirected to the captive portal page when the **radius-reauth-interva**l period expires. This issue was observed in APs running AOS-W Instant 8.3.0.7 or later versions.	AOS-W Instant 8.3.0.7

Table 4: *Resolved Issues in AOS-W Instant 8.7.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-198355	—	An AP did not connect to OmniVista 3600 Air Manager. This issue occurred in APs that used certificate based authentication to connect to OmniVista 3600 Air Manager. The fix ensures that APs connect to OmniVista 3600 Air Manager using certificate based authentication. This issue was observed in access points running AOS-W Instant 8.6.0.0 or later versions.	AOS-W Instant 8.6.0.0
AOS-198363	—	Clients were either unable to connect to the AP or were getting disconnected when the **SAPD process** over utilizes CPU memory. The fix ensures that clients connect to the access point as expected. This issue was observed in OAW-APAP-324 access points running AOS-W Instant 8.3.0.7 or later versions.	AOS-W Instant 8.3.0.7
AOS-198488 AOS-205955		An AP rebooted unexpectedly and set an **F** flag. Enhancements to the wireless driver resolved this issue. This issue occurred when an 801.1X client was connected to the AP in bridge mode or tunnel mode for wired 802.1X authentication. This issue was observed in OAW-AP205H and OAW-AP303H access points running AOS-W Instant 8.5.0.3 or later versions.	AOS-W Instant 8.5.0.3
AOS-198787 AOS-198929	—	Uplink preemption for IAP-VPN connections did not work as expected when the primary uplink of the AP failed. This issue occurred under the following conditions: ■ The primary uplink of the AP was **Cellular**. ■ The AP used a U730L modem for Internet connectivity. The fix ensures that uplink pre-emption works as expected. This issue was observed in OAW-AP303H Series access points running AOS-W Instant 8.5.0.4 or later versions.	AOS-W Instant 8.5.0.4
AOS-198931 AOS-204554	—	A slave AP failed to join the cluster after a software upgrade. This issue occurred when the software version of the cluster was upgraded from AOS-W Instant 8.4.0.0 or later versions to 8.6.0.0 or later versions. The fix ensures that the slave AP joins the cluster after software upgrade to AOS-W Instant 8.6.0.0 or later versions. 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-199041 AOS-199506 AOS-202191	—	A OAW-AP510 Series access point acting as mesh point AP failed to establish mesh link to the mesh portal AP. This occurred when **Wide Bands** and **Very High Throughput** were disabled on the AP. The fix ensures that the mesh link to the mesh portal AP is established as expected. This issue was observed in OAW-AP510 Series access points running 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 8.7.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-199151	—	Clients connecting to a slave AP in an AOS-W Instant cluster were not redirected to the captive portal splash page. This issue occurred because of an error that caused the slave AP to receive a wrong firewall rule. The fix ensures that clients are redirected to the captive portal splash page as expected. This issue was observed in OAW-IAP clusters running AOS-W Instant 8.6.0.1 or later versions.	AOS-W Instant 8.6.0.1
AOS-199449 AOS-203660	—	Few clients were unable to connect to an OAW-AP515 access point. This issue occured when the AP was upgraded to AOS-W Instant 8.6.0.2. The fix ensures that clients are able to connect to the AP as expected. This issue was observed in OAW-AP515 access points running AOS-W Instant 8.6.0.2 or later versions.	AOS-W Instant 8.6.0.2
AOS-199612 AOS-200367 AOS-200997 AOS-202745	—	Few APs in an AOS-W Instant cluster reported the status in OmniVista 3600 Air Manager as **Down** and the CLI of the AP was unresponsive during this period. The fix ensures that the AP reports the correct status to OmniVista 3600 Air Manager and the CLI of the AP works as expected. This issue was observed in AOS-W Instant clusters running AOS-W Instant 8.6.0.2 or later versions.	AOS-W Instant 8.6.0.2
AOS-199699	—	A mesh portal AP crashed and rebooted unexpectedly. The log file listed the reason for the reboot as: **Reboot caused by kernel panic: softlockup: hung tasks**. The fix ensures that the mesh portal AP works as expected. This issue was observed in mesh APs running AOS-W Instant 8.6.0.1 or later versions.	AOS-W Instant 8.6.0.1
AOS-200447	—	The **Destination NAT** rule for **SSH** traffic in the **Inbound Firewall** settings configured under **Configuration > Settings** was not enforced. The fix ensures that the destination NAT firewall rules for SSH traffic are enforced on the AP. 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-200707 AOS-200645	—	An AP sent master beacons with the Virtual Switch's IP address when the DHCP lease of the IP address assigned to the AP expired. This issue occurred when Virtual Switch IP was configured for the AP. The fix ensures that the AP procures a new IP address from the DHCP server when its IP address expires and uses that IP address to send master beacons instead of the Virtual Switch IP address. This issue was observed in APs running 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 8.7.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-200997	—	A OAW-RAP failed to connect to the Switch. This issue occurred under the following scenarios: ■ The OAW-RAP was converted from an OAW-IAP through an Activate rule. ■ The OAW-IAP was running AOS-W Instant 8.6.0.2 or later versions. The fix ensures that the OAW-RAP conversion works as expected and the OAW-RAP is able to connect to the Switch. 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-201638 AOS-202772	—	An AP failed to establish TLS connection with the RadSec server when a custom certificate was used. This issue occurred when the AP used the default device certificate instead of the custom certificate to connect to the RadSec server. The fix ensures that the AP established TLS connections using the custom certificate. 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-201901	—	An AP changed all access rules to **deny** when the configuration was restored through the CLI from a Windows TFTP server. This issue occurred when the Windows configuration retrieved from the TFTP server included newline (\n) and carriage return (\r) characters. The fix ensures that the AP restores old ACL rules 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-202115	—	An AP failed to download **ClearPass Root CA** certificate from the ClearPass Policy Manager server. This issue occurred when: ■ The AP was connected to the ClearPass Policy Manager server through a VPN concentrator. ■ The VPN connection failed during the download of **ClearPass Root CA** certificate. The fix ensures that the **ClearPass Root CA** is downloaded to the AP as expected. 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-202118	—	APs in a cluster reported high CPU usage and failed to service clients. The slave APs lost connectivity with the master AP during this period. This issue occurred when a network scan was running on the AOS-W Instantcluster. The fix ensures that network operations are not interrupted during scans. 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 8.7.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-202139 AOS-203595	—	Clients connecting to a guest SSID in an AOS-W Instant cluster were not redirected to the captive portal splash page. This issue occurred because the **inbound-firewall** rules contained a **deny all** rule, which caused the master AP to deny traffic from guest users. The fix ensures that clients connecting to the guest SSID are serviced 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-202857	—	Clients connecting to slave APs were unable to authenticate to the RADIUS server. The fix ensures that the RADIUS authentication is successful. This issue occurred due to an issue with the Broadcom archer driver. 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-203263	—	OAW-AP325 access points intermittently lost connectivity with OmniVista 3600 Air Manager when the AOS-W Instant software was upgraded from 6.5.4.12 or later versions to 8.3.0.0 or later versions. The fix ensures that the OAW-AP325 access points do not experience intermittent connectivity issues. This issue occurred in AOS-W Instant clusters managed by OmniVista 3600 Air Manager when the number of APs in the cluster exceeded the scalability limit. This issue was observed in OAW-AP325 access points running AOS-W Instant 8.3.0.0 or later versions.	AOS-W Instant 8.5.0.5
AOS-203766	—	Custom AirGroup service IDs were not saved in the WebUI. The fix ensures that the services IDs can be saved successfully. This issue occurred as the number of service IDs that can be saved on the AP had reached the maximum limit. 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-204556 AOS-205117	—	An OAW-IAP did not delete the **/state/ApInfo/radios/radio {34:fc:b9:7d:4d:60}/rssi/sta{84:d4:7e:c0:0d:41}/snr** record when the wireless client went offline. This issue occurred due to high CPU memory utilization. The fix ensures that the record is deleted. This issue was observed in APs running AOS-W Instant 8.4.0.6 or later versions.	AOS-W Instant 8.4.0.6

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 8.7.0.0.

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 8.7.0.0:

- 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.

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 8.7.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-198905	—	In a cluster deployment with 128 OAW-IAPs, all slave APs take approximately 30 minutes to join the cluster. This issue occurs when DTLS is enabled on the AOS-W Instant cluster and is observed in APs running AOS-W Instant 8.6.0.0 or later versions.	AOS-W Instant 8.6.0.0
AOS-200633	—	Users are unable to view the AOS-W Instant WebUI in Internet Explorer browser. A **Certificate Invalid** error message is displayed. This issue is observed in APs running AOS-W Instant 8.7.0.0.	AOS-W Instant 8.7.0.0

Table 5: *Known Issues in AOS-W Instant 8.7.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-203678	—	An OAW-IAP does not generate UCM call records. This issue occurs when data packets are fragmented due to low MTU on the client. This issue is observed in APs running AOS-W Instant 8.7.0.0. **Workaround:** Increase the MTU size on the client.	AOS-W Instant 8.7.0.0
AOS-205206	—	VoIP calls made from a SIP application are not getting prioritized and classified. This issue occurs when the opmode setting on the OAW-IAP is set to Open. This issue is observed in OAW-AP500 Series access points, running AOS-W Instant 8.7.0.0.	AOS-W Instant 8.7.0.0
AOS-207599 AOS-207665	—	The local WebUI for some access points does not work in the following scenarios and displays the error message **ERR_SSL_SERVER_CERT_BAD_FORMAT**: ■ The AP is new out-of-the-box and is in its factory default state with the AOS-W Instant 8.7.0.0 manufacturing build. ■ The web browser used to access the local WebUI is Google Chrome, Microsoft Edge 79 and later versions, or Apple Safari. This issue is observed in OAW-AP505H, OAW-AP570 Series, OAW-AP577, and OAW-AP518 access points shipped with the AOS-W Instant 8.7.0.0 software image. **Workaround:** Use either Internet Explorer, Microsoft Edge Legacy, or Mozilla Firefox web browsers to access the local WebUI. **NOTE:** This issue impacts all other AP platforms if they are rebooted in the factory default state after upgrading to AOS-W Instant 8.7.0.0.	AOS-W Instant 8.7.0.0

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.

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.

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 to achieve this goal. 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_8.7.0.x_xxxx
OAW-AP504, OAW-AP505, and OAW-AP505H	AlcatelInstant_Gemini_8.7.0.x_xxxx
OAW-IAP314, OAW-IAP315, OAW-IAP324, OAW-IAP325, OAW-AP374, OAW-AP375, OAW-AP377, OAW-AP318, and OAW-AP387	AlcatelInstant_Hercules_8.7.0.x_xxxx
OAW-IAP334 and OAW-IAP335	AlcatelInstant_Lupus_8.7.0.x_xxxx

Access Points	Image File Format
OAW-AP534, OAW-AP535, and OAW-AP535	AlcatelInstant_Scorpio_8.7.0.x_xxxx
OAW-AP303, OAW-AP303H, 303P Series, OAW-IAP304, OAW-IAP305, OAW-AP365, and OAW-AP367	AlcatelInstant_Ursa_8.7.0.x_xxxx
OAW-AP203H, OAW-AP203R, OAW-AP203RP, and OAW-IAP207	AlcatelInstant_Vela_8.7.0.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_8.7.0.x_xxxx
  - TFTP - tftp://<IP-address>/<image-file>. For example, tftp://<IP-address>/AlcatelInstant_Hercules_8.7.0.x_xxxx
  - FTP - ftp://<IP-address>/<image-file>. For example, ftp://<IP-address>/AlcatelInstant_Hercules_8.7.0.x_xxxx
  - FTP - ftp://<user name:password>@<IP-address>/<image-file>. For example, ftp://<alcatel:123456>@<IP-address>/AlcatelInstant_Hercules_8.7.0.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_8.7.0.x_xxxx
OAW-AP504, OAW-AP505, and OAW-AP505H	AlcatelInstant_Gemini_8.7.0.x_xxxx
OAW-IAP314, OAW-IAP315, OAW-IAP324, OAW-IAP325, OAW-AP374, OAW-AP375, OAW-AP377, OAW-AP318, and OAW-AP387	AlcatelInstant_Hercules_8.7.0.x_xxxx
OAW-IAP334 and OAW-IAP335	AlcatelInstant_Lupus_8.7.0.x_xxxx
OAW-AP534, OAW-AP535, and OAW-AP535	AlcatelInstant_Scorpio_8.7.0.x_xxxx
OAW-AP303, OAW-AP303H, 303P Series, OAW-IAP304, OAW-IAP305, OAW-AP365, and OAW-AP367	AlcatelInstant_Ursa_8.7.0.x_xxxx
OAW-AP203H, OAW-AP203R, OAW-AP203RP, and OAW-IAP207	AlcatelInstant_Vela_8.7.0.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_8.7.0.x_xxxx
  - TFTP - tftp://<IP-address>/<image-file>. For example, tftp://<IP-address>/AlcatelInstant_Hercules_8.7.0.x_xxxx
  - FTP - ftp://<IP-address>/<image-file>. For example, ftp://<IP-address>/AlcatelInstant_Hercules_8.7.0.x_xxxx
  - FTP - ftp://<user name:password>@<IP-address>/<image-file>. For example, ftp://<alcatel:123456>@<IP-address>/AlcatelInstant_Hercules_8.7.0.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_8.7.0.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_8.7.0.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 8.7.0.x

Before you upgrade an OAW-IAP running AOS-W Instant 6.5.4.0 or earlier versions to AOS-W Instant 8.7.0.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.