AOS-W Instant 8.10.0.15

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:

- New Features and Enhancements
- Supported Platforms
- Regulatory Updates
- Resolved Issues
- Known Issues and Limitations
- Upgrade Procedure

For the list of terms, refer to the Glossary.

Related Documents

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

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

Supported Browsers

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

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

Terminology Change

As part of advancing HPE's commitment to racial justice, we are taking a much-needed step in overhauling HPE engineering terminology to reflect our belief system of diversity and inclusion. Some legacy products and publications may continue to include terminology that seemingly evokes bias against specific groups of people. Such content is not representative of our HPE culture and moving forward, Alcatel-Lucent will replace racially insensitive terms and instead use the following new language:

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

Contacting Support

Table 2: *Contact Information*

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

Chapter 2
What's New

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

Certificate Handling Process

AOS-W Instant.10.0.15 improves the certificate handling process by searching the Subject Alternate Name (SAN) field to encode the FQDN when there is no Common Name (CN) included in the certificate.

Larger Tech Support Logs

AOS-W Instant.10.0.15 improves the byte length of tech support logs.

Behavioral Changes

This release does not introduce any changes in AOS-W Instant behaviors, resources, or support that requires modifying the existing system configurations after updating to 8.10.0.15.

Chapter 3
Supported Platforms

Supported Platforms in AOS-W Instant.x

This section displays the supported platforms in AOS-W Instant.x. The **minimum version supported** column displays the minimum AOS-W Instant.x version that can be run on a platform. The **latest version supported** column displays the newest AOS-W Instant.x version that can be run on a certain device. Patch releases do not affect platform support. For example, a device which **latest supported version** is 8.10.0.x can run on any 8.10.0.x version, such as 8.10.0.2 or 8.10.0.10.

Access Point Platforms

Access Points			AOS-W Instant Versions Supported	
AP Family	**AP Series**	**AP Model**	**Minimum**	**Latest**
6xx	670 Series	AP-675, AP-675EX, AP-677, AP-677EX, AP-679, AP-679EX	8.12.0.x	AOS-W Instant 8.12.0.x
	OAW-650 Series	OAW-AP655	8.10.0.x	AOS-W Instant 8.12.0.x
		AP-654	8.11.2.x	AOS-W Instant 8.12.0.x
	OAW-630 Series	OAW-AP635	8.9.0.x	AOS-W Instant 8.12.0.x
		AP-634	8.11.2.x	AOS-W Instant 8.12.0.x
	610 Series	AP-615	8.11.0.x	AOS-W Instant 8.12.0.x
	600 Series	AP-605H	8.12.0.x	AOS-W Instant 8.12.0.x

Access Points			AOS-W Instant Versions Supported	
AP Family	**AP Series**	**AP Model**	**Minimum**	**Latest**
5xx	OAW-580 Series	OAW-AP-584, OAW-AP585, OAW-AP585EX, OAW-AP587, OAW-AP587EX	8.10.0.x	AOS-W Instant 8.12.0.x
	OAW-AP570 Series	OAW-AP574, OAW-AP575, OAW-AP577	8.7.0.x	AOS-W Instant 8.12.0.x
	OAW-560 Series	OAW-AP565, OAW-AP567	8.7.1.x	AOS-W Instant 8.12.0.x
	OAW-AP550 Series	OAW-AP535	8.5.0.x	AOS-W Instant 8.12.0.x
	OAW-AP530 Series	OAW-AP534, OAW-AP535	8.5.0.x	AOS-W Instant 8.12.0.x
	OAW-AP510 Series	OAW-AP518	8.7.0.x	AOS-W Instant 8.12.0.x
		OAW-AP514, OAW-AP515	8.4.0.x	AOS-W Instant 8.12.0.x
	OAW-AP500 Series	OAW-AP504, OAW-AP505	8.6.0.x	AOS-W Instant 8.12.0.x
		OAW-AP505H	8.7.0.x	AOS-W Instant 8.12.0.x
		OAW-AP503H	8.7.1.x	AOS-W Instant 8.12.0.x
		AP-503	8.11.1.x	AOS-W Instant 8.12.0.x

Access Points			AOS-W Instant Versions Supported	
AP Family	**AP Series**	**AP Model**	**Minimum**	**Latest**
3xx	380 Series	OAW-AP387	8.4.0.x	8.10.0.x
	OAW-AP370 Series	OAW-AP374, OAW-AP375, OAW-AP377, AP-375EX, AP-377EX, AP-375ATEX	8.3.0.x	AOS-W Instant 8.12.0.x
	OAW-AP360 Series	OAW-AP365, OAW-AP367	8.3.0.x	AOS-W Instant 8.12.0.x
	OAW-AP340 Series	OAW-AP344, OAW-AP345	8.3.0.x	8.10.0.x
	OAW-AP330 Series	OAW-AP334, OAW-AP335	8.1.0.x	8.10.0.x
	OAW-AP320 Series	OAW-APAP-324, OAW-AP325	8.0.0.x	8.10.0.x
	OAW-AP310 Series	OAW-AP318	8.3.0.x	AOS-W Instant 8.12.0.x
		OAW-AP314, OAW-AP315	8.1.0.x	AOS-W Instant 8.12.0.x
	OAW-AP300 Series	OAW-AP304, OAW-AP305	8.1.0.x	AOS-W Instant 8.12.0.x
		OAW-AP303H, AP-303HR	8.2.0.x	AOS-W Instant 8.12.0.x
		OAW-AP303P	8.4.0.x	AOS-W Instant 8.12.0.x
		OAW-AP303	8.3.0.x	AOS-W Instant 8.12.0.x
2xx	OAW-AP270 Series	OAW-AP274, OAW-AP275, OAW-AP277	8.0.0.x	8.6.0.x
	OAW-AP 220 Series	OAW-AP224, OAW-AP225, OAW-AP228	8.0.0.x	8.6.0.x
	OAW-AP210 Series	OAW-AP214, OAW-AP215	8.0.0.x	8.6.0.x
	OAW-AP200 Series	OAW-AP207	8.1.0.x	8.6.0.x
		OAW-AP203H, OAW-AP203R, OAW-AP203RP	8.2.0.x	8.6.0.x

Chapter 4
Regulatory Updates

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

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

For a complete list of countries and the regulatory domains in which the APs are certified for operation, refer to the Downloadable Regulatory Table or the DRT Release Notes at networkingsupport.hpe.commyportal.al-enterprise.com.

The following DRT file version is part of this release:

- DRT-1.0_91171

Chapter 5
Resolved Issues

The following issues are resolved in this release.

Table 3: *Resolved Issues in AOS-W Instant.10.0.15*

Bug ID	Description	Reported Version
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.6.0.4 or later versions.	AOS-W Instant.6.0.4
AOS-244911 AOS-257416	In some OAW-AP515 access points, client devices were unable to connect to the network from an **auth-text** Captive Portal with an active proxy port. This issue occurred when the Captive Portal configuration was not correctly reloaded after the AP rebooted. The output of the **show captive-portal** command showed **External proxy ports active: No** after the reboot. The fix ensures that client devices are able to connect the network from an **auth-text** Captive Portal with an active proxy port as expected. This issue was observed in APs running AOS-W Instant.10.0.0 or later versions.	AOS-W Instant.10.0.0
AOS-253692	Xerox C415 printers were unable to obtain an IP addresses via DHCP when connected to some APs, which was related to the options in DHCP packets for certain clients. The fix ensures the process works as expected. This issue was observed in OAW-AP303H access points running AOS-W Instant.11.2.1 or later versions.	AOS-W Instant.11.2.1
AOS-254606	In some APs, client devices did not receive a valid IP address from the external DHCP server when the client was connected to an SSID with time range configured as an ACL rule. This issue occurred when the DHCP lease time expired on the client side or the AP was rebooted. The fix ensures the APs work as expected. This issue was observed in OAW-AP535 access points running AOS-W Instant.10.0.11 or later versions.	AOS-W Instant.10.0.11
AOS-255120 AOS-257695	Some ad-hoc nodes were incorrectly detected as **Adhoc network using valid SSID**. The fix ensures the process works as expected. This issue was observed in APs running AOS-W Instant.12.0.0 or later versions.	AOS-W Instant.12.0.0
AOS-256621	The Hanshow USB dongle was unable to obtain an IP address after upgrading to AOS-W Instant.10.0.12 or later versions. The fix ensures the IP address is correctly assigned.	AOS-W Instant.10.0.12
AOS-257056	Disabling the mesh portal caused mesh point ESSIDs to be unavailable. The fix ensures the mesh points work as expected. This issue is observed in APs running AOS-W Instant.10.0.13 or later versions.	AOS-W Instant.10.0.13

Table 3: *Resolved Issues in AOS-W Instant.10.0.15*

Bug ID	Description	Reported Version
AOS-257181	OAW-IAPs did not send NAS Identifier details when **Key Management** was set to **Enhanced Open** and **WPA3 Transition** mode was **ON**. This issue occurred when the NAS Identifier was missed in the redirect URL. The fix ensures that APs send the NAS Identifier. This issue was observed in APs running AOS-W Instant.12.0.0 or later versions.	AOS-W Instant.12.0.0
AOS-258064	Clients could not 11r roam to WPA3-AES-CCM-128 VAPs on the 6 GHz band. This issue occurred when a deauthentication frame was sent to the target AP with **Reason 13 = Invalid Information Element** after receiving the 802.11r reassociation response. The client eventually did an initial full dot1x association with the 802.11r VAP. The fix ensures that the 802.11r reassociation response is valid according to the 802.11 specification. This issue was observed in 6 GHz APs running AOS-W Instant.6.0.0 or later versions.	AOS-W Instant.10.0.14
AOS-258740	Interworking and Access Network Query Protocol (ANQP) information elements were appended to all active 2.4 GHz and 5 GHz VAPs when a 6 GHz VAP was active. The fix ensures each radio band has its independent configurations. This issue was observed in APs running AOS-W Instant-8.9.0.0 or later versions.	AOS-W Instant.9.0.0

Chapter 6
Known Issues

This chapter describes the known issues observed in this release.

Limitations

This section describes the limitations in AOS-W Instant.10.0.15.

OAW-AP635 and OAW-AP655 Access Points

OAW-AP635 and OAW-AP655 access points have the following limitations:

- All radios for OAW-AP635 and OAW-AP655 access points currently do not support spectrum analysis.
- Hotspot and Air Slice configuration is not supported on the 6 GHz radio.
- 802.11mc responder and initiator functionality is not supported on any radio.
- Users can configure only up to 4 VAPs on the 6 GHz radio, instead of 16 VAPs.
- A maximum of 512 clients can be associated on any radio instead of 1024.

Air Slice

Air Slice is partially enabled on OAW-AP500 Series and OAW-AP510 Series access points. However, WMM boost will be functional even if Air Slice high-priority queuing is disabled.

Airtime Fairness Mode

Airtime Fairness Mode is not supported in 802.11ax access points.

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 and later versions:

- 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.

FIPS Mode

FIPS mode cannot be turned on or off in AOS-W Instant.10.0.11. TAA SKUs running AOS-W Instant.10.x do not support the following features:

- WEP
- PPPoE
- Wi-Fi Uplink
- L2TPv3
- PSK-based IPSec tunnels
- OpenDNS
- Telnet access
- L3 mobility
- SNMPv3

The software must be upgraded to AOS-W Instant.11.0.0 or later versions to re-enable support of the above features on TAA SKUs.

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 4: *Known Issues in AOS-W Instant.10.0.15*

Bug ID	Description	Reported Version
AOS-195769	In some OAW-IAPs set up with dynamic VLAN assignment, ARP or GARP traffic is unexpectedly sent to wireless clients, even if they are connected to a different VLAN and VAP. This issue is observed in the following scenarios: ■ When the broadcast packets from VLAN 1 and all of the clients on the SSID are on VLAN 2, the packets are sent to all VAPs belonging to the same SSID. ■ When the SSID has two VAPs that belong to the same VLAN, but only one VAP has clients on that VLAN, the traffic is forwarded to both VAPs. ■ When all of the VAPs of a given SSID have clients on different VLANs, the packets are broadcasted to all VLANs. This issue is observed in OAW-IAPs running AOS-W Instant.6.0.0 or later versions.	AOS-W Instant.6.0.0
AOS-204171	Clients intermittently experience high latency when the OAW-IAP is connected to the backup Switch after a failover event. This issue occurs under the following scenarios: ■ The AP attempts to reconnect to the primary Switch. ■ Fast failover is enabled on the AP. This issue is observed in OAW-AP203R Series access points running AOS-W Instant.3.0.0 or later versions.	AOS-W Instant.3.0.0

Table 4: *Known Issues in AOS-W Instant.10.0.15*

Bug ID	Description	Reported Version
AOS-220890	MPSK-Local SSID is broadcasted as Open SSID in OAW-IAPs when the software is downgraded to AOS-W Instant versions lower than 8.7.0.0. This issue is observed in APs running AOS-W Instant.6.0.8 or later versions.	AOS-W Instant.6.0.8
AOS-225601 AOS-224170	Some member APs in a cluster appear as **down** in the OmniVista 3600 Air Manager UI. This issue is observed in OmniVista 3600 Air Manager-managed APs running AOS-W Instant.6.0.0 or later versions.	AOS-W Instant.6.0.0
AOS-228967	Users are unable to configure the **Station Ageout Time** to a value over 3600 seconds. This issue is observed in APs running AOS-W Instant.7.1.4 or later versions.	AOS-W Instant.6.0.8
AOS-231129	AOS-W Instant APs do not send cold and warm SNMP traps when expected. This issue is observed in APs running AOS-W Instant.0.0.0 or later versions.	AOS-W Instant.6.0.8
AOS-232833	Member APs ignore the proxy configuration when trying to download firmware with the image URL provided by the virtual Switch. This issue is observed in APs running AOS-W Instant.9.0.0 or later versions.	AOS-W Instant.9.0.0
AOS-233149 AOS-235164	The OAW-IAP log generates 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. This issue is observed in APs running AOS-W Instant.7.1.9 or later versions.	AOS-W Instant.7.1.9
AOS-233215	If the TACACS server name contains a space, the AP does not save the server configuration after assigning the TACACS server as the management authentication server. The AP automatically removes the configuration when the client attempts to save the information. This issue is observed in APs running AOS-W Instant.9.0.3 or later versions.	AOS-W Instant.9.0.3
AOS-233784	When a user connects to the Captive Portal SSID in one accounting session, the RADIUS **Acct-Multi-Session-Id** changes. This issue is observed in APs running AOS-W Instant.9.0.2 or later versions.	AOS-W Instant.9.0.2
AOS-234828	OAW-IAPs in a cluster reboot automatically. The log file lists the reason for reboot as **Critical process /aruba/bin/stm [pid 26061] DIED, process marked as RESTART**. This issue is observed in APs running AOS-W Instant.9.0.3 or later versions.	AOS-W Instant.9.0.3
AOS-238137	The **traceroute** command returns the following error message: **Can't find tsgw src ip**. This issue occurs when the AP has multiple routing entries in the routing profile. This issue is observed in APs running AOS-W Instant.10.0.3 or later versions.	AOS-W Instant.10.0.3
AOS-239411	OAW-IAPs do not accept the serial number of the device as the default password after a factory reset. This issue occurs when the AP is reset using the **factory reset** command in AP boot mode. This issue is observed in APs running AOS-W Instant.9.0.0 or later versions.	AOS-W Instant.9.0.0

Table 4: *Known Issues in AOS-W Instant.10.0.15*

Bug ID	Description	Reported Version
AOS-239419	The **eth0** link of an AP appears offline in the OmniVista 3600 Air Manager UI. This issue is observed in OmniVista 3600 Air Manager-managed APs running AOS-W Instant.6.0.18 or later versions.	AOS-W Instant.6.0.18
AOS-240530	OAW-IAPs return the following error message: **auth_cppm_ instant.c, auth_cppm_transform:1859: Dldb Role pf_iap_dur-3008-26: Buffer too large**. This issue occurs when the buffer size of the downloadable user role sent from the ClearPass Policy Manager exceeds 16 KB. This issue is observed in APs running AOS-W Instant.10.0.0 or later versions.	AOS-W Instant.10.0.4
AOS-241316	The output of the **show ap debug lldp** command displays incorrect information. This issue is observed in APs running AOS-W Instant.6.0.0 or later versions.	AOS-W Instant.6.0.20
AOS-243184	An AP displays incorrect country codes in the air captured packet although the correct country code is configured on the AP. This issue is observed in APs running AOS-W Instant.10.0.5 or later versions.	AOS-W Instant.10.0.5
AOS-249946 AOS-247154	Some OAW-IAPs crash and reboot unexpectedly due to a UCM segmentation issue, which affected different VoIP applications. This issue is observed in APs running AOS-W Instant.10.0.2 or later versions.	AOS-W Instant.10.0.2
AOS-252434 AOS-252435	Some OAW-IAPs experience unexpected UCM crashes several times a day due to duplicate MAC addresses in the hash table. This issue is observed in APs running AOS-W Instant.10.0.2 or later versions.	AOS-W Instant.10.0.2

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

Upgrading an OAW-IAP Image Manually Using the WebUI

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

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

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

Access Points	Image File Format
OAW-AP344, OAW-AP345, OAW-AP514, OAW-AP515, OAW-AP518, OAW-AP574, OAW-AP575, OAW-AP575EX, OAW-AP577, and OAW-AP577EX	Alcatel Instant_Draco_8.10.0.x_xxxx
OAW-AP503H, OAW-AP504, OAW-AP505, OAW-AP505H, OAW-AP565, and OAW-AP567.	Alcatel Instant_Gemini_8.10.0.x_xxxx

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

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

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

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

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

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

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

Upgrading an OAW-IAP Image Manually Using CLI

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

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

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

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

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

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

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

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

The following command describes how to view the upgrade information:

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

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

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

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