

AOS-W Instant 8.5.0.7



Copyright Information

Alcatel-Lucent and the Alcatel-Lucent Enterprise logo are trademarks of Alcatel-Lucent. To view other trademarks used by affiliated companies of ALE Holding, visit:

<https://www.al-enterprise.com/en/legal/trademarks-copyright>

All other trademarks are the property of their respective owners. The information presented is subject to change without notice. Neither ALE Holding nor any of its affiliates assumes any responsibility for inaccuracies contained herein. (2020)

Open Source Code

This product includes code licensed under the GNU General Public License, the GNU Lesser General Public License, and/or certain other open source licenses.

| | |
|---|-----------|
| Contents | 3 |
| Revision History | 5 |
| Release Overview | 6 |
| Supported Browsers | 6 |
| Contacting Support | 7 |
| New Features and Enhancements | 8 |
| AOS-W Instant Certificate Expiry Issue | 8 |
| Dual Uplink for OAW-AP318, OAW-AP340 Series, OAW-AP370 Series, OAW-AP510 Series, OAW-AP530 Series, and OAW-AP555 Access Points | 8 |
| Enhancements to Uplink Ports of OAW-AP318 and OAW-AP370 Series Access Points | 9 |
| Enhancements to Control Ageout of Valid APs and Non-Valid APs | 10 |
| Supported Hardware Platforms | 11 |
| Supported OAW-IAPs | 11 |
| Regulatory Updates | 13 |
| Resolved Issues | 14 |
| Known Issues | 18 |
| Upgrading an OAW-IAP | 22 |
| Upgrading an OAW-IAP Using OmniVista 3600 Air Manager Management Platform | 22 |

| | |
|---|----|
| Upgrading an OAW-IAP Image Manually Using WebUI | 23 |
| Upgrading an OAW-IAP Image Manually Using CLI | 26 |
| Upgrade from AOS-W Instant 6.4.x.x-4.2.x.x to AOS-W Instant 8.5.0.x | 26 |

Revision History

The following table provides the revision history of this document.

Table 1: *Revision History*

| Revision | Change Description |
|-------------|--------------------|
| Revision 01 | Initial release. |

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

- [New Features and Enhancements on page 8](#)
- [Supported Hardware Platforms on page 11](#)
- [Regulatory Updates on page 13](#)
- [Resolved Issues on page 14](#)
- [Known Issues on page 18](#)
- [Upgrading an OAW-IAP on page 22](#)

For list of terms, refer [Glossary](#).



The AOS-W Instant 8.5.0.6 release contains only a DRT change and does not include any new fixes or enhancements.

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 Edge HTML 14.14393) on Windows 10
- Firefox 58 or later on Windows 7, Windows 8, Windows 10, and macOS
- Apple Safari 9.0 or later on macOS
- Google Chrome 67 and later on Windows 7, Windows 8, Windows 10, and macOS

Contacting Support

Table 2: *Contact Information*

| Contact Center Online | |
|--|--|
| Main Site | https://www.al-enterprise.com |
| Support Site | https://businessportal2.alcatel-lucent.com |
| Email | ebg_global_supportcenter@al-enterprise.com |
| Service & Support Contact Center Telephone | |
| North America | 1-800-995-2696 |
| Latin America | 1-877-919-9526 |
| EMEA | +800 00200100 (Toll Free) or +1(650)385-2193 |
| Asia Pacific | +65 6240 8484 |
| Worldwide | 1-818-878-4507 |

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

AOS-W Instant Certificate Expiry Issue

Instant Access Points (OAW-IAP) fail to load the Trust Anchor (TA) certificate bundle if it encounters an expired certificate within the bundle, because of an error in the AOS-W Instant software. This error impacts OAW-IAPs' ability to setup a secure SSL connection to Activate and OmniVista 3600 Air Manager, resulting in loss of connectivity to management platforms.

To avoid this issue, upgrade to the latest version of AOS-W Instant Software, before February 7, 2020.



This issue is observed when the existing connection between OAW-IAP and the management platform is lost or if Activate or OmniVista 3600 Air Manager services are reset.

For more information, see [Aruba Support Advisory ARUBA-SA-20191219-PLVL08](#).

Dual Uplink for OAW-AP318, OAW-AP340 Series, OAW-AP370 Series, OAW-AP510 Series, OAW-AP530 Series, and OAW-AP555 Access Points

Starting from AOS-W Instant 8.5.0.3, OAW-AP318, OAW-AP340 Series, OAW-AP370 Series, OAW-AP510 Series, OAW-AP530 Series, and OAW-AP555 access points can be provisioned as OAW-APs with both the Ethernet ports connected.

In versions prior to AOS-W Instant 8.5.0.3, deploying APs in Switch-managed networks as a OAW-AP introduced a broadcast storm into the network when both the Ethernet ports were connected to the same VLAN. This occurred during the master discovery phase under the following configuration conditions:

- Both eth0 and eth1 were connected to the uplink switch in the same VLAN.
- LACP was not configured on the upstream access ports.
- The AP models were OAW-AP318, OAW-AP340 Series, OAW-AP370 Series, OAW-AP510 Series, OAW-AP530 Series, and OAW-AP555 access points.

The workaround for this issue was to use a single uplink while provisioning the APs. The issue was resolved once the AP became Switch-managed. However, the issue is likely to re-appear in APs shipped with versions prior to 8.5.0.3, if they return to their factory default state, although the APs were successfully deployed in a Switch-managed network using a higher version of code.



If Zero Touch Provisioning of OAW-APs fails to function as expected, debug the AP using the local WebUI or CLI. Ensure that you disconnect the eth1 port from the Switch while debugging.

Enhancements to Uplink Ports of OAW-AP318 and OAW-AP370 Series Access Points

Starting from AOS-W Instant 8.5.0.3, OAW-AP318 and OAW-AP370 Series access points will have both eth1 and eth0 ports as default uplink ports. The eth1 port as the primary Ethernet uplink and eth0 as the backup Ethernet uplink by default. The primary Ethernet uplink can be configured using the **preferred-uplink** command. When eth0 port is configured as the primary Ethernet uplink, the eth1 port assumes the role of backup Ethernet uplink and vice versa.

The eth1 port cannot be configured as a downlink port whereas, if required, the eth0 port can be configured as a downlink port by configuring **enet0-bridging**. When enet0-bridging is enabled on the AP, the eth0 port assumes the downlink role irrespective of the preferred uplink configuration.

The following conditions apply to OAW-AP318 and OAW-AP370 Series access points:

- The downlink parameters configured in the wired port profile will not take effect.
- If LACP is configured, enet0-bridging cannot be enforced.
- In mesh scenarios, the mesh point change will only occur if uplink is down for both eth0 and eth1 ports.

Configuring Primary Ethernet Uplink Port

The primary Ethernet uplink for OAW-AP318 and OAW-AP370 Series access points can be configured using the **preferred-uplink** command. When configured, the primary Ethernet uplink port will be used for uplink and the backup Ethernet uplink will only be used if the primary Ethernet uplink is down. The uplink for these AP platforms will fall back to a different uplink, defined in the uplink priority list, only if both the primary and backup Ethernet link is down.

The preferred uplink command is a per-AP setting. Use the following syntax to configure the preferred uplink:

```
(Instant AP) # preferred-uplink <0,1>
```

Configuring Downlink Port

The eth0 port of OAW-AP318 and OAW-AP370 Series access points can be configured as a downlink port by enabling **enet0-bridging**. Only the eth0 port of these access points can be configured as a downlink port. If eth0 is configured as the primary Ethernet uplink and enet0 bridging is enabled, the eth0 port will become the downlink port and eth1 will become the primary Ethernet uplink port.

The enet0-bridging command is a per-AP setting. Use the following syntax to configure enet0-bridging:

```
(Instant AP) # enet0-bridging
```

Upgrading Networks with OAW-AP318 and OAW-AP370 Series Access Points from 8.5.0.0 or later versions to 8.5.0.3

Devices connected to the OAW-IAP using the eth0 port as a downlink will be disconnected from the network after upgrading to 8.5.0.3 as eth0 becomes an uplink port. The disconnected devices can be reconnected to the network by configuring **enet0-bridging** post the upgrade and rebooting the AP. The above scenario is also applicable to slave APs under OAW-AP318 and OAW-AP370 Series access points acting as master APs.



In order to prevent the disconnection of devices connected to the enet0 downlink port, it is recommended that **enet0-bridging** is configured before upgrading to AOS-W Instant 8.5.0.3.

Enhancements to Control Ageout of Valid APs and Non-Valid APs

The following CLI commands are introduced in AOS-W Instant 8.5.0.7 to control the ageout of valid APs and non-valid APs:

- **valid-ap-max-unseen-timeout <seconds>**
- **ap-max-unseen-timeout <seconds>**

Supported OAW-IAPs

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

Table 3: *Supported OAW-IAP Platforms*

| OAW-IAP Platform | Minimum Required AOS-W Instant Software Version |
|--|---|
| <ul style="list-style-type: none"> ■ OAW-AP530 Series — OAW-AP534 and OAW-AP535 ■ OAW-AP550 Series — OAW-AP555 | AOS-W Instant 8.5.0.0 or later |
| <ul style="list-style-type: none"> ■ OAW-AP303P ■ OAW-AP387 ■ OAW-AP510 Series — OAW-AP514 and OAW-AP515 | AOS-W Instant 8.4.0.0 or later |
| <ul style="list-style-type: none"> ■ OAW-AP303 Series ■ OAW-AP318 Series ■ OAW-AP340 Series — OAW-AP344 and OAW-AP345 ■ OAW-AP370 Series — OAW-AP374, OAW-AP375, and OAW-AP377 | AOS-W Instant 8.3.0.0 or later |
| <ul style="list-style-type: none"> ■ OAW-AP203H | AOS-W Instant 6.5.3.0 or later |
| <ul style="list-style-type: none"> ■ OAW-AP203R and OAW-AP203RP ■ OAW-AP303H ■ OAW-AP365 and OAW-AP367 | AOS-W Instant 6.5.2.0 or later |
| <ul style="list-style-type: none"> ■ OAW-IAP207 ■ OAW-AP300 Series — OAW-IAP304 and OAW-IAP305 | AOS-W Instant 6.5.1.0-4.3.1.0 or later |
| <ul style="list-style-type: none"> ■ OAW-AP310 Series — OAW-IAP314 and OAW-IAP315 ■ OAW-AP330 Series — OAW-IAP334 and OAW-IAP335 | AOS-W Instant 6.5.0.0-4.3.0.0 or later |
| <ul style="list-style-type: none"> ■ OAW-AP320 Series — OAW-IAP324 and OAW-IAP325 | AOS-W Instant 6.4.4.3-4.2.2.0 or later |
| <ul style="list-style-type: none"> ■ OAW-IAP228 ■ OAW-IAP277 | AOS-W Instant 6.4.3.1-4.2.0.0 or later |

Table 3: *Supported OAW-IAP Platforms*

| OAW-IAP Platform | Minimum Required AOS-W Instant Software Version |
|---|---|
| ■ OAW-AP210 Series — OAW-IAP214 and OAW-IAP215 | AOS-W Instant 6.4.2.0-4.1.1.0 or later |
| ■ OAW-AP270 Series — OAW-IAP274 and OAW-IAP275 | AOS-W Instant 6.4.0.2-4.1.0.0 or later |
| ■ OAW-AP 220 Series — OAW-IAP224 and OAW-IAP225 | AOS-W Instant 6.3.1.1-4.0.0.0 or later |
| ■ OAW-RAP155 and OAW-RAP155P | AOS-W Instant 6.2.1.0-3.3.0.0 or later |

Periodic regulatory changes may require modifications to the list of channels supported by an AP. For a complete list of channels supported by an AP using a specific country domain, access the OAW-IAP CLI and execute the **show ap allowed-channels** command.

For a complete list of countries and the regulatory domains in which the APs are certified for operation, refer to the Downloadable Regulatory Table or the DRT Release Notes at service.esd.alcatel-lucent.com.

The following DRT file version is part of this release:

- DRT-1.0_74492

This chapter describes the issues resolved in this release.



Since we have migrated to a new defect tracking tool, we have listed both, the old and the new bug ids for tracking purposes.

Table 4: Resolved Issues in AOS-W Instant 8.5.0.7

| New Bug ID | Old Bug ID | Description | Component | Platform | Reported Version |
|--------------------------|------------|--|-------------------|--|-----------------------|
| AOS-176763 AOS-189443 | 171718 | Symptom: OAW-IAPs acting as mesh points were found to be forming a loop. This issue occurred due to change in the mesh interface name. The fix ensures that the looping issue is resolved. Scenario: This issue was observed in APs running AOS-W Instant 8.4.0.0 or later versions. | Datapath | All Platforms | AOS-W Instant 8.4.0.0 |
| AOS-181829 | — | Symptom: The downstream traffic for a wireless client from the old VLAN was still sent to the old VLAN after the client changed over to a different VLAN and SSID on the same AP. The fix ensures that the downstream traffic is forward through the new VLAN. Scenario: This issue was observed in APs running AOS-W Instant 8.4.0.0 or later versions. | Datapath/Firewall | All platforms | AOS-W Instant 8.4.0.0 |
| AOS-185850 | — | Symptom: An AP reported INSUFFICIENT_POWER_SUPPLY when the power source was PoE-AT. The fix ensures that the AP logs the PoE source type and does not trigger incorrect power supply reports. Scenario: This issue occurred because the AP logged the power source as PoE for both PoE-AF and PoE-AT source types that triggered the insufficient power supply reports. This issue was observed in OAW-AP203H, OAW-AP207, OAW-AP303, and OAW-AP360 Series access points running AOS-W Instant 8.5.0.0 or later versions. | Telemetry | OAW-AP203H, OAW-AP207, OAW-AP303, and OAW-AP360 Series access points | AOS-W Instant 8.5.0.0 |

Table 4: Resolved Issues in AOS-W Instant 8.5.0.7

| New Bug ID | Old Bug ID | Description | Component | Platform | Reported Version |
|--|------------|--|----------------|--------------------------|-----------------------|
| AOS-187512 | — | <p>Symptom: An OAW-IAP experienced high latency and affected the network quality. The fix ensures that the AP does not exhibit high latency and works as expected.</p> <p>Scenario: This issue occurred when the AP generated ioctl syslog messages. This issue is observed in APs running AOS-W Instant 8.3.0.0 or later versions.</p> | Wi-Fi Driver | All platforms | AOS-W Instant 8.3.0.0 |
| AOS-187268 AOS-196356 | — | <p>Symptom: An OAW-IAP crashed and rebooted unexpectedly. The log file listed the reason for the event as Reboot caused by kernel panic: Fatal exception. The fix ensures that the AP works as expected.</p> <p>Scenario: This issue occurred when 802.11w standard was enabled in the OAW-IAP. This issue was observed in APs running AOS-W Instant 8.3.0.0 or later versions.</p> | Wi-Fi Driver | All platforms | AOS-W Instant 8.3.0.0 |
| AOS-187350 | — | <p>Symptom: An OAW-IAP did not update the client's username received from the ClearPass server. The fix ensures that the OAW-IAP updates the client's username returned from the ClearPass server after captive portal authentication.</p> <p>Scenario: This issue occurred when captive portal authentication was used. This issue was observed in APs running AOS-W Instant 8.3.0.0 or later versions.</p> | Authentication | All platforms | AOS-W Instant 8.3.0.0 |
| AOS-187773 AOS-196214 AOS-196551 | — | <p>Symptom: All OAW-IAPs in an AOS-W Instant cluster rebooted randomly and the log file listed the reason for the event as Gateway Unreachable. The fix ensures that the APs do not reboot and work as expected.</p> <p>Scenario: This issue occurred due to a packet counter error that triggered the reboot. This issue was observed in OAW-IAP305 access points running AOS-W Instant 8.4.0.1 or later versions.</p> | Datapath | OAW-IAP305 access points | AOS-W Instant 8.4.0.1 |
| AOS-188451 AOS-190008 | — | <p>Symptom: An OAW-IAP selected an inferior mesh point as the next hop when better alternatives were available. The fix ensures that routing happens through the best option available.</p> <p>Scenario: This issue occurred due to incorrect path costs in the routing table. This issue was observed in APs running AOS-W Instant 8.3.0.0 or later versions.</p> | Mesh | All platforms | AOS-W Instant 8.3.0.0 |

Table 4: Resolved Issues in AOS-W Instant 8.5.0.7

| New Bug ID | Old Bug ID | Description | Component | Platform | Reported Version |
|--------------------------|------------|---|----------------|--------------------------------|-----------------------|
| AOS-188751 AOS-187861 | — | Symptom: Clients were unable to access the network. The fix ensures that clients can connect to the network as expected. Scenario: This issue occurred when the client roamed between APs. This issue was observed in networks running AOS-W Instant 8.3.0.0 or later versions. | Datapath | All platforms | AOS-W Instant 8.3.0.0 |
| AOS-188976 AOS-197505 | — | Symptom: A client connected to an SSID using WPA3-Personal key management was unable to connect to an SSID using WPA3-Enterprise key management. The fix ensures that the client connects to the SSID configured with WPA3-Enterprise key management as expected. Scenario: This issue occurred when Opportunistic Key Caching (OKC) was enabled in the network. This issue was observed in APs running AOS-W Instant 8.5.0.0 or later versions. | STM | All platforms | AOS-W Instant 8.5.0.0 |
| AOS-192529 AOS-199126 | — | Symptom: An OAW-IAP rebooted unexpectedly and the log file listed the reason as Reboot caused by kernel panic- not syncing: Fatal exception in interrupt with PC/LR is at asap_firewall_forward+0xfc/0x92a0 . The fix ensures that the OAW-IAP works as expected. Scenario: This issue was observed in APs running AOS-W Instant 8.4.0.2 or later versions. | Datapath | All platforms | AOS-W Instant 8.4.0.2 |
| AOS-193901 AOS-196256 | — | Symptom: Samsung S10 devices were unable to authenticate into guest SSIDs with Enhanced Open security type. The fix ensures that Samsung S10 devices can authenticate into guest SSIDs with Enhanced Open security. Scenario: This issue was observed in APs running AOS-W Instant 8.4.0.2 or later versions. | Authentication | All platforms | AOS-W Instant 8.4.0.2 |
| AOS-194553 | — | Symptom: An OAW-IAP became unresponsive. The show ap debug crash-info command returned the message: Module SAPM Client is busy. Please try later . The fix ensures that the AP works as expected. Scenario: This issue was observed in OAW-AP340 Series access points running AOS-W Instant 8.3.0.0 or later versions. | Wi-Fi Driver | OAW-AP340 Series access points | AOS-W Instant 8.3.0.0 |

Table 4: Resolved Issues in AOS-W Instant 8.5.0.7

| New Bug ID | Old Bug ID | Description | Component | Platform | Reported Version |
|--|------------|--|------------------|-------------------------|-----------------------|
| AOS-195491 | — | <p>Symptom: An OAW-IAP generated random OFALD messages and affected the network performance. The fix ensures that random OFALD messages are not generated and the network performance remains unaffected.</p> <p>Scenario: This issue was observed in APs running AOS-W Instant 8.3.0.7 or later versions.</p> | OFA | All platforms | AOS-W Instant 8.3.0.7 |
| AOS-195564 AOS-196892 AOS-198878 | — | <p>Symptom: A client lost its IP address when roaming. The fix ensures that clients retain their IP address when roaming between APs.</p> <p>Scenario: This issue occurred under the following scenarios:</p> <ul style="list-style-type: none"> ■ When the client switched from the mesh portal AP to a mesh point AP when no other client was connected to the mesh portal AP. ■ This occurred in Instant networks in which Client VLAN Assignment was set to Dynamic in the Network > VLAN tab of the webUI. <p>This issue was observed in APs running AOS-W Instant 8.3.0.7 or later versions.</p> | Mesh | All platforms | AOS-W Instant 8.3.0.7 |
| AOS-195789 | — | <p>Symptom: An OAW-IAP reported high channel usage on the 5GHz radio. The debug logs showed high number of radio resets. The fix ensures that the OAW-IAP works as expected.</p> <p>Scenario: This issue was observed in OAW-AP377 access points running AOS-W Instant 8.4.0.1 or later versions.</p> | Wi-Fi Driver | OAW-AP377 access points | AOS-W Instant 8.4.0.1 |
| AOS-197205 | — | <p>Symptom: An OAW-IAP crashed and rebooted unexpectedly. The fix ensures that the AP does not reboot unexpectedly and works as expected.</p> <p>Scenario: This issue occurred under the following conditions:</p> <ul style="list-style-type: none"> ■ When a client connected to an SSID configured with bandwidth limit contracts. ■ When the OAW-IAP used cellular uplink for internet connectivity. <p>This issue was observed in APs running AOS-W Instant 8.5.0.0 or later versions.</p> | 3G/4G Management | All platforms | AOS-W Instant 8.5.0.0 |
| AOS-197245 AOS-197374 | — | <p>Symptom: The Facebook configuration link in the Configuration > Network > Security page was not displayed. The fix ensures that the Facebook configuration link is displayed in the webUI.</p> <p>Scenario: This issue was observed in APs running AOS-W Instant 8.4.0.6 or later versions.</p> | WebUI | All platforms | AOS-W Instant 8.4.0.6 |

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

Limitations

This section describes the limitations in this release.

DNS Traffic Policy Limitation

In releases prior to AOS-W Instant 8.4.0.0, different traffic policies could be applied to AP DNS traffic and client DNS traffic. That is, the AP DNS traffic would always take the next-hop through the management network or VLAN.

In AOS-W Instant 8.5.0.0, due to the implementation of a new NAT model, whenever a configured client data path subnet route (not a default route) overlaps with the AP DNS server, the AP DNS traffic will take the same next-hop path as the client DNS server or data traffic instead of the management VLAN. This behavior will be addressed in a future AOS-W Instant release.

Fast BSS Transition

802.11r feature is not supported in WLAN SSIDs using WPA3 security.

Known Issues

The following known issues are observed in this release.



Since we have migrated to a new defect tracking tool, we have listed both, the old and the new bug ids for tracking purposes.

Table 5: Known Issues in AOS-W Instant 8.5.0.7

| New Bug ID | Old Bug ID | Description | Component | Platform | Reported Version |
|--|--|--|--------------|--|-----------------------|
| AOS-140296 AOS-143139 AOS-143162 AOS-143164 AOS-172741 AOS-172788 AOS-173084 AOS-173839 AOS-174078 | 170643 174326 174359 174361 151748 151871 152748 156758 157826 | <p>Symptom: An OAW-IAP reboots unexpectedly. The log file lists the reason for the event as Reboot caused by kernel panic: softlockup: hung tasks.</p> <p>Scenario: This issue occurs when DMO is enabled. This issue is observed in APs running in AOS-W Instant 8.3.0.0 or later versions.</p> <p>Workaround: None.</p> | Datapath | All platforms | AOS-W Instant 8.3.0.0 |
| AOS-185064 | — | <p>Symptom: An OAW-IAP fails to stop clients from connecting to a rogue AP.</p> <p>Scenario: This issue is observed in APs running AOS-W Instant 8.3.0.0 or later versions.</p> <p>Workaround: Reboot the AP working as the Spectrum Monitor.</p> | IDS | All platforms | AOS-W Instant 8.3.0.0 |
| AOS-186192 | — | <p>Symptom: Clients experience connectivity issues when configured to receive its IP address from the Local or Distributed, L3 DHCP scope.</p> <p>Scenario: This issue occurs when the uplink-vlan is configured and ARP table entry for default gateway of master OAW-IAP ages out. This issue is observed in APs running AOS-W Instant 8.4.0.1 or later versions.</p> <p>Workaround: Clear the ARP entry for the default gateway in the master OAW-IAP.</p> | Datapath | All platforms | AOS-W Instant 8.4.0.1 |
| AOS-189484 AOS-189491 | — | <p>Symptom: Wired clients experience connectivity issues with OAW-IAPs using Wi-Fi uplink.</p> <p>Scenario: This issue occurs when enet0 bridging is enabled. This issue is observed in OAW-AP300 Series, OAW-AP310 Series, OAW-AP320 Series, and OAW-AP330 Series access points running AOS-W Instant 8.5.0.0 or later versions.</p> <p>Workaround: Reconfigure the wired port profile on the OAW-IAP in the Configuration > Networks page of the WebUI.</p> | Wi-Fi Uplink | OAW-AP300 Series, OAW-AP310 Series, OAW-AP320 Series, and OAW-AP330 Series access points | AOS-W Instant 8.5.0.0 |

Table 5: Known Issues in AOS-W Instant 8.5.0.7

| New Bug ID | Old Bug ID | Description | Component | Platform | Reported Version |
|------------|------------|---|----------------|--------------------------|-----------------------|
| AOS-190089 | — | <p>Symptom: An OAW-IAP classifies YouTube application traffic as UDP traffic and not YouTube app traffic.</p> <p>Scenario: This issue is observed in APs running AOS-W Instant 8.4.0.3 or later versions.</p> <p>Workaround: None.</p> | AppRF | All platforms | AOS-W Instant 8.4.0.3 |
| AOS-190211 | — | <p>Symptom: Wired clients of an Ethernet interface experience connectivity issues when other Ethernet ports are shut down because of loop protection.</p> <p>Scenario: This issue is observed in OAW-AP303H access points running AOS-W Instant 8.3.0.0 or later versions.</p> <p>Workaround: None.</p> | Datapath | OAW-AP303H access points | AOS-W Instant 8.3.0.0 |
| AOS-191329 | — | <p>Symptom: The output of show running-configuration command does not include IPM configuration logs.</p> <p>Scenario: This issue is observed in APs running AOS-W Instant 8.5.0.1 or later versions.</p> <p>Workaround: None.</p> | Configuration | All platforms | AOS-W Instant 8.5.0.1 |
| AOS-193088 | — | <p>Symptom: The client list registers the device name as the user name for some users in the post authentication role.</p> <p>Scenario: This issue occurs when the client roams to a different AP before the username is updated in the CLI. This issue is observed in APs running AOS-W Instant 8.5.0.0 or later versions.</p> <p>Workaround: None.</p> | Authentication | All platforms | AOS-W Instant 8.5.0.0 |
| AOS-196704 | — | <p>Symptom: An OAW-IAP acting as a mesh portal crashes and reboots. The log file lists the reason as: Reboot caused by kernel panic: Rebooting the AP because of FW ASSERT.</p> <p>Scenario: This issue is observed in APs running AOS-W Instant 8.5.0.2 or later versions.</p> <p>Workaround: None.</p> | Platform | All platforms | AOS-W Instant 8.5.0.2 |
| AOS-198275 | — | <p>Symptom: 802.1x reauthentication fails when 802.1x authentication and Captive Portal web authentication is configured on the role.</p> <p>Scenario: This issue is observed in OAW-AP303 access points running AOS-W Instant 8.3.0.7 or later versions.</p> <p>Workaround: None.</p> | Authentication | OAW-AP303 access points | AOS-W Instant 8.3.0.7 |

Table 5: *Known Issues in AOS-W Instant 8.5.0.7*

| New Bug ID | Old Bug ID | Description | Component | Platform | Reported Version |
|------------|------------|--|--------------|--------------------------|-----------------------|
| AOS-198363 | — | <p>Symptom: Clients are either unable to connect to the AP or are getting disconnected when the SAPD process over utilizes memory.</p> <p>Scenario: This issue is observed in OAW-IAP324 access points running AOS-W Instant 8.3.0.7 or later versions.</p> <p>Workaround: None.</p> | Wi-Fi Driver | OAW-IAP324 access points | AOS-W Instant 8.3.0.7 |
| AOS-198931 | — | <p>Symptom: Some APs are unable to join the cluster when the software version is upgraded to AOS-W Instant 8.5.0.5.</p> <p>Scenario: This issue occurs when the software version was upgraded from AOS-W Instant 8.4.0.4 to 8.5.0.5 on the cluster. This issue is observed in APs running AOS-W Instant 8.5.0.5 or later versions.</p> <p>Workaround: None.</p> | Datapath | All platforms | AOS-W Instant 8.5.0.5 |
| AOS-199471 | — | <p>Symptom: Wireless clients are getting disconnected when roaming from one AP to another in the cluster.</p> <p>Scenario: This issue occurs because the clients are unable to get an IP address while roaming. This issue is observed in OAW-AP515 access points running AOS-W Instant 8.5.0.5 or later versions.</p> <p>Workaround: None.</p> | Wi-Fi Driver | OAW-AP515 access points | AOS-W Instant 8.5.0.5 |

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

Topics in this chapter include:

- [Upgrading an OAW-IAP Using OmniVista 3600 Air Manager Management Platform on page 22](#)
- [Upgrading an OAW-IAP Image Manually Using WebUI on page 23](#)
- [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 8.5.0.x on page 26](#)

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

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

HTTP Proxy Support through Zero Touch Provisioning

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

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

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

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

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

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

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

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

Rolling Upgrade on OAW-IAPs with OmniVista 3600 Air Manager

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

Upgrading an OAW-IAP Image Manually Using WebUI

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

In the Old WebUI

To manually check for a new firmware image version and obtain an image file:

1. Navigate to **Maintenance > Firmware**.
2. Under **Manual** section, perform the following steps:
 - Select the **Image file** option. This method is only available for single-class OAW-IAPs.

The following table describes the supported image file format for different OAW-IAP models:

| Access Points | Image File Format |
|--|---------------------------------------|
| OAW-RAP155 and OAW-RAP155P | AlcatelInstant_Aries_8.5.0.x_xxxx |
| OAW-IAP214, OAW-IAP215, OAW-IAP224, OAW-IAP225, OAW-IAP228, OAW-IAP274, OAW-IAP275 and OAW-IAP277 | AlcatelInstant_Centaurus_8.5.0.x_xxxx |
| OAW-IAP314, OAW-IAP315, OAW-IAP324, OAW-IAP325, OAW-AP374, OAW-AP375, OAW-AP377, OAW-AP318 and OAW-AP387 | AlcatelInstant_Hercules_8.5.0.x_xxxx |
| OAW-IAP334 and OAW-IAP335 | AlcatelInstant_Lupus_8.5.0.x_xxxx |

| Access Points | Image File Format |
|---|-------------------------------------|
| OAW-RAP108, OAW-RAP109, OAW-IAP103, OAW-IAP114 and OAW-IAP115 | AlcatelInstant_Pegasus_8.5.0.x_xxxx |
| OAW-AP303, OAW-AP303H, 303P Series, OAW-IAP304, OAW-IAP305, OAW-AP365 and OAW-AP367 | AlcatelInstant_Ursa_8.5.0.x_xxxx |
| OAW-AP203H, OAW-AP203R, OAW-AP203RP and OAW-IAP207 | AlcatelInstant_Vela_8.5.0.x_xxxx |
| OAW-AP344, OAW-AP345, OAW-AP514 and OAW-AP515 | AlcatelInstant_Draco_8.5.0.x_xxxx |
| OAW-AP534, OAW-AP535 and OAW-AP555 | AlcatelInstant_Scorpio_8.5.0.x_xxxx |

- Select the **Image URL** option. Select this option to obtain an image file from a HTTP, TFTP, or FTP URL.
 - HTTP - http://<IP-address>/<image-file>. For example, http://<IP-address>/AlcatelInstant_Hercules_8.5.0.x_xxxx
 - TFTP - tftp://<IP-address>/<image-file>. For example, tftp://<IP-address>/AlcatelInstant_Hercules_8.5.0.x_xxxx
 - FTP - ftp://<IP-address>/<image-file>. For example, ftp://<IP-address>/AlcatelInstant_Hercules_8.5.0.x_xxxx
 - FTP - ftp://<user name:password>@<IP-address>/<image-file>. For example, ftp://<alcatel:123456>@<IP-address>/AlcatelInstant_Hercules_8.5.0.x_xxxx



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

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

3. Clear the **Reboot all APs after upgrade** check box if required. This check box is selected by default to allow the OAW-IAPs to reboot automatically after a successful upgrade. To reboot the OAW-IAP at a later time, clear the **Reboot all APs after upgrade** check box.
4. Click **Upgrade Now** to upgrade the OAW-IAP to the newer version.

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

To manually check for a new firmware image version and obtain an image file:

1. Navigate to **Maintenance > Firmware**.
2. Under **Manual** section, perform the following steps:
 - Select the **Image file** option. This method is only available for single-class OAW-IAPs.

The following table describes the supported image file format for different OAW-IAP models:

| Access Points | Image File Format |
|--|---------------------------------------|
| OAW-RAP155 and OAW-RAP155P | AlcatelInstant_Aries_8.5.0.x_xxxx |
| OAW-IAP214, OAW-IAP215, OAW-IAP224, OAW-IAP225, OAW-IAP228, OAW-IAP274, OAW-IAP275 and OAW-IAP277 | AlcatelInstant_Centaurus_8.5.0.x_xxxx |
| OAW-IAP314, OAW-IAP315, OAW-IAP324, OAW-IAP325, OAW-AP374, OAW-AP375, OAW-AP377, OAW-AP318 and OAW-AP387 | AlcatelInstant_Hercules_8.5.0.x_xxxx |
| OAW-IAP334 and OAW-IAP335 | AlcatelInstant_Lupus_8.5.0.x_xxxx |
| OAW-RAP108, OAW-RAP109, OAW-IAP103, OAW-IAP114 and OAW-IAP115 | AlcatelInstant_Pegasus_8.5.0.x_xxxx |
| OAW-AP303, OAW-AP303H, 303P Series, OAW-IAP304, OAW-IAP305, OAW-AP365 and OAW-AP367 | AlcatelInstant_Ursa_8.5.0.x_xxxx |
| OAW-AP203H, OAW-AP203R, OAW-AP203RP and OAW-IAP207 | AlcatelInstant_Vela_8.5.0.x_xxxx |
| OAW-AP344, OAW-AP345, OAW-AP514 and OAW-AP515 | AlcatelInstant_Draco_8.5.0.x_xxxx |
| OAW-AP534, OAW-AP535 and OAW-AP555 | AlcatelInstant_Scorpio_8.5.0.x_xxxx |

- Select the **Image URL** option. Select this option to obtain an image file from a HTTP, TFTP, or FTP URL.
 - HTTP - http://<IP-address>/<image-file>. For example, http://<IP-address>/AlcatelInstant_Hercules_8.5.0.x_xxxx
 - TFTP - tftp://<IP-address>/<image-file>. For example, tftp://<IP-address>/AlcatelInstant_Hercules_8.5.0.x_xxxx
 - FTP - ftp://<IP-address>/<image-file>. For example, ftp://<IP-address>/AlcatelInstant_Hercules_8.5.0.x_xxxx
 - FTP - ftp://<user name:password>@<IP-address>/<image-file>. For example, ftp://alcatel:123456@<IP-address>/AlcatelInstant_Hercules_8.5.0.x_xxxx



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

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

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

5. Click **Save**.

Upgrading an OAW-IAP Image Manually Using CLI

To upgrade an image using a HTTP, TFTP, or FTP URL:

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

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

```
(Instant AP)# upgrade-image ftp://192.0.2.7/AlcatelInstant_Hercules_8.5.0.x_xxxx
```

To upgrade an image without rebooting the OAW-IAP:

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

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

```
(Instant AP)# upgrade-image2-no-reboot ftp://192.0.2.7/AlcatelInstant_Hercules_8.5.0.x_xxxx
```

To view the upgrade information:

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

Upgrade from AOS-W Instant 6.4.x.x-4.2.x.x to AOS-W Instant 8.5.0.x

Before you upgrade an OAW-IAP running AOS-W Instant 6.5.4.0 or earlier versions to AOS-W Instant 8.5.0.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](#).
3. Verify the affected serial numbers of the OAW-IAP units.