AOS-W Instant 8.6.0.0

Alcatel·Lucent
Enterprise

Release Notes

Contents

Revision History

The following table provides the revision history of this document.

Table 1: *Revision History*

Revision	Change Description
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 8.6.0.0.

Authentication

Blacklisting Unauthorized Users

Unauthorized users trying to login to the network as an administrator using invalid credentials can be blacklisted and blocked from attempting further logins into the system. The number of allowed invalid login attempts and the lock out time period can be configured by the administrator. Enabling this feature enhances the security and prevents malicious login attempts into the network.

Priority for Local Cache Authentication

Priority for Local Cache Authentication feature for wireless networks is based on the Authentication Survivability framework of AOS-W Instant. This feature when enabled authenticates clients using the local cache of the AP before sending a RADIUS request to the server. This feature is supported for clients authenticated using MAC and 802.1X Authentication.

Enhancement for Authentication Survivability

The Authentication Survivability feature is now supported for clients authenticated using MAC authentication.

RADIUS Accounting with MPSK

AOS-W Instant supports RADIUS accounting with multiple PSKs in conjunction with ClearPass Policy Manager for WPA2 PSK-based deployments. When RADIUS accounting is enabled and MPSK authentication is successful, the AP sends an accounting start message to the ClearPass Policy Manager server to gather the accounting updates. The accounting updates are periodically sent based on the time interval configured on the AP.

Support for 256-bit Encryption with WPA3 Enterprise in non-CNSA Mode

AOS-W Instant supports 256-bit encryption with WPA3 enterprise in non-CNSA mode.

ARM

Radio Mode Switching Enhancement

The following enhancements are introduced in relation to switching between the **Access**, **Monitor**, and **Spectrum Monitor** OAW-IAP radio modes:

- Switching between radio modes no longer requires an AP reboot to take effect.
- Switching between radio modes is not allowed when extended SSID is disabled on the AP.

Split 5GHz Radio for 550 Series Access Points

The split 5GHz radio is an AOS-W Instant feature that leverages the power of software to provide three radios on550 Series access points. The 8X8 5GHz radio of these access points can be converted into two 4X4 5GHz radios operating on the upper and the lower part of the radio antenna offering a total of three radios available for configuration - radio 0 (5GHz), radio 1 (2.4GHz) and radio 2 (5GHz).

Clarity

Improvements to the Clarity Live Station Inline Monitoring Messages

The monitoring and analysis capabilities of the STA inline monitoring messages have been improved. You can view the history of the passive STA and passive STA DNS statistics generated by inline monitoring by using the **show clarity history sta|sta-dns** commands.

Configuration

BSS Color Feature for OAW-AP510 Series, 530 Series, and OAW-AP535 Access Points

BSS coloring feature enhances the Wi-Fi experience by optimizing RF usage in dense deployment scenarios. The BSS color feature is supported with OAW-AP510 Series, 530 Series, and OAW-AP535 access points. BSS Color is configured in the radio profile settings of the access point.

Configuration of Additional NTP Servers for AOS-W Instant Access Points

AOS-W Instant access points now support configuration upto four NTP servers.

Configuration of Additional Syslog Servers for AOS-W Instant Access Points

AOS-W Instant access points now support configuration upto of three syslog servers.

Configuring Reconnect Duration for IAP-VPN Switch Failover

The connectivity between IAP and the Switch is monitored by a heartbeat signal between the OAW-IAP and the Switch. When the heartbeat fails the OAW-IAP fails over to the backup Switch. The duration after which the OAW-IAP fails over to the backup Switch in IAP-VPN connections can now be configured by the administrator.

Configuring a Static IP Address with Two DNS Servers

When configuring a static IP address on an OAW-IAP, you can define up to two DNS Servers separated by a comma. If the first DNS is unavailable, the second DNS server will take charge of resolving the DNS requests in its place.

Datapath

Support for WebRTC Prioritization

This feature prioritizes the media traffic from WebRTC sources. WebRTC prioritization provides better end user experience, dashboard visibility of all WebRTC applications like voice, video, and application sharing, and call quality monitoring for audio calls using upstream and downstream RTP analysis.

IoT

Configuring a Client Specific VLAN for IoT Telemetry

The IoT telemetry data is transported to multiple users using BLE. The telemetry data is parsed and sent to the server through WSS or HTTPS protocols. To ensure the telemetry data is seamlessly transported to the server, the telemetry traffic should be isolated to a client specific VLAN. and must not reside on the same VLAN used for the AP management traffic.

Proxy Server Configuration for IoT Transport Profiles

The proxy server configuration in an IoT transport profile allows you to send IoT data to a proxy server that can in turn relay the IoT data to its final destination. This is useful when you cannot establish a direct link with a server that is hosted in the cloud. The proxy server configuration includes the IP address and port number of the proxy sever and the optional username and password to log in to the proxy server.

Support for ABB Sensor

AOS-W Instant supports the following ABB sensors and forwards the IoT data from these sensors over Telemetry-HTTPS and Telemetry-websocket server types:

- Motor sensor
- Pump sensor
- Bearing sensor
- Ambient sensor
- ECM drive sensor
- CoMo sensor

Support for AmberBox Sensor

AOS-W Instant supports AmberBox detectors and gateways that connect to a USB port in an AP. The AP relays the traffic from the detector or gateway to the destination server.

Support for SES-Imagotag Cloud TLS Authentication

AOS-W Instant allows an AP with ESL USB dongle to connect to the SES cloud by using TLS authentication. This allows you to configure and update the ESL through the SES cloud.

Support for Hanshow USB Dongle

AOS-W Instant supports Hanshow USB dongles. A Hanshow dongle plugs into the USB port of an Alcatel-Lucent AP and transfers electronic shelf label data from computer, server, or cloud to electronic shelf label tags through the AP. The USB port of the AP works as a wired Ethernet port and supports bridge and tunnel modes.

Support for MySphera Tag

MySphera is a leading provider of BLE-based asset tracking tags and services. When a MySphera BLE tag broadcasts an advertisement, an AP obtains the RSSI information, computes the location of the tag, and relays the location information to a destination server. A new device class filter, MySphera that matches the server type Telemetry-HTTPS and Telemetry-Websocket to configure the MySphera data in the IoT transport profile.

Vendor Filter

The vendor filter is either the vendor name or the vendor ID of the IoT device. The vendor ID is a 2-byte hexadecimal value preceding with 0x in 0xABCD format. The vendor name is a string that can be either a full vendor name (example: Aruba) or a substring of the actual vendor name (example: Aru) and can be case-insensitive. Configure the vendor filter in the IoT transport profile. The vendor filter accepts up to five combinations of vendor names or vendor IDs separated by commas, for example:

- Aruba, Favendo, HanVit, SoluM, ABB
- 0xABCD, 0xBCDE, 0xCDEF, 0xDEF0, 0xEF01
- Aruba, 0xABCD, Favendo, 0xBCDE, HanVit

If more than one vendor name or vendor ID is configured, then any of the matching vendor names or vendor IDs in the vendor filter is applied. A vendor filter is reported only if the vendor data or vendor name is not empty and matches the vendor information configured in the IoT transport profile. If the vendor field is not populated for the IoT devices, the IoT devices are reported because there is not matching vendor filter in the IoT transport profile.

Wi-Fi RTLS and BLE Telemetry Streams

The Wi-Fi RTLS and BLE telemetry streams are combined into a single telemetry stream in the IoT transport profile. This optimizes the integration of telemetry streams with third party location engines.

Mesh

Fast Roaming on Mesh Access Points

AOS-W Instant supports fast roaming for APs deployed in a wireless mesh network. The mesh points for which fast roaming is enabled are called mobility mesh points. Fast roaming on mesh APs is required mainly in fast moving environments such as buses or the subway. To support fast roaming, mobility mesh points perform a scan of other mesh points in the background first and then choose the best neighbor to connect from all the neighbors. The background scan implies when mesh is connected, the mesh point collects information about surrounding channels through background scanning. The mobility mesh point scan time between radio channels is altered to be faster than the mesh point scan in a regular mesh

network. This feature is currently supported only on OAW-AP320 Series, OAW-AP305, OAW-AP315, OAW-AP370 Series, OAW-AP365, AP-328, and OAW-AP334 access points.

Platforms

500 Series Access Point

The 500 Series access points (AP-504 and AP-505) are high-performance, dual-radio wireless devices 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 2x2 MU-MIMO technology.

The APs provide the following capabilities:

- 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
- Compatibility with IEEE 802.3af PoE
- Integrated BLE radio

For complete technical details and installation instructions, see *Alcatel-Lucent 500 Series Access Points Installation Guide* .

Enhancements for Wi-Fi Uplink

The Wi-Fi uplink feature in AOS-W Instant 8.6.0.0 adds support for bridge mode using MAC Address Translation (MAT), 802.1X Authentication for 802.11ac AP platforms, IPv6 and Mesh configuration when 2.4 Ghz band is used for uplink.

Hardware Offloading for Increased Transmission Performance in OAW-AP535 and OAW-AP535 Access Points

The hardware offloading feature optimizes the transmission performance of access points by offloading established session flows to hardware forwarding from the datapath software. This feature is supported on OAW-AP535 and OAW-AP535 access points.

Support for Wireless Client Bridging

Allows you to configure the maximum number of IPv4 users for wireless client bridging. The default value is 2 and the maximum threshold value is 32 users.

Thermal Shutdown Support in Access Points

The Alcatel-Lucent 530 Series and 550 Series APs support operating temperatures of up to 50℃ (indoor) or 60℃ (outdoor). Starting from AOS-W Instant 8.6.0.0, these APs are enabled with thermal shutdown feature.

Uplink

Setting Uplink Wired Port VLAN

Starting from AOS-W Instant 8.6.0.0 release, the client traffic can be controlled to the uplink port and the traffic from downlink ports is not bridged or flooded to the uplink port automatically. By default, the client traffic from downlink port is still flooded to uplink port automatically.

Wi-Fi Driver

Multi Band Operation (MBO)

AOS-W Instant provides Agile Multiband support on 802.11ax capable APs. MBO enables the network to utilize the available spectrum efficiently, and helps in optimizing connectivity experience for the end-users.

This chapter describes the platforms supported in this release.

Supported OAW-IAPs

The following table displays the OAW-IAP platforms supported in this release.

Table 3: *Supported OAW-IAP Platforms*

OAW-IAP Platform	Minimum Required AOS-W Instant Software Version
■ 500 Series	AOS-W Instant 8.6.0.0 or later
■ 530 Series ■ 550 Series	AOS-W Instant 8.5.0.0 or later
■ OAW-AP303P ■ OAW-AP387 ■ OAW-AP510 Series — OAW-AP514 and OAW-AP515	AOS-W Instant 8.4.0.0 or later
■ OAW-AP303 Series ■ OAW-AP318 Series ■ OAW-AP340 Series — OAW-AP344 and OAW-AP345 ■ OAW-AP370 Series — OAW-AP374, OAW-AP375, and OAW-AP377	AOS-W Instant 8.3.0.0 or later
■ OAW-AP203H	AOS-W Instant 6.5.3.0 or later
■ OAW-AP203R and OAW-AP203RP ■ OAW-AP303H ■ OAW-AP365 and OAW-AP367	AOS-W Instant 6.5.2.0 or later
■ OAW-IAP207 ■ OAW-IAP304 and OAW-IAP305	AOS-W Instant 6.5.1.0-4.3.1.0 or later
■ OAW-IAP314 and OAW-IAP315 ■ OAW-IAP334 and OAW-IAP335	AOS-W Instant 6.5.0.0-4.3.0.0 or later

Table 3: *Supported OAW-IAP Platforms*

OAW-IAP Platform	Minimum Required AOS-W Instant Software Version
■ OAW-IAP324 and OAW-IAP325	AOS-W Instant 6.4.4.3-4.2.2.0 or later
■ OAW-IAP228 ■ OAW-IAP277	AOS-W Instant 6.4.3.1-4.2.0.0 or later
■ OAW-IAP214 and OAW-IAP215	AOS-W Instant 6.4.2.0-4.1.1.0 or later
■ OAW-IAP274 and OAW-IAP275	AOS-W Instant 6.4.0.2-4.1.0.0 or later
■ OAW-IAP224 and OAW-IAP225	AOS-W Instant 6.3.1.1-4.0.0.0 or later
■ OAW-RAP155 and OAW-RAP155P	AOS-W Instant 6.2.1.0-3.3.0.0 or later

Chapter 4
Regulatory Updates

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

Periodic regulatory changes may require modifications to the list of channels supported by an AP. For a complete list of channels supported by an AP using a specific country domain, access the 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_72905

This chapter describes the issues resolved in this release.

Table 4: *Resolved Issues in AOS-W Instant 8.6.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-146760 AOS-187344	179150	The memory in the wireless driver of an AP was corrupted. Enhancements to the wireless driver resolved the issue. 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-157343 AOS-186055	193800	A hidden mesh SSID was broadcast on the Wi-Fi network. The fix ensures that the mesh SSID is not displayed in the list of available networks. This issue was observed in OAW-IAPs running AOS-W Instant 8.4.0.1 or later versions.	AOS-W Instant 8.4.0.1
AOS-179882 AOS-191427	186851	An OAW-IAP crashed and entered a degraded state. This issue occurred when DPI was enabled on the OAW-IAP. The fix ensures that OAW-IAPs work as expected when DPI is enabled. This issue was observed in access points running AOS-W Instant 8.4.0.0 or later versions.	AOS-W Instant 8.4.0.0
AOS-176763 AOS-189443	171718	APs acting as mesh points were found to be forming a loop. This issue occurred due to change in the mesh interface name. The fix ensures that the looping issue is resolved. This issue was observed in OAW-IAPs running AOS-W Instant 8.4.0.0 or later versions.	AOS-W Instant 8.4.0.0
AOS-180490 AOS-185090	189842	Clients associated to an OAW-IAP were unable to access the internet intermittently. This issue occurred in OAW-IAPs configured with a static IP and the default gateway route of the was removed after an Ethernet flap. The fix ensures that the clients are able to access the internet seamlessly. This issue was observed in OAW-IAPs running AOS-W Instant 8.3.0.0 or later versions.	AOS-W Instant 8.3.0.0
AOS-180611 AOS-181158 AOS-183542 AOS-190040	190428 192504	Clients experienced frequent RADIUS connection failures. This issue occurred when DRP was enabled. The fix ensures that the OAW-IAP deletes only stale session entries related to these clients. This issue was observed in OAW-IAPs 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 8.6.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-181829	195194	The downstream traffic for a wireless client from the old VLAN was still sent to the old VLAN after the client changed over to a different VLAN and SSID on the same AP. The fix ensures that the downtream traffic is forward through the new VLAN. This issue is observed in OAW-IAPs running AOS-W Instant 8.4.0.0 or later versions.	AOS-W Instant 8.4.0.0
AOS-184780 AOS-190165 AOS-191082	—	An OAW-IAP forwarded DNS requests to the internal DNS server instead of the public DNS server configured. This issue occurred because the OAW-IAP performed dns-proxy for local DHCP clients irrespective of the VPN configuration status. The fix ensures that DNS requests are forwarded to the correct server as per the VPN configuration. This issue was observed in access points running AOS-W Instant 8.3.0.0 or later versions.	AOS-W Instant 8.3.0.0
AOS-185064	—	An OAW-IAP failed to stop the client from connecting to the Rogue AP. The fix ensures that the client does not connect to the Rogue AP. This issue was observed in OAW-IAPs running AOS-W Instant 8.3.0.0 or later versions.	AOS-W Instant 8.3.0.0
AOS-185411 AOS-185879	—	An OAW-IAP rebooted unexpectedly. The log file listed the following reason **Reboot caused by kernel panic: because of FW ASSERT([00] : 0x00000009)**. Enhancements to the software resolved the issue. This issue was observed in OAW-IAPs running AOS-W Instant 8.5.0.0.	AOS-W Instant 8.5.0.0
AOS-185951	—	The NTP logs displayed by the **show ntp debug** command did not refresh. The fix ensures that the latest NTP logs are displayed by the console. This issue was observed in OAW-IAPs running 8.5.0.0 or later versions.	AOS-W Instant 8.5.0.0
AOS-186192	—	Clients were experiencing connectivity issues when uplink vlan is configured and the clients were configured to receive IP from the Local or Distributed,L3 DHCP scope. This issue occurred when the uplink-vlan was configured and ARP table entry for default gateway of the master OAW-IAP ages out. The fix resolves the connectivity issues. This issue was observed in access points running AOS-W Instant 8.4.0.1 or later versions.	AOS-W Instant 8.4.0.1
AOS-187331 AOS-188142 AOS-188540 AOS-189168	—	An OAW-AP515 access point in an AOS-W Instant cluster did not detect nearby APs. Enhancements to the wireless driver resolved this issue. This issue was observed in OAW-AP515 access points running AOS-W Instant 8.4.0.0 or later versions.	AOS-W Instant 8.4.0.0

Table 4: *Resolved Issues in AOS-W Instant 8.6.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-187861 AOS-188751	—	Clients were unable to connect to the network. The fix ensures that clients can connect to the network as expected. This issue occurred in access points running AOS-W Instant running 8.3.0.0 or later versions.	AOS-W Instant 8.3.0.0
AOS-187929 AOS-193561 AOS-193434	—	The OAW-IAP did not switch primary uplink back to eth0 from secondary 3G/4G uplink when the Ethernet link was restored after a failover. The fix ensures that the primary uplink switches to the higher priority uplink, when the uplink is active. This issue was observed in access points running AOS-W Instant 8.4.0.2 or later versions.	AOS-W Instant 8.4.0.2
AOS-188451 AOS-190008	—	The mesh point selected an inferior mesh point as the next hop when better alternatives were available. This issue occurred due to incorrect path costs in the routing table. The fix ensures that the routing happens through the best option available. This issue was observed in access points running AOS-W Instant 8.3.0.0 or later versions.	AOS-W Instant 8.3.0.0
AOS-190211	—	Wired clients of an Ethernet interface experienced connectivity issues when other ethernet ports were shut down because of loop protection. The fix ensures that the Ethernet interface works as expected. This issue was observed in OAW-AP303H access points running AOS-W Instant 8.3.0.0 or later versions.	AOS-W Instant 8.3.0.0
AOS-190255	—	The IP address of the client was displayed in hexadecimal format in the debug logs. The fix ensures that the IP address of the clients is displayed in the decimal format. This issue was observed in access points running AOS-W Instant 8.4.0.2 or later versions.	AOS-W Instant 8.4.0.2
AOS-190335	—	Clients were unable to connect to Facebook Wi-Fi and received an **Authentication failed** message. The fix ensures that clients can connect to the Facebook Wi-Fi as expected. This issue was observed in access points running AOS-W Instant 8.3.0.0 or later versions.	AOS-W Instant 8.3.0.0
AOS-191329	—	The output of **show running-configuration** command did not include IPM configuration logs. The fix ensures that IPM configuration log is included in the output of show running-configuration command. This issue was observed in access points running AOS-W Instant 8.5.0.1 or later versions.	AOS-W Instant 8.5.0.1
AOS-192108	—	An OAW-IAP could not connect to Activate through a proxy using username and password. This issue occurred when the connecting proxy used the string **Connection Established** as the acknowledgment response. The fix ensures that theOAW-IAP connects to the proxy as expected. This issue was observed in access points 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 8.6.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-192817	—	An OAW-IAP failed to convert to a OAW-AP when both CPsec and PAPI enhanced security was enabled on the Switch. This issue occurred when the access point used static or DHCP discovery for provisioning. The fix ensures that the OAW-IAP converts to a OAW-AP as expected. This issue was observed in access points running AOS-W Instant 8.4.0.2 or later versions.	AOS-W Instant 8.4.0.2
AOS-193901	—	Samsung S10 devices were unable to authenticate into Guest SSIDs with **Enhanced Open** security. The fix ensures that Samsung S10 devices can authenticate into Guest SSIDs with Enhanced Open security. This issue was observed in access points running AOS-W Instant 8.4.0.2 or later versions.	AOS-W Instant 8.4.0.2
AOS-193977	—	Slave OAW-IAPs failed to sync configuration with the master OAW-IAP. This issue occurred due to a checksum error between the master AP and the slave AP that was triggered because of an issue in the uplink manager. The fix ensures that the configuration syncs as expected between the master and the slave APs. This issue was observed in OAW-AP318 and OAW-AP370 Series access points running AOS-W Instant 8.5.0.3 or later versions.	AOS-W Instant 8.5.0.3
AOS-194198	—	The OAW-IAP did not convert to a OAW-AP using Zero Touch Provisioning when both the ports of the access point were connected to the wired network. This issue occurred under the following conditions: ■ The network used IPv4 or IPv6 addresses. ■ The access point and the Switch were in the same VLAN. The fix ensures that the OAW-IAP converts to a OAW-AP as expected. This issue is observed in OAW-AP318, OAW-AP340 Series, OAW-AP370 Series, OAW-AP510 Series and 550 Series access points running AOS-W Instant 8.3.0.0 or later versions.	AOS-W Instant 8.3.0.0

This chapter describes the known issues and limitations identified in Alcatel-Lucent AOS-W Instant 8.6.0.0.

Important Update on OAW-AP210 Series, OAW-AP 220 Series, OAW-AP228, and OAW-AP270 Series Access Points

The OAW-AP210 Series, OAW-AP 220 Series, OAW-AP228, and OAW-AP270 Series access points will be deprecated for future releases and include the following limitations in AOS-W Instant 8.6.0.x, which is the last supported software version for these access points:

- No support for BLE interface (with USB)
- The DPI engine used for AppRF will have limitations in terms of enhancements and fixes in the future.
- These APs use WolfSSL libraries in AOS-W Instant 8.6.0.0 and not OpenSSL.
- No support for WPA3 security.

All of these platforms have already been marked as end-of-sale. Please review the end-of-sale and end-of-support dates for these platforms here.

OAW-AP535 Mesh Portal Limitation

The OAW-AP535 access points operating as a mesh portal reboot automatically when **split-5ghz-mode** is enabled.

Known Issues

The following known issues are observed in Alcatel-Lucent AOS-W Instant 8.6.0.0.

Table 5: *Known Issues in AOS-W Instant 8.6.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-185299 AOS-185381	—	The operational status of the eth0 and eth1 ports sent to OmniVista 3600 Air Manager is incorrect. This issue occurs when LACP is configured with an uplink switch on the OAW-IAP. This issue is observed in OAW-IAPs running AOS-W Instant 8.5.0.0 or later versions.	AOS-W Instant 8.5.0.0
AOS-186257 AOS-187250	—	The connection requests sent by the OAW-IAP to OmniVista 3600 Air Manager are failing. This issue occurs when the AP is set up in an Intranet environment and has multiple unreachable DNS server addresses configured. This issue is observed in access points running AOS-W Instant 8.4.0.0 or later versions.	AOS-W Instant 8.4.0.0
AOS-187646	—	The AP database show two records created for the same AP. This issue occurs when an OAW-AP375 OAW-IAP is converted to a OAW-AP. This issue is observed in OAW-AP375 access points running AOS-W Instant 8.6.0.0.	AOS-W Instant 8.6.0.0
AOS-187703	—	The client DHCP IP address is synched incorrectly in the L2 mobility response message. This issue occurs when **enforce-dhcp** fails to and **max-ipv4-users** are simultaneously enabled during L2 roaming. This issue is observed in OAW-IAPs running AOS-W Instant 8.6.0.0.	AOS-W Instant 8.6.0.0
AOS-187929	—	An OAW-IAP does not switch primary uplink back to eth0 from secondary 3G/4G uplink when the Ethernet link is restored after a failover. This issue is observed in OAW-IAPs running AOS-W Instant 8.6.0.0.	Alcatel-Lucent AOS-W Instant 8.6.0.0
AOS-189054 AOS-193754 AOS-193757	—	The system returns an error: **could not program ACL = 167, OOM** when the overall ACL entries configured on the OAW-IAP exceeds 8192 entries. This issue is observed in OAW-IAPs running AOS-W Instant 8.6.0.0.	AOS-W Instant 8.6.0.0
AOS-189217	—	Clients continue to send the accounting packets even after the session with the MPSK SSID has timed out. This issue is observed in OAW-IAPs running AOS-W Instant 8.6.0.0	Alcatel-Lucent AOS-W Instant 8.6.0.0
AOS-189249	—	Clients are unable to authenticate using credentials stored in the cache when the SSID uses both MAC and 802.1X authentication. This issue occurs when the authentication server is down and is observed in OAW-IAPs running AOS-W Instant 8.6.0.0.	Alcatel-Lucent AOS-W Instant 8.6.0.0

Table 5: *Known Issues in AOS-W Instant 8.6.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-189250 AOS-189251	—	The number of Datapath ACL entries exceeds the maximum configurable limit of 1024 entries. This issue occurs when **access-list session** and **eth profiles** are bound to the **access-rule profile** and each access-list contains 512 entries; and users are still able to create additional ACL entries. This issue is observed in OAW-IAPs running AOS-W Instant 8.6.0.0.	AOS-W Instant 8.6.0.0
AOS-189464	—	Wired accounting on the eth1 port does not work when hardware offloading is enabled on the OAW-IAP. This issue is observed in OAW-AP535 access points running AOS-W Instant 8.6.0.0.	Alcatel-Lucent AOS-W Instant 8.6.0.0
AOS-190089	—	The OAW-IAP classifies YouTube application traffic as UDP traffic and not as YouTube app traffic. This issue is observed in access points runningAOS-W Instant 8.3.0.10 or later versions.	Alcatel-Lucent AOS-W Instant 8.3.0.10
AOS-190183	—	Clients connecting to a guest SSID are able to access certain HTTP and HTTPS sites in the pre-auth role before taken to the splash page for authentication. This issue is oberved in access points running AOS-W Instant 8.3.0.0 or later versions.	AOS-W Instant 8.3.0.0
AOS-190510	—	Aruba Central??? does not identify OAW-IAPs and displays a **TCP connect error** message. This issue is observed in access points running AOS-W Instant 8.3.0.6 or later versions.	AOS-W Instant 8.3.0.6
AOS-191673	—	Clients accesing blocked sites are not redirected to the url defined in the **dpi-error-page-url** and the client browser returns a **Connection Reset** message. This issue is observed in access points running AOS-W Instant 8.3.0.0 or later versions.	AOS-W Instant 8.3.0.0
AOS-191920 AOS-192411	—	OpenSSL certificate authentication fails. This issue occurs because the internal free radius does not support ECDHE for openssl cipher. This issue is observed in OAW-IAP running AOS-W Instant 8.6.0.0.	Alcatel-Lucent AOS-W Instant 8.6.0.0
AOS-192061	—	Mesh points are disconnected from the mesh network when the Wi-Fi uplink is broken and are restored when the Wi-Fi uplink is restored. This issue occurs in mesh networks that use Wi-Fi as uplink. This issue is observed in access points running AOS-W Instant 8.6.0.0.	Alcatel-Lucent AOS-W Instant 8.6.0.0
AOS-192332	—	The Wi-Fi uplink status is shown as up when the WAN uplink is broken. This issue occurs when the Wi-Fi uplink is broken due to a channel change and the service AP is down. This issue is observed in access points using Wi-Fi uplink running AOS-W Instant 8.6.0.0.	Alcatel-Lucent AOS-W Instant 8.6.0.0

Table 5: *Known Issues in AOS-W Instant 8.6.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-193205	—	A factory default OAW-IAP removes the eth0 interface from the LACP configuration when connected to a LACP enabled Switch. This issue is observed in access points running AOS-W Instant 8.6.0.0.	Alcatel-Lucent AOS-W Instant 8.6.0.0
AOS-194703	—	An OAW-IAP occupies two DHCP leases when converted to a OAW-AP. This issue occurs when both Ethernet ports of the OAW-IAP are connected to the Switch. The first IP address is allocated during the OAW-IAP phase and the second IP address is allocated during the OAW-AP phase. This issue is observed in OAW-AP318 and OAW-AP370 Series access points running AOS-W Instant 8.5.0.0 or later versions. **Workaround:** Use any of the following workarounds: ■ Allocate a sufficiently large pool to cover the excess DHCP lease per AP. ■ Use a short-lived lease time during initial deployment. ■ Deploy APs in batches to prevent exhaustion of IP addresses in the DHCP pool.	Alcatel-Lucent AOS-W Instant 8.5.0.0
AOS-194736	—	The eth1 interface of the factory default AP does not connect to the uplink switch in the same VLAN as the eth0 interface and affects the Switch discovery process. This issue is observed in OAW-AP340 Series, OAW-AP510 Series, 530 Series and OAW-AP535 access points running AOS-W Instant 8.5.0.0 or later versions. **Workaround:** Disconnect eth1 from the uplink switch before logging into the CLI or WebUI, if LACP or active/ standby dual uplink mode is configured and factory reset the AP.	Alcatel-LucentAOS-W Instant 8.5.0.0
AOS-196109	—	Some slave OAW-IAPs are unable to join a cluster with DTLS enabled and keep attempting to reconnect. This issue is observed in OAW-IAPs running AOS-W Instant 8.6.0.0.	AOS-W Instant 8.6.0.0

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 Alcatel-LucentAOS-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-RAP155 and OAW-RAP155P	AlcatelInstant_Aries_8.6.0.x_xxxx
OAW-IAP214, OAW-IAP215, OAW-IAP224, OAW-IAP225, OAW-IAP228, OAW-IAP274, OAW-IAP275 and OAW-IAP277	AlcatelInstant_Centaurus_8.6.0.x_xxxx
OAW-IAP314, OAW-IAP315, OAW-IAP324, OAW-IAP325, OAW-AP374, OAW-AP375, OAW-AP377, OAW-AP318 and OAW-AP387	AlcatelInstant_Hercules_8.6.0.x_xxxx
OAW-IAP334 and OAW-IAP335	AlcatelInstant_Lupus_8.6.0.x_xxxx

Access Points	Image File Format
OAW-RAP108, OAW-RAP109,OAW-IAP103, OAW-IAP114 and OAW-IAP115	AlcatelInstant_Pegasus_8.6.0.x_xxxx
OAW-IAP204, OAW-IAP205 and OAW-IAP205H	AlcatelInstant_Taurus_8.6.0.x_xxxx
OAW-AP303, OAW-AP303H, 303P Series, OAW-IAP304, OAW-IAP305, OAW-AP365 and OAW-AP367	AlcatelInstant_Ursa_8.6.0.x_xxxx
OAW-AP203H, OAW-AP203R, OAW-AP203RP and OAW-IAP207	AlcatelInstant_Vela_8.6.0.x_xxxx
OAW-AP344, OAW-AP345, OAW-AP514 and OAW-AP515	AlcatelInstant_Draco_8.6.0.x_xxxx
OAW-AP534, OAW-AP535 and OAW-AP535	AlcatelInstant_Scorpio_8.6.0.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_8.6.0.x_xxxx
  - TFTP - tftp://<IP-address>/<image-file>. For example, tftp://<IP-address>/AlcatelInstant_Hercules_8.6.0.x_xxxx
  - FTP - ftp://<IP-address>/<image-file>. For example, ftp://<IP-address>/AlcatelInstant_Hercules_8.6.0.x_xxxx
  - FTP - ftp://<user name:password>@<IP-address>/<image-file>. For example, ftp://<alcatel:123456>@<IP-address>/AlcatelInstant_Hercules_8.6.0.x_xxxx

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

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

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-RAP155 and OAW-RAP155P	AlcatelInstant_Aries_8.6.0.x_xxxx
OAW-IAP214, OAW-IAP215, OAW-IAP224, OAW-IAP225, OAW-IAP228, OAW-IAP274, OAW-IAP275 and OAW-IAP277	AlcatelInstant_Centaurus_8.6.0.x_xxxx
OAW-IAP314, OAW-IAP315, OAW-IAP324, OAW-IAP325, OAW-AP374, OAW-AP375, OAW-AP377, OAW-AP318 and OAW-AP387	AlcatelInstant_Hercules_8.6.0.x_xxxx
OAW-IAP334 and OAW-IAP335	AlcatelInstant_Lupus_8.6.0.x_xxxx
OAW-RAP108, OAW-RAP109,OAW-IAP103, OAW-IAP114 and OAW-IAP115	AlcatelInstant_Pegasus_8.6.0.x_xxxx
OAW-IAP204, OAW-IAP205 and OAW-IAP205H	AlcatelInstant_Taurus_8.6.0.0_xxxx
OAW-AP303, OAW-AP303H, 303P Series, OAW-IAP304, OAW-IAP305, OAW-AP365 and OAW-AP367	AlcatelInstant_Ursa_8.6.0.x_xxxx
OAW-AP203H, OAW-AP203R, OAW-AP203RP and OAW-IAP207	AlcatelInstant_Vela_8.6.0.x_xxxx
OAW-AP344, OAW-AP345, OAW-AP514 and OAW-AP515	AlcatelInstant_Draco_8.6.0.x_xxxx
OAW-AP534, OAW-AP535 and OAW-AP535	AlcatelInstant_Scorpio_8.6.0.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_8.6.0.x_xxxx
  - TFTP - tftp://<IP-address>/<image-file>. For example, tftp://<IP-address>/AlcatelInstant_Hercules_8.6.0.x_xxxx
  - FTP - ftp://<IP-address>/<image-file>. For example, ftp://<IP-address>/AlcatelInstant_Hercules_8.6.0.x_xxxx
  - FTP - ftp://<user name:password>@<IP-address>/<image-file>. For example, ftp://<alcatel:123456>@<IP-address>/AlcatelInstant_Hercules_8.6.0.x_xxxx

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

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

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_8.6.0.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_8.6.0.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 8.6.0.x

Before you upgrade an OAW-IAP running AOS-W Instant 6.5.4.0 or earlier versions to AOS-W Instant 8.6.0.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.