AOS-W Instant 8.12.0.0

Release Notes

Copyright Information

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 AOS-W Instant release notes includes the following topics:

- What's New on page 7
- Supported Hardware Platforms on page 13
- Regulatory Updates on page 14
- Resolved Issues on page 15
- Known Issues and Limitations on page 23
- Upgrading an OAW-IAP on page 24

For the list of terms, refer to the Glossary.

Related Documents

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

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

Supported Browsers

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

Web Browser	Operating System
Microsoft Edge (Microsoft Edge 92.0.902.62 and Microsoft EdgeHTML 18.19041) or later	■ Windows 10 or later ■ macOS
Firefox 107.0.1 or later	■ Windows 10 or later ■ macOS
Apple Safari 15.4 (17613.1.17.1.13) or later	■ macOS
Google Chrome 108.0.5359.71 or later	■ Windows 10 or later ■ macOS

Terminology Change

As part of advancing HPE's commitment to racial justice, we are taking a much-needed step in overhauling HPE 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 HPE culture and moving forward, Alcatel-Lucent will replace racially insensitive terms and instead use the following new language:

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

Contacting Support

Table 2: *Contact Information*

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

Chapter 2
What's New

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

New Features and Enhancements

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

Short Supported Release

AOS-W Instant 8.12.0.0 is a Short Supported Release (SSR).

Enhancement for Configuring Non-DFS Channels

Starting with AOS-W Instant 8.12.0.0, when configuring access point control settings for the 5 GHz radio, a new checkbox named **Check All Non-DFS Channels** is available to select all Non-DFS channels at once in order to remove them from the allow-channel list. In the WebUI, this new checkbox can be found under **Configuration > RF > ARM > Show advanced options > Customize valid channels > Valid 5 GHz channels> Edit > Check All Non-DFS Channels**.

No Support for Air Slice in OAW-IAP Deployments

Starting with AOS-W Instant 8.12.0.0, Air Slice support will not be available. If Air Slice is enabled prior to the upgrade, it will be displayed as enabled in the configuration, but it will not take effect internally. The following commands have been impacted:

- **show datapath session dpi**
- **show datapath ipv6 session**
- **show datapath acl**
- **show datapath acl-rule**
- **airslice-policy**
- **show ap debug airslice client-stats**
- **show ap bss-table**

External Antenna Provision Support for 6 GHz

In AOS-W Instant 8.12.0.0, 6 GHz external antenna provision configuration is available in the radio settings of APs. The **external-antenna-6ghz** and **ant-pol-6ghz** commands have been included as a knob to properly configure 6 GHz external antenna gain.

Support for 6 GHz Configurations in REST APIs

AOS-W Instant 8.12.0.0 supports 6 GHz in REST APIs, which includes the addition of radio-profile-6ghz, utb-filter-block and rf-zone APIs, as well as new JSON parameters in ssid, channel and radio-state APIs. It also adds Norma and Leo as platforms to the allowed list of API upgrades.

Enhanced Debugging Experience in the Radio Profile

The **scheduler-mode** parameter is added to the radio profile in order to provide a better debugging experience. The parameter accepts two possible configurations, **fairness** and **latency**. The default parameter is set to **fairness**, which enables Traffic Allocation Framework (TAF) on the radio profile. The **latency** parameter disables TAF.

OAW-AP-584 Outdoor Operation is now Supported in France and Israel

The DRT information for OAW-AP-584 access points now complies with the regulatory guidelines that allow for outdoor operation in France and Israel.

Support for 670 Series Outdoor Access Points

The 670 Series access points (OAW-AP675, OAW-AP675EX, OAW-AP677, OAW-AP677EX, OAW-AP679, and OAW-AP679EX) are 802.11ax Wi-Fi 6E Outdoor Access Points that offer 2x2 MIMO radios, allowing for simultaneous tri-band operation. These APs also feature a wired 2.5 Gbps Smart Rate network interface and one SFP port for fiber support. If deployed with AOS-W Instant, the Alcatel-Lucent670 Series access points will only operate as a dual-band AP in the 2.4 GHz and 5 GHz radios. For 6 GHz operation, the APs require AOS-W 8.12.0.0 or later versions and deployments managed by a Mobility Conductor.

Additional features include:

- Data rates up to 2.4 Gbps
- Maximum Ratio Combining (MRC)
- Orthogonal Frequency Division Multiple Access (OFDMA)
- IoT-ready (integrated Bluetooth 5 and 802.15.4 radio for Zigbee support)
- Target Wake Time (TWT) for improved client power savings
- Advanced Cellular Coexistence (ACC)

Support for AP-605H Access Points

The AP-605H access point is a high-end dual-radio tri-band 2x2 MIMO 802.11ax WiFi 6E hospitality AP platform supporting concurrent operation in any two of the three supported bands (2.4 GHz, 5 GHz and 6 GHz). The mode of operation is configurable either manually or through AirMatch. Ideal for hospitality, branch, and teleworker use-cases, the AP-605H access points can be deployed in either controller-based (AOS-W) or controller-less (AOS-W Instant) network environments.

Additional features include:

- Flexible coverage across any two bands (2.4 GHz, 5 GHz, and 6 GHz) for up to 3.6 Gbps combined peak data rate.
- Up to seven 160 MHz channels in 6 GHz support low-latency, bandwidth-hungry applications like high-definition video and AR/VR applications.
- Combines wireless and wired access in compact desktop or wall mount model that can be PoE powered.
- Convenient wired connectivity and support for PoE with fast 2.5 GbE uplink port, two 1 GbE ports, and two 1 GbE PSE ports capable of supplying up to a total of 30W PoE.
- IoT-ready with integrated Bluetooth 5 and Zigbee.

Enhanced LLDP Information for Neighbor Devices

This enhancement enables users to access more detailed information about neighboring devices. The output of the **show ap debug lldp info** command has been upgraded to provide a richer set of data regarding neighboring devices. A new **remote_system_description** field in the command output now includes device information such as device model information, software version information, among others.

Enhanced Telemetry with New Radio, Client, and VAP Statistics

This release broadens our telemetry capabilities with the addition of new statistics for radios, clients, and virtual APs (VAPs). These new metrics provide deeper visibility into network performance, user experience, and the wireless environment. These new statistics are visible in the output of the commands **show ap debug radio-stats**, **show ap debug client-stats**, and **show ap debug bss-stats**.

Enhancements to the show audit-trail Command Output

This release introduces improvements to the **show audit-trail** command output to assist users in better diagnosing and understanding system events. The command now provides a more detailed and comprehensive output, offering deeper insights into system operations and changes. New output details:

- Member Receive Full Config Events
- Conductor Receive Delta Events
- Config Init Event with Reason
- System Time Change Events
- Capture Fail Reason for Command Execution.
- Reboot Event Logging

Tracking of Randomized MAC Addresses

This feature enables the tracking of probe requests from clients using randomized MAC addresses, offering deeper insights into client presence within the network infrastructure. This update is pivotal for businesses seeking advanced analytics in environments where understanding visitor behavior and network usage patterns is essential. New commands **laa-counter-msg** and **laa-counter-msg-interval** are introduced. Counters are sent to ALE using **profile default-ale**.

Virtual Access Point Configuration for 6 GHz in MBSSID Groups

This release introduces support for up to 8 Virtual Access Points (VAPs) on the 6 GHz radio. This update significantly expands the possibilities for network customization and segmentation, particularly beneficial for complex or high-density environments. The commands **show mbssid-group-profile**, **show mbssid-group-profile <profile name>**, **mbssid-group-profile <profile name>**, and **no mbssid-group-profile <profile name>** are introduced for visualizing and configuring MBSSID group profiles and their references to SSID profiles.

Ability to Specify Key Type When Using EST

A new option to select RSA-4096 key length and ECDSA certificates is available. We support two types of ECDSA keys and three types of RSA keys. For each type of RSA keys, two key lengths 2048 and 4096 are available. Selecting any of the following certificates will override the default RSA-2048:

- csr-attribute ecdsa-prime256v1-with-sha256
- csr-attribute ecdsa-prime384r1-with-sha384
- csr-attribute rsa-with-sha256 key-length <INT:key_length:2048,4096>

- csr-attribute rsa-with-sha384 key-length <INT:key_length:2048,4096>
- csr-attribute rsa-with-sha512 key-length <INT:key_length:2048,4096>

For complete technical details, see the *AOS-W Instant CLI Guide*.

New Counters for AP-Wired Client to Cloud

The feature reports the physical port's speed, duplex and error frames counter to the central in 8.12. In the output of show interface counters command, the following results are populated:

- CRC/FCS errors
- Collision errors
- Runts errors
- Giants errors

Auto-assign an EST Provisioned Certificate to the Wi-Fi Uplink

AOS-W Instant8.12.0.0 introduces the ability to auto-assign an EST received certificate to the Wi-Fi Uplink features, such that it can be used to support an EAP-TLS authentication. This implementation automatically renews the digital certificate that is about to expire, which solves the problem where the wifi1x function is not available if the certificate is not manually uploaded after it expires. The process to configure this feature is outlined below:

1. Connect the AP to the network through eth or another Wifi-uplink connection.
2. Configure the EST service on CPPM For complete technical details and installation instructions, see the CPPM User Manual
3. Configure an accessible EST server on the AP
4. Obtain all certificates through the EST server.

For complete technical details, see the AOS-W Instant User Guide.

Enhanced USB Dongle Firmware Upgrade for SES-Imagotag SCD

This release introduces an advanced feature for the SES-Imagotag SCD. This enhancement enables the capability for dongles to generate a Claim-ID, a critical component for establishing a secure connection to V:Cloud. This feature addresses the need for enhanced security in data communication between retail management systems and V:Cloud.

Port Bounce for Wired Clients on Instant Access Points

This release introduces a new feature for OAW-IAPs that automatically reinitiates DHCP requests following a VLAN change. This enhancement specifically affects wired non-802.1x clients in scenarios where there is a change in authorization events.

Deprecation of SHA-1 Cipher Suites for RadSec Server

The **radsec-ciphers-level <all|high>** parameter has been introduced under the **wlan auth-server** command. The parameter allows users to include or exclude SHA-1 cipher suites from the RadSec server.

Detection and Containment of Wi-Fi Direct Devices

The **detect-wifi-direct-p2p-groups**, **protect-wifi-direct-p2p-groups**, and **wifi-direct-network-quiet-time** commands have been introduced to detect and contain devices associated with Wi-Fi Direct groups under the IDS profile.

Vendor Specific IE based Containment

AOS-W Instant allows users to configure exclusions for IDS containment based on vendor specific IE information. This feature allows APs to be exempted from containment even when the devices use randomized MAC addresses. To exempt APs from containment, users should configure the vendor OUI and OUI type in the IDS unauthorized device profile. A maximum of five vendor OUI and OUI types can be defined for confinement exclusion.

Support for NTP Authentication Mode

AOS-W Instant allows users to configure Network Time Protocol (NTP) keys to authenticate servers. This feature can be configured through the CLI using the **ntp-authentication-key**, **ntp-trustedkey**, and **ntp-server-key** commands. The **show ntp authentication keys** and **show running-config | include ntp** commands list the details of the configured ntp authentication keys.

Enhancement to IDS Rogue Classification

Both wireless and wired MAC addresses are recorded for IDS rogue detection, thus ensuring that the OAW-IAP provides more details on IDS rogue classification to the user.

Support for SSL Throttling

SSL throttle can now be configured manually using the **set-sysctl ssl_throttle_table** command to a value between 1–32; the default value is 16. The **get-sysctl ssl_throttle_table** command can be used to view the configured SSL throttle value.

Firmware Synchronization Improvement in CoP for OAW-IAP Cluster with Different Models

AOS-W Instant 8.12.0.0 improves firmware synchronization in CoP for OAW-IAP cluster with different models.

Enhancement to debug pkt dump for Enforce DHCP Violation

The output for **debug pkt dump** includes information regarding packets drops that occur due to enforce DHCP violations.

VAP Creation in OAW-AP500 Series APs with New Toggle for GCM-256 Encryption

The **gcm-256-sw-encrypt-support** command has been introduced to enable/disable GCM-256 software encryption and allow for Virtual AP creation in both CNSA and non-CNSA SSIDs. This new configuration benefits those APs that do not support hardware encryption, like the OAW-AP510 Series and OAW-AP570 Series. By default, this configuration is **disabled**. So, it is important to note that if upgrading from AOS-W Instant 8.11.x to AOS-W Instant 8.12.x, GCM-256-based VAPs on the affected platforms will be disabled, and enabling the command will be required to configure them. Also, please be aware that software encryption has significantly lower performance than hardware encryption.

Behavioral Changes

This release does not introduce any changes in AOS-W Instant behaviors, resources, or support that would require you to modify the existing system configurations after updating to 8.12.0.0.

Chapter 3
Supported Hardware Platforms

The following table displays the OAW-IAP platforms supported in AOS-W Instant 8.12.0.x release.

Table 3: *Supported OAW-IAP Platforms*

OAW-IAP Platform	Minimum Required AOS-W Instant Software Version
670 Series — OAW-AP675, OAW-AP675EX, OAW-AP677, OAW-AP677EX, OAW-AP679, and OAW-AP679EX	AOS-W Instant 8.12.0.0
600 Series — AP-605H	AOS-W Instant 8.12.0.0
503 Series — OAW-AP503	AOS-W Instant 8.11.1.0 or later
503 Series — OAW-AP503	AOS-W Instant 8.11.1.0 or later
OAW-AP610 Series — OAW-AP615	AOS-W Instant 8.11.0.0 or later
OAW-650 Series — OAW-AP655	AOS-W Instant 8.10.0.0 or later
OAW-630 Series — OAW-AP635	AOS-W Instant 8.9.0.0 or later
OAW-500H Series — OAW-AP503H OAW-560 Series — OAW-AP565 and OAW-AP567	AOS-W Instant 8.7.1.0 or later
OAW-500H Series — OAW-AP505H OAW-518 Series — OAW-AP518 OAW-AP570 Series — OAW-AP574, OAW-AP575, and OAW-AP577 OAW-570EX 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-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-AP370 Series — OAW-AP374, OAW-AP375, and OAW-AP377	AOS-W Instant 8.3.0.0 or later
OAW-AP360 Series — OAW-AP365 and OAW-AP367	AOS-W Instant 6.5.2.0 or later
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	AOS-W Instant 6.5.0.0-4.3.0.0 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 Command Line Interface (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 networkingsupport.hpe.commyportal.al-enterprise.com.

The following DRT file version is part of this release:

- DRT-1.0_89073

Chapter 5
Resolved Issues

The following issues are resolved in this release.

Table 4: *Resolved Issues in AOS-W Instant 8.12.0.0*

Bug ID	Description	Reported Version
AOS-195769	In some OAW-IAPs set up with dynamic VLAN assignment, ARP or GARP traffic was unexpectedly sent to wireless clients, even if they were connected to a different VLAN and VAP. This issue was observed in the following scenarios: ■ When the broadcast packets from VLAN 1 and all of the clients on the SSID were on VLAN 2, the packets were sent to all VAPs belonging to the same SSID. ■ When the SSID had two VAPs that belong to the same VLAN, but only one VAP had clients on that VLAN, the traffic was forwarded to both VAPs. ■ When all of the VAPs of a given SSID have clients on different VLANs, the packets were broadcasted to all VLANs. The fix ensures that GARP traffic function as expected. This issue was observed in Instant APs running AOS-W Instant 8.6.0.0 or later versions.	AOS-W Instant 8.6.0.0
AOS-215025	Information was missing from the output of the **show ap dot11k-beacon-report** and **show ap dot11k-stat** commands when the **dot11k** setting was enabled on an OAW-IAP. The fix ensures that the **show ap dot11k-beacon-report** and **show ap dot11k-stat** commands function as expected when the **dot11k** setting is enabled. This issue was observed in APs running AOS-W Instant 8.4.0.0 or later versions.	AOS-W Instant 8.6.0.6
AOS-231129	AOS-W Instant APs did not send the cold and warm SNMP traps when expected. THe fix ensures that the APs function as expected. This issue was observed in APs running AOS-W Instant 8.0.0.0 or later versions.	AOS-W Instant 8.6.0.8
AOS-234042 AOS-234060 AOS-236584	Some OAW-IAPs in a cluster crashed and rebooted unexpectedly. The log file listed the reason for reboot as: **Reboot Time and Cause: AP Reboot reason: Some Crash Warm-reset**. The fix ensures that the APs function as expected. This issue was observed in OAW-AP345 access points running AOS-W Instant 8.6.0.16 or later versions.	AOS-W Instant 8.6.0.16
AOS-236052	An OAW-IAP did not update its IP address and retained its original IP address. This issue occurred when the AP switched to a different VLAN using ClearPass. The fix ensures the IP address of the AP is updated as expected. This issue was observed in APs running AOS-W Instant 8.7.1.3 or later versions.	AOS-W Instant 8.7.1.3
AOS-237132	The MSS value did not change when the data packets were routed through the IAP-VPN tunnel. This issue occurred when PPPoE uplink was configured. The fix ensures that the correct MSS value is displayed. This issue was observed in APs running AOS-W Instant 6.4.3.4-4.2.1.0 or later versions.	AOS-W Instant 6.4.3.4-4.2.1.0

Table 4: *Resolved Issues in AOS-W Instant 8.12.0.0*

Bug ID	Description	Reported Version
AOS-237413	High memory utilization was observed in a cluster consisting of APs. The issue occurred in environments where the SNMP server did not have **username** field in trap inform response message, which caused the process memory leak. This issue was observed in Instant AP clusters running AOS-W Instant 8.6.0.18 or later versions.	AOS-W Instant 8.6.0.18
AOS-237750 AOS-239650	An OAW-IAP crashed and rebooted when pre-auth roles was not configured and DPI was enabled. The log file listed the reason for the reboot as **BadPtr: 00000000 PC: strncpy+0xc/0x28 Warm-reset**. The fix ensures that the AP does not crash when pre-auth roles are not configured. This issue was observed in APs running AOS-W Instant 8.10.0.0 or later versions.	AOS-W Instant 8.10.0.4
AOS-237859 AOS-237874	OAW-IAPs experienced connectivity issues in an environment where both wifi-uplink and mesh links coexisted in the same radio. The fix ensures the mesh link moves to a non-interfering band in this scenario. For example: ■ wifi-uplink on band **a** and mesh link operates in 5 GHz or 6 GHz bands. Mesh link will connect to the 6 GHz band. ■ wifi-uplink on 6 GHz, and mesh link operates in 5 GHz or 6 GHz bands. Mesh link will connect to the 5 GHz band. ■ wifi-uplink and mesh -band are on 6 GHz , mesh will go to 5 GHz This issue was observed in access points running AOS-W Instant 8.11.0.0 or later versions.	AOS-W Instant 8.11.0.0
AOS-237965 AOS-237699	View-only users were unable to perform debug operations. This issue occurred when the user was able to log in while the OAW-IAP was in a degraded state. The fix ensures that view-only users are able to perform debug operations. This issue was observed in APs running AOS-W Instant 8.10.0.2 or later versions.	AOS-W Instant 8.10.0.2
AOS-238137	The **traceroute** command returned the following error message: **Can't find tsgw src ip**. This issue occurred when the OAW-IAP had multiple routing entries in the routing profile. The fix ensures that the **traceroute** command functions as expected. This issue was observed in APs running AOS-W Instant 8.10.0.3 or later versions.	AOS-W Instant 8.10.0.3
AOS-238198	Some OAW-IAPs took longer than expected to apply uplink band configurations. The fix ensures the OAW-IAPs work as expected. This issue was observed in OAW-IAPs running AOS-W Instant 8.11.0.0 or later versions.	AOS-W Instant 8.11.0.0
AOS-238228	Client devices experienced network connectivity issues intermittently. This issue occurred when: ■ An OAW-IAP was in Wi-Fi uplink dot1x mode. ■ The AP attempted to connect with a device having a reauthentication configuration. The fix ensures that the clients can connect to the network seamlessly. This issue was observed in OAW-AP303H access points running AOS-W Instant 8.7.1.8 or later versions.	AOS-W Instant 8.7.1.8

Table 4: *Resolved Issues in AOS-W Instant 8.12.0.0*

Bug ID	Description	Reported Version
AOS-238326	An OAW-IAP crashed and rebooted due to high memory utilization. The log file listed the reason for the event as **Reboot caused by kernel panic: MemLeak: mem low for 60 seconds, under 0MB 10 times, MB free 11 (4%), total 247**. The fix ensures that the AP functions as expected. This issue was observed in APs with less than 256 MB RAM and OAW-AP203H access points running AOS-W Instant 8.6.0.18 or later versions.	AOS-W Instant 8.6.0.18
AOS-238393	HE clients were unable to pass traffic when the SSID was configured with WPA3 enterprise encryption. The fix ensures that HE clients are able to pass traffic when WPA3 enterprise encryption is configured for the SSID. This is issue was observed in OAW-AP500 Series and OAW-AP510 Series access points running AOS-W Instant 8.11.0.0 or later versions.	AOS-W Instant 8.11.0.0
AOS-238447	Some OAW-AP303Haccess points crashed when a USB LTE modem was connected. The fix ensures the AP works as expected in this scenario. This issue was observed in APs running AOS-W Instant 8.11.1.0 or later versions.	AOS-W Instant 8.11.1.0
AOS-238535 AOS-240748	The output of the **show dpi-app stats full** command displayed incorrect values when the command was executed after a 15 minute interval. The fix ensures that the correct values are displayed when the **show dpi-app stats full** command is executed. This issue was observed in APs running AOS-W Instant 8.6.0.19 or later versions.	AOS-W Instant 8.11.0.0
AOS-238808	An OAW-IAP was unable to form a mesh link at the 60 GHz and was denylisted. The fix ensures that the 60 GHz connection was formed by default. This issue was observed in OAW-AP387 access points running AOS-W Instant 8.6.0.19 or later versions.	AOS-W Instant 8.6.0.19
AOS-239368	OAW-IAPs in a cluster did not retain the configured CPPM username and password. This issue occurred when the APs were rebooted while the password exceeded 23 characters. The fix ensures that the APs retain the configured CPPM username and password. This issue was observed in APs running AOS-W Instant 8.9.0.2 or later versions.	AOS-W Instant 8.9.0.2
AOS-239411	OAW-IAPs did not accept the serial number of the device as the default password after a factory reset. This issue occurred when the AP was reset using the **factory reset** command in AP boot mode. The fix ensures that the AP accepts the serial number as the default password after a factory reset. This issue was observed in APs running AOS-W Instant 8.9.0.0 or later versions.	AOS-W Instant 8.10.0.0
AOS-239419 AOS-238100	The eth0 link of an OAW-IAP appeared offline in the OmniVista 3600 Air Manager UI. The fix ensures that the eth0 link status is displayed correctly in the OmniVista 3600 Air Manager UI. This issue was observed in OmniVista 3600 Air Manager-managed APs running AOS-W Instant 8.6.0.18 or later versions.	AOS-W Instant 8.6.0.18
AOS-239919	An OAW-IAP connected to a switch port with single stack IPv6 VLAN was unable to obtain DHCPv6 addresses. This caused the AP to revert to IAP mode. The fix ensures that the IPv6 process for obtaining the DHCPv6 addresses is restarted if the AP fails to obtain the addresses. This issue was observed in APs running AOS-W Instant 8.10.0.1 or later versions.	AOS-W Instant 8.10.0.2

Table 4: *Resolved Issues in AOS-W Instant 8.12.0.0*

Bug ID	Description	Reported Version
AOS-240114	Client traffic was not forwarded by an OAW-IAP. This issue occurred when the **deny-intra-vlan-traffic** was enabled and VRRP was configured on the upstream default router. This issue was observed in OAW-IAPs running AOS-W Instant 8.10.0.6 or later versions. The fix ensures that users are able to pass client traffic.	AOS-W Instant 8.11.0.0
AOS-240139	An OAW-IAP in a cluster did not generate an SNMP trap when rogue APs were detected. The fix ensures that the AP generates SNMP traps when rogue APs are present. This issue was observed in APs running AOS-W Instant 8.7.0.0 or later versions.	AOS-W Instant 8.10.0.4
AOS-240180	An OAW-IAP was unable to resolve the FQDN. This issue occurred when the AP DNS packet failed to skip the default tunnel route when **Dynamic DNS** was enabled in the DHCP profile. The fix ensures that the AP DNS packet does not skip the default tunnel route even if **Dynamic DNS** was enabled. This issue was observed in APs running AOS-W Instant 8.10.0.3 or later versions.	AOS-W Instant 8.10.0.3
AOS-240266	An OAW-IAP rejected association requests. The log file listed the reason as: **AP is resource constrained-Max Clients Associated**. This issue occurred even though there were no clients associated with the AP. The 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 8.10.0.3
AOS-240398	Wireless users did not receive IP addresses from the DHCP server when the software version of OAW-IAPs was upgraded to AOS-W Instant 8.6.0.19 or later. The fix ensures that users receive IP addresses from the server when the AP boots up. This issue was observed in APs running AOS-W Instant 8.6.0.19 or later versions.	AOS-W Instant 8.6.0.19
AOS-240459	Static IP addresses of locally managed OAW-IAPs were changed to DHCP IP addresses if the configured default gateway was unreachable. The fix ensures that the IP address configuration does not change when the default gateway is unreachable. This issue was observed in APs running AOS-W Instant 6.5.0.0 or later versions.	AOS-W Instant 6.5.4.20
AOS-240507	The output of the **iftype** command displayed incorrect SNMP values. The fix ensures that the **iftype** command displays the correct SNMP values. This issue was observed in APs running AOS-W Instant 8.6.0.0 or later versions.	AOS-W Instant 8.7.1.11
AOS-240530	OAW-IAPs returned the following error message **auth_cppm_instant.c, auth_cppm_transform:1859: Dldb Role pf_iap_dur-3008-26: Buffer too large**. This issue occurred when the buffer size of the downloadable user role sent from the ClearPass Policy Manager exceeded 16 KB. The fix ensures that the AP functions as expected. This issue was observed in APs running AOS-W Instant 8.10.0.0 or later versions.	AOS-W Instant 8.10.0.4
AOS-240727	The DHCP server failed to start with the correct interface. The server also did not issue IPv4 or IPv6 addresses in the guest or DHCP scope defined VLANs. The fix ensures that the DHCP server starts with the correct interface. This issue was observed in APs running AOS-W Instant 8.10.0.0 or later versions.	AOS-W Instant 8.11.0.1

Table 4: *Resolved Issues in AOS-W Instant 8.12.0.0*

Bug ID	Description	Reported Version
AOS-240805	Users were unable to upgrade the software version of OAW-AP635 and OAW-AP655 access points using REST API. The fix ensures that the software upgrades using REST API are successful for OAW-AP635 and OAW-AP655 access points. This issue was observed in APs running AOS-W Instant 8.10.0.0 or later versions.	AOS-W Instant 8.11.0.0
AOS-241109	The backup SSID was enabled when internet connectivity went down. However, the backup SSID was still enabled when the internet connectivity was restored. This issue occurred as the device statistics were not cleared automatically. The fix ensures that the backup SSID is disabled when internet connectivity is restored. This issue was observed in APs running AOS-W Instant 8.10.0.5 or later versions.	AOS-W Instant 8.10.0.5
AOS-241197	An OAW-IAP generated **sapd** core during boot up. The fix ensures that the APs work as expected. This issue was observed in OAW-AP575 access points running AOS-W Instant 8.10.0.5 or later versions.	AOS-W Instant 8.10.0.5
AOS-241203	High memory utilization was reported on some OAW-IAPs because the AWC process was consuming high memory. This caused the APs to become unresponsive. The fix ensures that the APs function as expected. This issue was observed in APs running AOS-W Instant 8.10.0.0 or later versions.	AOS-W Instant 8.10.0.0
AOS-241395	Some OAW-IAPs repeatedly formed a connection with PAN firewall despite there being no user connected to the APs. The fix ensures that the APs function 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-241743 AOS-242212 AOS-244549	Users were unable to connect to the cloud guest SSID, and were being redirected to the Captive Portal page. The log file listed the following reason for the error: **Internal Error while getting request ID in radsec server**. The fix ensures that users are able to connect to cloud guest SSID without issues. This issue was observed in APs running AOS-W Instant 8.10.0.5 or later versions.	AOS-W Instant 8.10.0.6
AOS-242008	OAW-IAPs crashed and rebooted unexpectedly. The log file listed the reason for reboot as **Reboot caused by kernel panic: assert**. The fix ensures that the APs function as expected. This issue was observed in AP running AOS-W Instant 8.10.0.0 or later versions.	AOS-W Instant 8.10.0.5
AOS-242056	A delay in IDS to classify OAW-IAPs as rogue was observed in OAW-AP535 access points running AOS-W Instant 8.10.0.5 or later versions. This issue occurred because the time taken to detect the rogue AP included the scanning duration time. This issue was fixed by changing the rogue classification delay from monitored time to discovered time.	AOS-W Instant 8.10.0.5
AOS-242249 AOS-244271	Multiple client devices connected to OAW-IAP315 access points were not obtaining an IP address. After rebooting the AOS-W Instant APs, the client's devices obtained the IP address. This was caused by a memory leak when DMO was enabled and air-time-fairness-mode config preferred-access. The fix ensures the AOS-W Instant APs perform as expected. This issue was observed in OAW-IAP315 access points running AOS-W Instant 8.9.0.2 or later versions.	AOS-W Instant 8.10.0.5

Table 4: *Resolved Issues in AOS-W Instant 8.12.0.0*

Bug ID	Description	Reported Version
AOS-242512	The dynamic TACACS proxy authentication process did not work as expected in APs running AOS-W Instant 8.11.0.1 or later versions. The fix ensures this process works as intended.	AOS-W Instant 8.11.0.1
AOS-242628	The **MIB_WLAN_INDEX** entry displayed an incorrect value in **MIB_WAP_TABLE**. As a result, the correct ESSID of the OAW-IAPs were not displayed in the OmniVista 3600 Air Manager WebUI. The fix ensures that the correct ESSID names are displayed. This issue was observed in OmniVista 3600 Air Manager managed OAW-IAP clusters running AOS-W Instant 8.3.0.0 or later versions.	AOS-W Instant 8.3.0.0
AOS-242732	AOS-W Instant 802.11ax access points experienced a noticeable performance drop when the **air-time-fairness** setting was set to **fair-access** instead of **default-access**. The issue was related to the **air-time-fairness** feature not being compatible with modern APs. The fix ensures this configuration does not impact newer APs negatively. This issue was observed in APs running AOS-W Instant 8.10.0.0 or later versions.	AOS-W Instant 8.10.0.0
AOS-242779	In some APs running AOS-W Instant 8.10.0.6 or later versions, a **Check sum mismatch** error was displayed. The issue occurred when the MPSK key name included a space. The fix ensures the correct checksum value is displayed.	AOS-W Instant 8.10.0.6
AOS-242841 AOS-250716 AOS-247907	In some cases, AppRF displayed unreliable aggregated statistics after a long period of time. The fix ensures the AppRF aggregated statistics are accurate. This issue was observed in APs running AOS-W Instant 8.6.0.0 or later versions.	AOS-W Instant 8.11.1.0
AOS-243184	An OAW-IAP displayed incorrect country codes in the air captured packet, although the correct country code was configured on the AP. The fix ensures that the configured country codes are displayed in the air capture packet. This issue was observed in APs running AOS-W Instant 8.10.0.5 or later versions.	AOS-W Instant 8.10.0.5
AOS-244068	The containment feature was not effectively functioning for clients connected across various channels. The fix ensures the feature works as expected. This issue was observed in IAP-505 running AOS-W Instant 8.10.0.0 or later versions.	AOS-W Instant 8.10.0.0
AOS-244640	Users were unable to perform EAP-TLS authentication when a custom certificate was used. 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 8.11.1.0
AOS-244876	The output of the **show ap regulatory** command was missing from the tech-support supplemental. The fix ensures that the output of the **show ap regulatory** command is included in the tech-support supplemental. This issue was observed in APs running AOS-W Instant 8.6.0.0 or later versions.	AOS-W Instant 8.11.0.1

Table 4: *Resolved Issues in AOS-W Instant 8.12.0.0*

Bug ID	Description	Reported Version
AOS-245417	Some access points configured as a mesh portal transmitted at reduced power levels despite being set to full power. The issue was observed after the APs were rebooted and powered up with the 5 GHz band disabled under all WLAN profiles. The fix ensures the APs work as expected. This issue was observed in OAW-AP575 access points running AOS-W Instant 8.10.0.6 or later versions.	AOS-W Instant 8.10.0.6
AOS-246408	The **aiRadioChannel** parameter of the MIB node did not include details about the 40 MHz, 80 MHz, and 160 MHz channels. The fix ensures that the information appears as expected. 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-246617	After upgrading to AOS-W Instant 8.10.0.7, some OAW-IAPs crashed and rebooted unexpectedly, disconnecting every 2-3 hours due to IPv6 packet synchronization problems. The crash logs listed the reason for the error as **Panic:Ktrace core monitor: cpu3 hung for 45 seconds, hung cpu count: 1 Warm-reset.** The fix ensures that the APs work as expected. This issue was observed in OAW-AP515 access points running AOS-W Instant 6.5.4.0 or later versions.	AOS-W Instant 8.10.0.7
AOS-246735 AOS-246633 AOS-247461	Some access points crashed with reason **BadAddr:ffffffc133b1e424 PC:memcmp+0xd0/0x1c0 Warm-reset.** The fix ensures Instant APs work as expected. This issue was observed in OAW-AP515 and OAW-AP575 access points running AOS-W Instant 8.10.0.0 or later versions.	AOS-W Instant 8.10.0.0
AOS-247151	The output of the **show backup-config** command did not include configuration details for OAW-AP635 access points. The fix ensures that the output of the **show backup-config** command includes the configuration details. This issue was observed in OAW-AP635 access points running AOS-W Instant 6.5.4.0 or later versions.	AOS-W Instant 8.11.1.0
AOS-247318 AOS-249944	OAW-IAPs crashed unexpectedly when the **show ap debug radius-statistics** command was executed. The command returned the following error message: **Module AP STM Low Priority is busy**. The fix ensures that the **show ap debug radius-statistics** command functions as expected. This issue was observed in APs running AOS-W Instant 8.10.0.0 or later versions.	AOS-W Instant 8.10.0.8
AOS-247394	While running the **show auth-survivability cache-info** command, the username displayed random characters for strings longer than 16 characters. The fix ensures the usernames are displayed correctly. This issue was observed in some OAW-IAPs runningAOS-W Instant 6.5.4.0 or later versions.	AOS-W Instant 6.5.4.0
AOS-248170 AOS-205658	Some APs became virtual Switches after experiencing a power outage. The issue occurred when the uptime beacon protocol was designed in 32 bits instead of 64 bits, and the uptime was less than 300 seconds. The fix ensures the APs work as expected. This issue was observed in access points running AOS-W Instant 8.10.0.6 or later versions.	AOS-W Instant 8.10.0.6
AOS-248634	OAW-IAPs randomly generated the following error message: **An internal system error has occurred at file cli_swarm.c function get_user_acct_counters_ctx line 34902**. The fix ensures that the APs do not generate random error messages. This issue was observed in APs running AOS-W Instant 8.11.2.0 or later versions.	AOS-W Instant 8.11.2.0

Table 4: *Resolved Issues in AOS-W Instant 8.12.0.0*

Bug ID	Description	Reported Version
AOS-249004	The **Cellular Status** and **USB Modem Information** tables were missing from the output of the **show cellular status** command. The fix ensures that the output includes the **Cellular Status** and **USB Modem Information** tables. This issue was observed in OAW-IAPs running AOS-W Instant 8.10.0.0 or later versions.	AOS-W Instant 8.11.2.0
AOS-249437 AOS-250853	Mesh point OAW-IAPs failed to connect to the portal and the portal failed to update the channel bandwidth to the configured value. This issue occurred when: ■ **no 80mhz-support** was configured under the ARM profile. ■ **mesh-band 6ghz** was configured. The fix ensures that the mesh point APs function as expected. This issue was observed in APs running AOS-W Instant 8.10.0.0 or later versions.	AOS-W Instant 8.11.2.1
AOS-249817	The AP BLE antenna was not able to scan. The issue occurred if the AP was broadcasting the SSID on Wi-Fi channel 11 or Wi-Fi channel 1. The fix ensures the AP works as expected. This issue was observed in OAW-AP635 access points running AOS-W Instant 8.11.2.0 or later versions.	AOS-W Instant 8.11.2.0
AOS-250160 AOS-250315	The **Non-DTLS Members** parameter changed to **Deny** on the **Configuration > System** page when the WebUI was refreshed. However, the output of the **show cluster-security** command indicated that the Non-DTLS members parameter was set to **Allow**. The fix ensures the values match correctly. This issue was observed in APs running AOS-W Instant 8.10.0.1 or later versions.	AOS-W Instant 8.10.0.1

Chapter 6
Known Issues and Limitations

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

Known Issues

Following are the known issues observed in this release.

Table 5: *Known Issues in AOS-W Instant 8.12.0.0*

Bug ID	Description	Reported Version
AOS-239482	Some OAW-IAPs with Wi-Fi configuration and a 5 GHz radio connectivity are unable to setup a mesh topology. This issue is observed in OAW-AP635 and OAW-AP655 OAW-IAPs running AOS-W Instant 8.12.0.0.	AOS-W Instant 8.12.0.0

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.

NOTE

While upgrading an OAW-IAP, you can use the image check feature to allow the OAW-IAP to find new software image versions available on a cloud-based image server hosted and maintained by Alcatel-Lucent. The location of the image server is fixed and cannot be changed by the user. The image server is loaded with the latest versions of the AOS-W Instant software.

Topics in this chapter include:

- Upgrading an OAW-IAP Using OmniVista 3600 Air Manager Management Platform on page 24
- Upgrading an OAW-IAP Image Manually Using the WebUI on page 25
- Upgrading an OAW-IAP Image Manually Using CLI on page 26
- Upgrade from AOS-W Instant 6.4.x.x-4.2.x.x to AOS-W Instant 8.10.0.x on page 27

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.

NOTE

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

HTTP Proxy Support through Zero Touch Provisioning

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

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

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

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

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

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

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

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

Rolling Upgrade on OAW-IAPs with OmniVista 3600 Air Manager

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

Upgrading an OAW-IAP Image Manually Using the WebUI

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

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

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

Access Points	Image File Format
OAW-AP344, OAW-AP345, OAW-AP514, OAW-AP515, OAW-AP518, OAW-AP574, OAW-AP575, OAW-AP575EX, OAW-AP577, and OAW-AP577EX	Alcatel Instant_Draco_8.10.0.x_xxxx
OAW-AP503H, OAW-AP504, OAW-AP505,	Alcatel Instant_Gemini_8.10.0.x_xxxx

Access Points	Image File Format
OAW-AP505H, OAW-AP565, and OAW-AP567.	
OAW-IAP314, OAW-IAP315, OAW-IAP324, OAW-IAP325, OAW-AP374, OAW-AP375, OAW-AP377, OAW-AP318, and OAW-AP387	Alcatel Instant_Hercules_8.10.0.x_xxxx
OAW-IAP334 and OAW-IAP335	Alcatel Instant_Lupus_8.10.0.x_xxxx
OAW-AP534, OAW-AP535, OAW-AP535, OAW-AP-584, OAW-AP585, OAW-AP585EX, OAW-AP587, OAW-AP587EX	Alcatel Instant_Scorpio_8.10.0.x_xxxx
OAW-AP303, OAW-AP303H, 303P Series, OAW-IAP304, OAW-IAP305, OAW-AP365, and OAW-AP367	Alcatel Instant_Ursa_8.10.0.x_xxxx
OAW-AP203H, OAW-AP203R, OAW-AP203RP, and OAW-IAP207	Alcatel Instant_Vela_8.10.0.x_xxxx

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

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

  ii. Enter the image URL in the **URL** text field. The syntax to enter the URL is as follows:
  - HTTP - http://<IP-address>/<image-file>. For example, http://<IP-address>/Alcate Instant_Hercules_8.10.0.x_xxxx
  - TFTP - tftp://<IP-address>/<image-file>. For example, tftp://<IP-address>/Alcatel Instant_Hercules_8.10.0.x_xxxx
  - FTP - ftp://<IP-address>/<image-file>. For example, ftp://<IP-address>/Alcatel Instant_Hercules_8.10.0.x_xxxx
  - FTP - ftp://<user name:password>@<IP-address>/<image-file>. For example, ftp://<alcatel :123456>@<IP-address>/AlcatelInstant_Hercules_8.10.0.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.

4. Disable the **Reboot all APs after upgrade** toggle switch if required. This option is enabled by default to allow the OAW-IAPs to reboot automatically after a successful upgrade. To reboot the OAW-IAP at a later time, clear the **Reboot all APs after upgrade** check box.
5. Click **Upgrade Now** to upgrade the OAW-IAP to the newer version.
6. Click **Save**.

Upgrading an OAW-IAP Image Manually Using CLI

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

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

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

```
(Instant AP)# upgrade-image ftp://192.0.2.7/AlcatelInstant_Hercules_8.10.0.x_xxxx
```

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

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

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

```
(Instant AP)# upgrade-image2-no-reboot ftp://192.0.2.7/Alcatel Instant_Hercules_
8.10.0.x_xxxx
```

The following command describes how to view the upgrade information:

```
(Instant AP)# show upgrade info
Image Upgrade Progress
----------------------
Mac IP Address AP Class Status Image Info Error Detail
--- --------- -------- ------ ---------- ------------
d8:c7:c8:c4:42:98 10.17.101.1 Hercules image-ok image file none
Auto reboot :enable
Use external URL :disable
```

Upgrade from AOS-W Instant 6.4.x.x-4.2.x.x to AOS-W Instant 8.10.0.x

Before you upgrade an OAW-IAP running AOS-W Instant 6.5.4.0 or earlier versions to AOS-W Instant 8.10.0.x, follow the procedures mentioned below:

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