AOS-W Instant 8.11.0.0

Release Notes

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:

For the list of terms, refer to the Glossary.

Important Upgrade Information for Clusters that Include OAW-AP320 Series, OAW-AP340 Series, and OAW-AP387 Series Access Points

Starting from AOS-W Instant 8.11.0.0, OAW-AP320 Series, OAW-AP340 Series, and OAW-AP387 Series access points are not supported. However, you may find the images, Hercules and Draco, available for download. They are meant for installation on platforms supported by AOS-W Instant 8.11.0.0. Attempting to install AOS-W Instant 8.11.0.x firmware on the aforementioned APs may cause these APs to disconnect themselves from the current cluster and form a new cluster running the software version available in the partition.

Therefore, ensure that OAW-AP320 Series, OAW-AP340 Series, and OAW-AP387 Series access points are removed from the cluster before upgrading it to AOS-W Instant 8.11.0.0.

For more information on OAW-IAP upgrade procedure, see Upgrading an OAW-IAP.

For more information on supported platforms, see Supported Hardware Platforms.

Related Documents

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

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

Supported Browsers

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

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

Terminology Change

As part of advancing 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, Aruba 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

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.

Release Type

Short Supported Release

AOS-W Instant 8.11.0.0 is a Short Supported Release. Short supported releases have support for up to 2 years.

Authentication

Enhancement to OKC Roaming

Starting from this release, the WPA2 OKC function is replaced with the WPA3 OKC function, currently the most secure method for enterprise-level access authentication. WPA3-CNSA also supports PMKSA caching, which cuts down the authentication overhead after roaming.

To enable this feature:

- Use the existing **okc** parameter under the **wlan ssid profile** configure command.
- Enable the existing **Opportunistic Key Caching(OKC)** knob under **Security Level** for a chosen OAW-IAP on the **Configuration > Networks** page.

Datapath

Enhancements to Commands that Display Routing Profile and Datapath Session Information

New parameters to view routing profile information and datapath sessions are added. The following is the list of new parameters added:

- show datapath route verbose
- show datapath session verbose
- show log routing
- show routing-profile verbose

For more information, see the *AOS-W Instant 8.x CLI Reference Guide*.

Modified Commands to view Per-AP Settings

Starting from this release, the **show ap debug cloud-restore-status** command includes new fields related to the Per-ap-settings. The new **show ap-env-pre-backup** command displays the Per-ap setting that is saved before the OAW-IAP is rebooted.

IoT

BLE Daemon Support for Per-AP Calibrated RSSI Tables

Starting from this release, APs with Gen-2 BLE/IoT radios will adjust the calibrated RSSI values for iBeacon advertisements when BLE transmit power levels are modified using the ble-txpower setting in the IoT Radio Profile configuration. The calibrated values can then be verified using the **show ap debug ble-advertisement-info** command.

Enable or Disable BLE Periodic Telemetry

The BLE Telemetry setting can now be enabled or disabled in the AOS-W Instant webUI. A new parameter **blePeriodicTelemetryDisable** is introduced in the iot transportProfile command to disable periodic telemetry reporting.

Improvement in the WebSocket Secure Connection

AOS-W Instant now enhances the retry behavior for WebSocket Secure (wss) connections when a connection needs to be re-established. The WebSocket now continues to retry until the connection is successful.

Improvements to Health Messages Reported during IoT Transport

The health messages sent during IoT transport have been updated to include more information on the health statuses of the devices.

- Radio health message now includes information about the Up or Down status of the radio mode, BLE mode or Zigbee Mode etc.
- USB health message now reports as healthy, only if the dongle is up-and-running. The USB device includes USB Nordic APB and Serial-Data USB device such as Enocean device.
- AP health message will now include the AP layer's metrics status which are related to reporting data.

Increased Timeout Duration for Assa Abloy Door Locks

The timeout duration of Assa Abloy door locks has been increased to a maximum of 11 days. The following CLI command is used to manually set the timeout duration for Assa Abloy door locks:

```
(Instant AP)# zigbee-init-action kick-out radio <radio mac-address> client <client
mac-address>
```

IoT Audit Trail

The **show ap debug iot-audit-trail** command is introduced to display all the action commands executed in the CLI and report the Southbound API messages received from the server.

Support for Multiple Long-Lasting Connections with Nordic Chip Radio

Starting from this release, AOS-W Instant supports concurrent scanning and bleConnect connections to the IoT devices. A maximum of ten concurrent connections can be established. This function is currently supported only on OAW-IAPs with nordic radios —OAW-AP500 Series, OAW-AP510 Series, OAW-AP530

Series, OAW-AP550 Series, OAW-560 Series, OAW-AP570 Series, OAW-AP610 Series, and OAW-630 Series access points, along with an external USB dongle.

Support for New ABB Sensors

The following two new ABB sensors are supported by OAW-IAPs. Listed below are details on how to identify the sensor type and and work out the sensor identifier from the advertisement packets:

- **DFU Target Device**—The DFU target is the device that runs the DFU having at least one active DFU transport. It can be the bootloader in DFU mode, or an application with DFU running in the background. To be able to perform an update using the AP the sensor must be discovered when it enters the bootloader mode.
  - **Sensor Identifier**—The DFU target device sensor is recognized by service class UUID : **0xFE59**. This service UUID needs to be configured under **Filters** in the IoT transport profile.

    The following procedure describes how to configure DFU Target Device on an OAW-IAP:

    1. When configuring the IoT transport profile, ensure that the **Server Type** is either set to **Telemetry Https**, **Telemetry Websocket**, or **Azure IoT Hub**.
    2. Under **Filters**, click **Company Identifier**, and the click **+**.
    3. Enter the sensor identifier **FE59** in the text box and click **Ok**.

    The following CLI command is used to configure DFU Target Device on an OAW-IAP:

    ```
    (Instant AP)(Config)# iot transportProfile example
    (Instant AP)(IoT Transport Profile "example")# companyIdentifierFilter FE59
    ```

    For more information, see *Configuring an IoT Transport Profile* in the *Aruba Instant 8.11.0.0 User Guide*.
- **SALT Star Vario**—The SALT Star Vario sensor is recognized by local name : **perma**. When the local name is parsed to the OAW-IAP, the identity of the sensor is assigned as SALT + MAC Address. For example, if device's MAC address is 00:80:25:FB:1A:73, then its identity is SALT008036FB1A73. This sensor identifier can be configured under **Filters** in the IoT transport profile.

  The following procedure desccribes how to configure SALT Star Vario on an OAW-IAP:

  1. When configuring the IoT transport profile, ensure that the **Server Type** is either set to **Telemetry Https**, **Telemetry Websocket**, or **Azure IoT Hub**.
  2. Under **Filters**, click **Local Name**, and the click **+**.
  3. Enter the sensor identifier **Perma** in the text box and click **Ok**.

  The following CLI command is used to configure SALT Star Vario on an OAW-IAP:

  ```
  (Instant AP)(Config)# iot transportProfile example
  (Instant AP)(IoT Transport Profile "example")# localNameFilter perma
  ```

  For more information, see *Configuring an IoT Transport Profile* in the *AOS-W Instant 8.11.0.0 User Guide*.

Platform

OAW-AP610 Series Access Points

The Alcatel-Lucent OAW-AP610 Series access points (OAW-AP615) are high performance, dual-radio, tri-band indoor access points that can be deployed in either Switch-based (AOS-W) or Switch-less (AOS-W

Instant) network environments. These APs deliver high performance 2.4 GHz, 5 GHz, and 6 GHz 802.11ax Wi-Fi (Wi-Fi 6E) functionality with dual radios (2x2 in 2.4 GHz, 5 GHz, and 6 GHz), with the ability to operate these radios on any two out of three bands simultaneously. Additionally, these APs deliver capacity with OFDMA (Orthogonal Frequency Division Multiple Access) technologies while also supporting 802.11a, 802.11b, 802.11g, 802.11n, and 802.11ac wireless services.

OAW-AP615 access points operate in 2.4 GHz and 5 GHz radio band by default. To enable the AP to broadcast on 6 GHz radio band, set the flexible dual band radio mode to either **5 GHz and 6 GHz** or **2.4 GHz and 6 GHz**. For more information, refer to the Flexible Dual Band Radio section in the *AOS-W Instant 8.11.0.x User Guide*.

Additional features include:

- IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac, and IEEE 802.11ax spectrum monitor.
- One Ethernet port, ENET0, capable of data rates up to 2.5 Gbps.
- Compatible with IEEE 802.3bt, IEEE 802.3at, and IEEE 802.3af PoE standards on the Ethernet port.
- Mesh.
- Thermal management.
- High power BLE.

For complete technical details and installation instructions, see *Alcatel-Lucent OAW-AP610 Series Access Points Installation Guide*.

Enhancements to DTLS Port

The port used for DTLS connections, port 4434, now opens and closes based on the status of DTLS configuration. The port opens when DTLS is enabled and closes when DTLS is disabled. This enhances the security of the AP by closing unused ports.

Enhancements to DHCP Relay Port

The port used for DHCP relay, port 1067, now opens and closes based on the status of DHCP relay configuration. The port opens when DHCP relay is configured and closes when the configuration is removed. This enhances the security of the AP by closing unused ports.

Flexible Dual Band Radios in OAW-AP615 Access Points

The new Alcatel-Lucent OAW-AP610 Series are equipped with Flexible Dual Band radios. These radios can operate in 2 different bands- radio 0 can operate in 5 GHz and 2.4 GHz bands while radio 1 can operate in 2.4 GHz and 6 GHz band. With this radio combination, the AP can operate in one of the three radio band modes: 5 GHz and 2.4 GHz, 5 GHz and 6 GHz, and 2.4 GHz and 6 GHz, allowing the flexibility to change the operating radio bands based on the deployment scenario.

OAW-AP615 access points operate in 2.4 GHz and 5 GHz radio band by default. To enable the AP to broadcast on 6 GHz radio band, set the flexible dual band radio mode to either **5 GHz and 6 GHz** or **2.4 GHz and 6 GHz**. For more information, refer to the Flexible Dual Band Radio section in the *AOS-W Instant 8.11.0.x User Guide*.

New Show Command to View the Power Consumption Statistics of the AP

A new show command, **show ap power-mgmt-statistics**, that allows you to view the power consumption statistics of the AP is introduced. Use this command to view the AP power consumption

info, power consumption policies of various components, status of IPM configuration among other power related information.

Modifications to CLI Parameters that Configure IPM Reduction Steps

All references to the radio bands (2.4 GHz, 5 GHz, secondary 5 GHz, and 6 GHz bands) in IPM reduction steps are removed and replaced with radio indices (0, 1, or 2). These indices refer to the corresponding radio of the AP.

Support for Frame Bursting Mode

AOS-W Instant allows users to control frame bursting behavior of the AP irrespective of whether there are one or more active clients associated to it. Frame bursting mode is configured in the radio profile settings and is available in 5 GHz, secondary 5 GHz, and 6 GHz radios.

Support for Location Co-ordinate Information Broadcast

OAW-IAPs can now broadcast AP location information to clients. The LCI broadcast feature enables the AP to respond with location information to FTM queries, probe requests, and beacon responses. APs broadcast the location information stored on the AP. Please reach out to Alcatel Technical Support for configuring location data for your AP.

This feature is supported on OAW-AP500 Series, OAW-AP510 Series, OAW-518 Series, OAW-AP530 Series, OAW-AP550 Series, OAW-560 Series, OAW-AP570 Series, OAW-570EX Series, OAW-580 Series, OAW-580EX Series, OAW-AP610 Series, OAW-630 Series, and OAW-650 Series access points.

Support for RTS Frame Transmission

AOS-W Instant allows users to control RTS frame transmission to the clients. RTS is configured in the radio profile settings and is available in 2.4 GHz, 5 GHz, secondary 5 GHz, and 6 GHz radios.

Support for UNII-4 Channels

AOS-W Instant supports broadcast on UNII-4 channels (169-177) in the 5 GHz radio band. This is supported only on OAW-AP530 Series, OAW-AP550 Series, OAW-630 Series, and OAW-650 Series access points.

Zero-wait DFS Support for OAW-650 Series Access Points

AOS-W Instant supports zero-wait DFS feature on OAW-650 Series access points. The zero-wait DFS feature is available in the 5 GHz radio profile settings.

WebUI

Configuration of 160 MHz Channels using the WebUI

A new option, **160MHz support**, is added to the AOS-W Instant webUI under **ARM > Access Point Control** in the **Configuration > RF** page. This allows you to configure 160 MHz channels on an AOS-W Instant AP. This option is visible only when 80 MHz channel support is enabled on the AP.

The following table displays the OAW-IAP platforms supported in AOS-W Instant 8.11.0.x release.

Table 3: *Supported OAW-IAP Platforms*

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

Deprecated OAW-IAPs

The following OAW-IAPs are no longer supported from AOS-W Instant 8.11.0.0 onwards:

- 203H Series — OAW-AP203H
- 203R Series — OAW-AP203R and OAW-AP203RP
- 207 Series — OAW-IAP207

- OAW-AP320 Series — OAW-IAP324 and OAW-IAP325
- OAW-AP330 Series — OAW-IAP334 and OAW-IAP335
- OAW-AP340 Series — OAW-AP344 and OAW-AP345

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 myportal.al-enterprise.com.

The following DRT file version is part of this release:

- DRT-1.0_85075

Chapter 5
Resolved Issues

The following issues are resolved in this release.

Table 4: *Resolved Issues in AOS-W Instant 8.11.0.0*

Bug ID	Description	Reported Version
AOS-220890	MPSK-Local SSID was broadcasted as Open SSID in OAW-IAPs when the software version was downgraded to AOS-W Instant versions lower than 8.7.0.0. The fix ensures that the AP does not default to Open SSID when downgrading to AOS-W Instant versions lower than 8.7.0.0. This issue was observed in APs running AOS-W Instant 8.6.0.8 or later versions.	AOS-W Instant 8.6.0.8
AOS-222053	Multicast traffic from a mesh portal OAW-IAP to a mesh point AP dropped intermittently. The fix ensures that the multicast traffic is not dropped. This issue was observed in APs running AOS-W Instant 8.7.1.2 or later versions.	AOS-W Instant 8.7.1.2
AOS-224170 AOS-225601	Some member APs in a cluster appeared as down in the OmniVista 3600 Air Manager UI. The fix ensures that the member APs display their correct status in OmniVista 3600 Air Manager UI. This issue was observed in OmniVista 3600 Air Manager-managed APs running AOS-W Instant 8.6.0.0 or later versions.	AOS-W Instant 8.6.0.0
AOS-225553 AOS-226997	Clients were unable to access the Internet. The debug logs indicated that the DNS requests of clients were incorrectly forwarded to the member AP. This issue occurred when one of the member AP's MAC address was cached as the DNS server IP after a conductor failover. The fix ensures that the routing information is updated correctly after a failover event. This issue was observed in APs running AOS-W Instant 8.6.0.11 or later versions.	AOS-W Instant 8.6.0.11
AOS-225656	The AP was stuck in the **MASTER_FOUND** state for a prolonged duration and went into degraded state when login was attempted during this period. The fix ensures that the AP cycles through the discovery stages as expected. . This issue was observed in APs running AOS-W Instant 8.3.0.0 or later versions.	AOS-W Instant 8.3.0.0
AOS-227814 AOS-232336	Certain Windows clients and mobile devices were unable to connect to WPA3 SSID. This issue occurred due a handshake error. The fix ensures that the devices can connect to the WPA3 SSID as expected. This issue was observed in APs running AOS-W Instant 8.8.0.3 or later versions.	AOS-W Instant 8.8.0.3
AOS-228888	The Ethernet port link of an OAW-IAP was caught in a loop condition. This caused the link to switch between the enabled and disabled status although the uplink switch port was stable. The fix ensures that OAW-IAP functions as expected. This issue was observed in APs running AOS-W Instant 8.7.1.4 or later versions.	AOS-W Instant 8.7.1.4

Table 4: *Resolved Issues in AOS-W Instant 8.11.0.0*

Bug ID	Description	Reported Version
AOS-228967	The **Station Ageout Time** in the SSID profile settings could not be configured to a value over 3600 seconds. The fix ensures that the **Station Ageout Time** can be configured to a value between 60–86,400 seconds. This issue was observed in APs running AOS-W Instant 8.7.1.4 or later versions.	AOS-W Instant 8.7.1.4
AOS-229903	The **Match MAC** information was not displayed in the **Rogue Device Info** page of the OmniVista 3600 Air Manager UI. This issue occurred when the OAW-IAP failed to send the match MAC information to OmniVista 3600 Air Manager. The fix ensures that all rogue devices connected to the AP are listed on the OmniVista 3600 Air Manager UI. This issue was observed in APs running AOS-W Instant 8.6.0.4 or later versions.	AOS-W Instant 8.6.0.4
AOS-230900 AOS-231081 AOS-231941	OAW-IAPs operating as the Virtual Switch crashed and rebooted unexpectedly. The log file listed the reason for reboot as: **Reboot caused by kernel panic: Take care of the TARGET ASSERT first**. The fix ensures that the APs function as expected. This issue was observed in OAW-AP530 Series and OAW-AP550 Series access points running AOS-W Instant 8.6.0.0 or later versions.	AOS-W Instant 8.7.1.7
AOS-231019 AOS-232063	An OAW-IAP failed to reconnect after an LTE outage. The output of the **show cell status** command was missing information. The fix ensures that the AP functions as expected. This issue was observed in APs running AOS-W Instant 8.6.0.16 or later versions.	AOS-W Instant 8.7.1.7
AOS-231437 AOS-234673 AOS-233640	Some OAW-AP300 Series and OAW-AP500 Series access points rebooted randomly. The log file listed the reason for reboot as: **AP Reboot reason: Power-reset**. This issue occurred when the AP unexpectedly requested very low power from the Switch due to a malformed request packet. The fix ensures that the AP does not generate malformed request packets and works as expected. 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-231569	The VPN Switch was missing from the **Topology** page, despite the OAW-IAP forming a VPN connection with the Switch. The fix ensures that the VPN Switch is displayed on the **Topology** page. This issue was observed in APs running AOS-W Instant 8.9.0.0 or later versions.	AOS-W Instant 8.9.0.0
AOS-232112	An OAW-IAP returned the following message: **503 Service Unavailable** when using REST API. When this occurred, the client was unable to use REST API to retrieve information from the AP. The fix ensures that the REST API functions as expected. This issue was observed in APs running AOS-W Instant 8.6.0.6 or later versions.	AOS-W Instant 8.6.0.6
AOS-232305	Clients were unable to acquire IP addresses on Centralized, L2 VLAN when the OAW-IAP routing settings were changed. This issue occurred when: ■ The first tunnel message was silently ignored by a member AP. ■ The config load took more than 60 seconds. ■ The conductor AP did not send the second tunnel message. The fix ensures that the second tunnel message from the conductor AP to a member AP is never skipped even if config load takes more than 60 seconds. This issue was observed in OmniVista 3600 Air Manager-managed APs running AOS-W Instant 8.6.0.15 or later versions.	AOS-W Instant 8.6.0.15

Table 4: *Resolved Issues in AOS-W Instant 8.11.0.0*

Bug ID	Description	Reported Version
AOS-232501	The client was unable to discover Airtame servers. The server was dropped from the response to the user query because: ■ The user role was missing. ■ The role based CPPM policy was not present. The fix ensures that available Airtame servers are visible. This issue was observed in APs running AOS-W Instant 8.6.0.16 or later versions.	AOS-W Instant 8.6.0.16
AOS-232510	The client was unable to access OAW-AP505 access points through the webUI. This issue occurred when: ■ The OAW-IAP was configured with a static IP address. ■ Wi-Fi uplink was enabled. The fix ensures that the APs can be accessed. 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-232748	Some OAW-IAPs in a cluster crashed unexpectedly. The log file listed the reason for reboot as: **Kernel panic - not syncing: MemLeak: mem low for 60 seconds, under 6% 597 times, MB free 6 (1%), total 465**. The fix ensures that the AP functions as expected. This issue was observed in APs running AOS-W Instant 8.9.0.3 or later versions.	AOS-W Instant 8.9.0.3
AOS-232833	Member OAW-IAPs ignored the proxy server configuration, and failed to download the firmware using the image URL provided by the virtual Switch. The fix ensures that the APs download the firmware as expected. This issue was observed in APs running AOS-W Instant 8.9.0.0 or later versions.	AOS-W Instant 8.9.0.0
AOS-232843	An OAW-IAP failed to translate the source IP address of its clients for outgoing traffic. This issue occurred: ■ with clients connected to the conductor AP. ■ when the **Client IP assignment** was set to Virtual Switch managed. ■ when the conductor OAW-IAP was configured with a static IP address. The fix ensures that the AP translates the source IP address for outgoing traffic. This issue was observed in APs running AOS-W Instant 8.9.0.3 or later versions.	AOS-W Instant 8.9.0.3
AOS-233057	Cisco phones encountered a one-way audio issue. This issue occurred when: ■ An OAW-IAP was upgraded to AOS-W Instant 8.9.0.2. ■ The VPN tunnel was terminated at a Switch. The fix ensures that Cisco phones function as expected. 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-233149 AOS-235164	The AP log generated a lot of **xhci-hcd xhci-hcd.0.auto: Ring expansion failed: ep_state 3; ring_type 2; trbs 1, free 1; id 0** messages when connected to USB LTE modems. The fix ensures that random messages are not generated by the AP. This issue was observed in APs running AOS-W Instant 8.7.1.9 or later versions.	AOS-W Instant 8.7.1.9

Table 4: *Resolved Issues in AOS-W Instant 8.11.0.0*

Bug ID	Description	Reported Version
AOS-233215	The OAW-IAP did not save the TACACS server configuration after assigning it as the management auth server. This issue occurred when the TACACS server name contained a space. The AP automatically removed the configuration when the client attempted to save the information. The fix ensures the TACACS server configuration is saved on the OAW-IAP as expected. This issue was observed in APs running AOS-W Instant 8.9.0.3 or later versions.	AOS-W Instant 8.9.0.3
AOS-233264	The configured bandwidth contract of an OAW-IAP did not function as expected. This issue occurred when: ■ The upstream bandwidth contract rule was configured under a user role. ■ The user role was routed into a VPN tunnel. The fix ensures that the bandwidth contract functions as configured. This issue was observed in APs running AOS-W Instant 8.6.0.16 or later versions.	AOS-W Instant 8.6.0.16
AOS-233372	The DHCP server failed to start with the correct interface when the AP did not have an active Ethernet uplink at boot time. The server also did not issue IPv4 or IPv6 addresses in the guest or DHCP scope defined VLANs. The fix ensures that: ■ The server process starts correctly regardless of the Ethernet uplink status. ■ The server issues IPv4 and IPv6 addresses properly according to configuration. This issue was observed in APs running AOS-W Instant 8.8.0.0 or later versions.	AOS-W Instant 8.10.0.0
AOS-233426	Clients were unable to open the Captive Portal page when internal Captive Portal was configured on the SSID. This issue occurred when the OAW-IAP did not spoof DNS requests and respond to the user query. This issue was observed in Centralized, L2 DHCP mode and when VRRP or HSRP is deployed in the client gateway in the datacenter. The fix ensures that clients are able to open the Captive Portal page as expected. This issue was observed in APs running AOS-W Instant 8.6.0.14 or later versions.	AOS-W Instant 8.6.0.14
AOS-233772	OAW-AP505 access points could not perform 802.1X authentication for Aruba 2930F Switch Series and Aruba 2930M Switch Series. The fix ensures that the APs complete 802.1X authentication for Aruba 2930F Switch Series and Aruba 2930M Switch Series. This issue was observed in APs running AOS-W Instant 8.7.1.8 or later versions.	AOS-W Instant 8.7.1.8
AOS-233987 AOS-235089	IDS related messages for SNMPv3 traps were not generated by the OAW-IAP. The fix ensures that SNMPv3 traps are generated for IDS messages. 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-234448	An OAW-IAP sent DNS queries to the DHCP-learned DNS server IP address instead of the configured VC DNS IP address. The fix ensures that the AP sends the queries to the configured VC DNS IP address. This issue was observed in APs running AOS-W Instant 8.8.0.0 or later versions.	AOS-W Instant 8.8.0.2

Table 4: *Resolved Issues in AOS-W Instant 8.11.0.0*

Bug ID	Description	Reported Version
AOS-234828	OAW-AP315 access points in a cluster rebooted automatically. The log file listed the reason for reboot as: **Critical process /aruba/bin/stm [pid 26061] DIED, process marked as RESTART**. The fix ensures that the AP works as expected. This issue was observed in OAW-AP315 access points running AOS-W Instant 8.9.0.3 or later versions.	AOS-W Instant 8.9.0.3
AOS-234976	An OAW-IAP cluster reported **checksum mismatch** errors. This issue occurred when a PKCS8 certificate was uploaded for Captive Portal, where: ■ An AP using OpenSSL library acted as the conductor. ■ APs using WolfSSL library acted as member APs. The fix ensures the certificates are synchronized across all APs in the cluster as expected. This issue was observed in APs running AOS-W Instant 8.6.0.17 or later versions.	AOS-W Instant 8.6.0.17
AOS-235428	OAW-IAP clusters intermittently lose connectivity with Aruba Central??? and displayed the error message: **master failover**. This issue occurred when the OAW-IAP cluster lost its VPN connection. The fix ensures that the AP works as expected. This issue was observed in Aruba Central???-managed OAW-IAP clusters running AOS-W Instant 8.6.0.17 or later versions.	AOS-W Instant 8.6.0.17
AOS-235678	The WebUI certificate could not be deleted on the OAW-IAP. This issue occurred due to a mismatch during configuration synchronization in the AOS-W Instant cluster. The fix ensures that the WebUI certificates are removed as expected. This issue was observed in APs running AOS-W Instant 8.6.0.15 or later versions.	AOS-W Instant 8.6.0.15
AOS-235761	The core dump files were not saved in the OAW-IAP. The output of the **show ap debug core-info** command was missing information. The fix ensures that the core dump files are saved in the OAW-IAP in the event of a core dump. This issue was observed in OAW-IAPs running AOS-W Instant 8.6.0.17 or later releases.	AOS-W Instant 8.6.0.17
AOS-235895	The ASSA ABLOY locks that were connected to an AP timed out unexpectedly. This issue occurred when the locks did not send data requests for 256 minutes. The fix ensures that the ASSA ABLOY locks remain connected for the maximum allowed duration set by the users. This issue was observed in APs running ArubaOS 8.10.0.0 or later versions.	AOS-W Instant 8.10.0.0
AOS-236369	The 2.4 GHz and 5 GHz radios operated on more power than the settings configured. The fix ensures that the radios operate as per the power level defined in the settings. This issue was observed in mesh point APs running AOS-W Instant 8.9.0.3 or later versions.	AOS-W Instant 8.9.0.3
AOS-236488	Authentication issues were caused by IAPP packets that were created with the BSSID MAC address instead of the client MAC address. Updates to the wireless driver ensures that client MAC is used as the source MAC for generating IAPP messages. This issue was observed in Aruba Central???-managed APs running AOS-W Instant 8.10.0.1 or later versions.	AOS-W Instant 8.10.0.1

Table 4: *Resolved Issues in AOS-W Instant 8.11.0.0*

Bug ID	Description	Reported Version
AOS-236638	Wireless clients connected to an SSID using native VLAN were unable to receive IP addresses from the DHCP server. This was observed in deployments that used a VPN connection to connect the AP and the DHCP server. This issue occurred after an AP boot when there was a delay in connecting to the VPN that connects to the DHCP server. The fix ensures that the VPN connection is made as expected after an AP boot. 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-237704	An OAW-IAP failed to broadcast SSIDs that had the VLAN names - **gues, gue, gu, g**. The fix ensures that the strings, **gues, gue, gu, g**, can be configured as VLAN names for SSIDs. This issue was observed in AOS-W Instant 8.9.0.3 or later versions.	AOS-W Instant 8.9.0.3

Chapter 6
Known Issues and Limitations

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

Limitations

This section describes the limitations in AOS-W Instant 8.11.0.0.

AP Hostname Character Limit Extension

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

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

Dynamic Multicast Optimization Unsupported with VLAN Derivation

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

Inbound Firewall

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

Unified Communications Manager

UCM does not prioritize NAT traffic.

Known Issues

Following are the known issues observed in this release.

Table 5: *Known Issues in AOS-W Instant 8.11.0.0*

Bug ID	Description	Reported Version
AOS-234261	An OAW-IAP fails to forward IPv6 traffic when the client connects to the SSID. This issue is observed in APs running AOS-W Instant 8.11.0.0.	AOS-W Instant 8.11.0.0
AOS-236383	Users experience network performance issues with an OAW-IAP when using Wi-Fi uplink. This is issue is observed in APs running AOS-W Instant 8.11.0.0.	AOS-W Instant 8.11.0.0

Table 5: *Known Issues in AOS-W Instant 8.11.0.0*

Bug ID	Description	Reported Version
AOS-236630 AOS-238707	Traffic for YouTube application is not blocked despite having an AppRF rule specified to block them. However, YouTube traffic is blocked when it is accessed through the browser. This issue is observed in APs running AOS-W Instant 8.9.0.3 or later versions.	AOS-W Instant 8.9.0.3
AOS-237700	FTM ranging for 6 GHz radio does not function as expected on the WifiRTT app. This is issue is observed in OAW-AP615 access points running AOS-W Instant 8.11.0.0.	AOS-W Instant 8.11.0.0
AOS-238443	Uplink preemption fails to function as expected. This issue occurs when a higher priority interface does not resume primary uplink during interface faillover recovery and ignores the configured interface priority. This is issue is observed in APs running AOS-W Instant 8.11.0.0.	AOS-W Instant 8.11.0.0
AOS-238614	An OAW-IAP crashes unexpectedly. The log file lists the reason for reboot as: **BadPtr: 00000004 PC: __skb_try_recv_from_ queue+0x160/0x190 Warm-reset**. This issue is observed in APs running AOS-W Instant 8.11.0.0.	AOS-W Instant 8.11.0.0

Chapter 7
Upgrading an OAW-IAP

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

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

Topics in this chapter include:

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

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

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

HTTP Proxy Support through Zero Touch Provisioning

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

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

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

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

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

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

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

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

Rolling Upgrade on OAW-IAPs with OmniVista 3600 Air Manager

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

Upgrading an OAW-IAP Image Manually Using the WebUI

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

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

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

Access Points	Image File Format
OAW-AP514, OAW-AP515, OAW-AP518, OAW-AP574, OAW-AP575, OAW-AP575EX, OAW-AP577, and OAW-AP577EX	AlcatelInstant_Draco_8.11.0.x_xxxx
OAW-AP503H, OAW-AP504, OAW-AP505, OAW-AP505H, OAW-AP565, and OAW-AP567.	AlcatelInstant_Gemini_8.11.0.x_xxxx

Access Points	Image File Format
OAW-IAP314, OAW-IAP315, OAW-AP374, OAW-AP375, OAW-AP377, and OAW-AP318.	AlcatelInstant_Hercules_8.11.0.x_xxxx
OAW-AP534, OAW-AP535, OAW-AP535, OAW-AP-584, OAW-AP585, OAW-AP585EX, OAW-AP587, and OAW-AP587EX	AlcatelInstant_Scorpio_8.11.0.x_xxxx
OAW-AP303, OAW-AP303H, 303P Series, OAW-IAP304, OAW-IAP305, OAW-AP365, and OAW-AP367	AlcatelInstant_Ursa_8.11.0.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_8.11.0.x_xxxx
- TFTP - tftp://<IP-address>/<image-file>. For example, tftp://<IP-address>/Alcatel Instant_Hercules_8.11.0.x_xxxx
- FTP - ftp://<IP-address>/<image-file>. For example, ftp://<IP-address>/Alcatel Instant_Hercules_8.11.0.x_xxxx
- FTP - ftp://<user name:password>@<IP-address>/<image-file>. For example, ftp://<alcatel :123456>@<IP-address>/AlcatelInstant_Hercules_8.11.0.x_xxxx

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

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

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

Upgrading an OAW-IAP Image Manually Using CLI

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

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

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

```
(Instant AP)# upgrade-image ftp://192.0.2.7/AlcatelInstant_Hercules_8.11.0.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_
8.11.0.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 8.11.0.x

Before you upgrade an OAW-IAP running AOS-W Instant 6.5.4.0 or earlier versions to AOS-W Instant 8.11.0.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.