

AOS-W Instant 8.5.0.5



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. (2019)

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, 530 Series, and OAW-AP535 Access Points	8
Enhancements to Uplink Ports of OAW-AP318 and OAW-AP370 Series Access Points	9
Supported Hardware Platforms	11
Supported OAW-IAPs	11
Regulatory Updates	13
Resolved Issues	14
Known Issues	17
Upgrading an OAW-IAP	23
Upgrading an OAW-IAP Using OmniVista 3600 Air Manager Management Platform	23
Upgrading an OAW-IAP Image Manually Using WebUI	24

Upgrading an OAW-IAP Image Manually Using CLI	27
Upgrade from AOS-W Instant 6.4.x.x-4.2.x.x to AOS-W Instant 8.5.0.x	27

Revision History

The following table provides the revision history of this document.

Table 1: *Revision History*

Revision	Change Description
Revision 03	AOS-W Instant Certificate Expiry Issue is added to the New Features and Enhancements chapter.
Revision 02	AOS-195357 added to the list of Resolved Issues .
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 17](#)
- [Upgrading an OAW-IAP on page 23](#)

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

Supported Browsers

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

- Microsoft Internet Explorer 11 on Windows 7 and Windows 8
- Microsoft Edge (Microsoft Edge 38.14393.0.0 and Microsoft 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 (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 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 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-20191218-PLVL01](#).

Dual Uplink for OAW-AP318, OAW-AP340 Series, OAW-AP370 Series, OAW-AP510 Series, 530 Series, and OAW-AP535 Access Points

Starting from AOS-W Instant 8.5.0.3, OAW-AP318, OAW-AP340 Series, OAW-AP370 Series, OAW-AP510 Series, 530 Series, and OAW-AP535 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, 530 Series, and OAW-AP535 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.

This chapter describes the hardware platforms supported in this release.

Supported OAW-IAPs

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

Table 3: *Supported OAW-IAP Platforms*

OAW-IAP Platform	Minimum Required AOS-W Instant Software Version
<ul style="list-style-type: none"> ■ 530 Series — OAW-AP534 and OAW-AP535 ■ 550 Series — OAW-AP535 	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

Table 3: *Supported OAW-IAP Platforms*

OAW-IAP Platform	Minimum Required AOS-W Instant Software Version
<ul style="list-style-type: none">■ OAW-IAP228■ OAW-IAP277	AOS-W Instant 6.4.3.1-4.2.0.0 or later
<ul style="list-style-type: none">■ OAW-AP210 Series — OAW-IAP214 and OAW-IAP215	AOS-W Instant 6.4.2.0-4.1.1.0 or later
<ul style="list-style-type: none">■ OAW-AP270 Series — OAW-IAP274 and OAW-IAP275	AOS-W Instant 6.4.0.2-4.1.0.0 or later
<ul style="list-style-type: none">■ OAW-AP 220 Series — OAW-IAP224 and OAW-IAP225	AOS-W Instant 6.3.1.1-4.0.0.0 or later
<ul style="list-style-type: none">■ 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_73310

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 8.5.0.5

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-180241	188464	<p>Symptom: Some clients were unable to connect to the access point. The log file listed the reason for the event as AP is resource constrained. The fix ensures that sticky clients are not steered away from the band if three connection attempts are made in two minutes.</p> <p>Scenario: This issue occurred when sticky clients were trying to connect to a particular band and band steering was configured to move clients to a different band. This issue was observed in access points running AOS-W Instant 8.3.0.0 or later versions.</p>	ClientMatch	All platforms	AOS-W Instant 8.3.0.0
AOS-184780 AOS-190165 AOS-191082	—	<p>Symptom: An OAW-IAP forwarded DNS requests to the internal DNS server instead of the public DNS server configured. The fix ensures that DNS requests are forwarded to the correct server as per the VPN configuration.</p> <p>Scenario: This issue occurred because the AP performed DNS proxy for local DHCP clients irrespective of the VPN configuration. This issue was observed in access points running AOS-W Instant 8.3.0.0 or later versions.</p>	Datapath	All platforms	AOS-W Instant 8.3.0.0
AOS-186512	—	<p>Symptom: An OAW-IAP sent incorrect client MAC addresses to the Switch and the Switch sent MAC authentication requests to the RADIUS server based on these MAC addresses. Enhancement to the wireless driver ensures that invalid MAC authentication requests are not sent to the RADIUS server.</p> <p>Scenario: This issue occurred with clients using Intel 8260 wireless chipset and when the Switch terminating the OAW-IAP had MAC authentication enabled. This issue was observed in access points running AOS-W Instant 8.3.0.0 or later versions.</p>	Wi-Fi Driver	All platforms	AOS-W Instant 8.3.0.0

Table 4: Resolved Issues in AOS-W Instant 8.5.0.5

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-187514	—	Symptom: The download performance of the AP reduced when AppRF was enabled. The fix ensures that the performance of the access point does not reduce when AppRF is enabled. Scenario: This issue was observed in access points running AOS-W Instant 8.4.0.0 or later versions.	AppRF	All platforms	AOS-W Instant 8.4.0.0
AOS-189166	—	Symptom: The WebUI was unresponsive when AirGroup services was selected in the Configuration > Services > AirGroup > AirGroup settings page. The fix ensures that the WebUI works as expected. Scenario: This issue was observed in access points running AOS-W Instant 8.3.0.0 or later versions.	AirGroup	All platforms	AOS-W Instant 8.3.0.0
AOS-190255	—	Symptom: The IP address of the client was displayed in hexadecimal format in the debug logs. The fix ensures that the IP address is displayed in the decimal format. Scenario: This issue was observed in access points running AOS-W Instant 8.4.0.2 or later versions.	Platform	All platforms	AOS-W Instant 8.4.0.2
AOS-192108	—	Symptom: An OAW-IAP could not connect to Activate through proxy. The fix ensures that the AP connects to Activate as expected. Scenario: This issue was observed in access points running AOS-W Instant 8.3.0.0 or later versions.	Activate	All platforms	AOS-W Instant 8.3.0.0
AOS-193434	—	Symptom: The OAW-IAP did not switch the primary uplink back to eth0 from the secondary 3G/4G uplink when the Ethernet link was restored after a failover. The fix ensures that the primary uplink switches to the higher priority uplink, when the uplink is active. Scenario: This issue was observed in access points running AOS-W Instant 8.4.0.2 or later versions.	Datapath	All platforms	AOS-W Instant 8.4.0.2
AOS-193910	—	Symptom: An OFALD process crash was observed on the OAW-IAP. The fix ensures that the AP works as expected. Scenario: This issue was observed in access points running AOS-W Instant 8.5.0.3 or later versions.	OFA	All platforms	AOS-W Instant 8.5.0.3

Table 4: Resolved Issues in AOS-W Instant 8.5.0.5

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-194772	—	<p>Symptom: iPhone 11 devices connected to an OAW-IAP did not receive an IP address. The fix ensures that iPhone 11 devices receive the IP address from the OAW-IAP.</p> <p>Scenario: This issue occurred when 802.1X authentication and Fast BSS Transition was enabled on the SSID. This issue was observed in OAW-AP510 Series, 530 Series and 550 Series access points running AOS-W Instant 8.5.0.0 or later versions.</p>	Platform	OAW-AP510 Series, 530 Series, and 550 Series access points	AOS-W Instant 8.5.0.0
AOS-195009 AOS-195357	—	<p>Symptom: Clients were assigned incorrect roles. The fix ensures that the clients are assigned correct user roles.</p> <p>Scenario: This issue occurred when the access point was moved to a different AP group. This issue was observed in access points running AOS-W Instant 8.3.0.0 or later versions.</p>	L2 Mobility	All platforms	AOS-W Instant 8.3.0.0
AOS-195169	—	<p>Symptom: An OAW-IAP crashed and the log file listed the reason as Reboot caused by kernel panic: softlockup: hung tasks. The fix ensures that the AP works as expected.</p> <p>Scenario: This issue occurred due to CPU overload when there was heavy upstream bridge traffic. This issue was observed in 530 Series and OAW-AP535 access points running AOS-W Instant 8.5.0.0 or later versions.</p>	Datapath	530 Series and OAW-AP535 access points	AOS-W Instant 8.5.0.0

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 8.5.0.5

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 access points 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 access points 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 access points running AOS-W Instant 8.4.0.1 or later versions.</p> <p>Workaround: Clear the ARP entry for the default gateway in Master OAW-IAP.</p>	Datapath	All platforms	AOS-W Instant 8.4.0.1
AOS-187268	—	<p>Symptom: An OAW-IAP crashes and reboots unexpectedly. The log files list the reason for the event as Reboot caused by kernel panic: Fatal exception.</p> <p>Scenario: This issue occurs when 802.11w standard is enabled on the OAW-IAP. This issue is observed in access points running AOS-W Instant 8.3.0.0 or later versions.</p> <p>Workaround: None.</p>	Wi-Fi Driver	All platforms	AOS-W Instant 8.3.0.0

Table 5: Known Issues in AOS-W Instant 8.5.0.5

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
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
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 access points 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 access points 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 access points 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

Table 5: Known Issues in AOS-W Instant 8.5.0.5

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-193901 AOS-196256	—	Symptom: Some smartphone clients are unable to authenticate to guest SSIDs with Enhanced Open security. Scenario: This issue is observed in access points running AOS-W Instant 8.4.0.2 or later versions. Workaround: None.	Authentication	All platforms	AOS-W Instant 8.4.0.2
AOS-193977	—	Symptom: A slave OAW-IAP fails to synchronize its configuration with the master OAW-IAP. Scenario: This issue occurs due to a checksum error between the master AP and the slave AP triggered due to an issue in the uplink manager. This issue is observed in OAW-AP318 and OAW-AP370 Series access points running AOS-W Instant 8.5.0.3. Workaround: Use one of the following workarounds: <ul style="list-style-type: none">■ Remove the uplink priority from OAW-AP318 or OAW-AP370 Series access points before upgrading to AOS-W Instant 8.5.0.3.■ Assign a non-default wired port profile on eth1 before upgrading to AOS-W Instant 8.3.0.5.	VC Management	OAW-AP318 and OAW-AP370 Series access points	AOS-W Instant 8.5.0.3
AOS-194553	—	Symptom: An OAW-IAP becomes unresponsive and the show ap debug crash-info command returns the message: Module SAPM Client is busy. Please try later. Scenario: This issue is observed in OAW-AP340 Series access points running AOS-W Instant 8.5.0.3 or later versions. Workaround: Limit the number of virtual access points on the AP to 15.	Wi-Fi Driver	OAW-AP340 Series access points	AOS-W Instant 8.5.0.3

Table 5: Known Issues in AOS-W Instant 8.5.0.5

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-194703	—	<p>Symptom: An AP occupies two DHCP leases when converted to a OAW-AP.</p> <p>Scenario: This issue occurs when both Ethernet ports of the AP are connected to the Switch. The first IP address is allocated during the OAW-IAP phase and the second IP address is allocated during the OAW-AP phase. This issue is observed in OAW-AP318 and OAW-AP370 Series access points running AOS-W Instant 8.5.0.0 or later versions.</p> <p>Workaround: Use any of the following workarounds:</p> <ul style="list-style-type: none"> ■ Allocate a sufficiently large pool to cover the excess DHCP lease per AP. ■ Use a short-lived lease time during initial deployment. ■ Deploy APs in batches to prevent exhaustion of IP addresses in the DHCP pool. 	Platform	OAW-AP318 and OAW-AP370 Series access points	AOS-W Instant 8.5.0.0
AOS-194725	—	<p>Symptom: The master AP loses its configuration to a new AP joining the cluster.</p> <p>Scenario: This issue occurs when the master AP has no user configured SSID profile and preferred-master setting is not enabled. The new AP joining the VLAN assumes the role of the master AP and overwrites its configuration, if it has custom SSIDs configured. This issue is observed in access points running AOS-W Instant 8.5.0.3.</p> <p>Workaround: Set Preferred Master to Enabled in the Access Point > Edit > General page in the old WebUI or Configuration > Access Point > edit > Uplink page in the New WebUI of the master AP.</p>	VC Management	All platforms	AOS-W Instant 8.5.0.3
AOS-194736	—	<p>Symptom: The eth1 interface of the factory default AP does not connect to the uplink switch in the same VLAN as the eth0 interface and affects the controller discovery process.</p> <p>Scenario: This issue is observed in OAW-AP340 Series, OAW-AP510 Series, 530 Series, and OAW-AP535 access points running AOS-W Instant 8.5.0.0 or later versions.</p> <p>Workaround: Disconnect eth1 from the uplink switch before logging into the CLI or WebUI, if LACP or active/standby dual uplink mode is configured and factory reset the AP.</p>	UAP	OAW-AP340 Series, OAW-AP510 Series, 530 Series, and OAW-AP535 access points	AOS-W Instant 8.5.0.0

Table 5: *Known Issues in AOS-W Instant 8.5.0.5*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-195491	—	Symptom: An OAW-IAP randomly generates OFALD messages and affects the quality of the network. Scenario: This issue is observed in access points running AOS-W Instant 8.3.0.7 or later versions. Workaround: None.	OFA	All platforms	AOS-W Instant 8.3.0.7

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 23](#)
- [Upgrading an OAW-IAP Image Manually Using WebUI on page 24](#)
- [Upgrading an OAW-IAP Image Manually Using CLI on page 27](#)
- [Upgrade from AOS-W Instant 6.4.x.x-4.2.x.x to AOS-W Instant 8.5.0.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.

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-AP535	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-AP535	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.