AOS-W Instant 8.5.0.12

Alcatel·Lucent
Enterprise

Release Notes

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:

For list of terms, refer to the 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.

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.

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
■ OAW-AP530 Series — OAW-AP534 and OAW-AP535 ■ OAW-AP550 Series — OAW-AP555	AOS-W Instant 8.5.0.0 or later
■ OAW-AP303 Series — OAW-AP303P ■ OAW-AP510 Series — OAW-AP514 and OAW-AP515	AOS-W Instant 8.4.0.0 or later
■ OAW-AP303 Series — OAW-AP303 ■ OAW-AP318 Series — OAW-AP318 ■ OAW-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
■ OAW-AP203H Series — OAW-AP203H	AOS-W Instant 6.5.3.0 or later
■ OAW-AP203R Series — OAW-AP203R and OAW-AP203RP ■ OAW-AP303H Series — OAW-AP303H ■ OAW-AP360 Series — OAW-AP365 and OAW-AP367	AOS-W Instant 6.5.2.0 or later
■ OAW-AP207 Series — OAW-IAP207 ■ OAW-AP300 Series — OAW-IAP304 and OAW-IAP305	AOS-W Instant 6.5.1.0-4.3.1.0 or later
■ OAW-AP310 Series — OAW-IAP314 and OAW-IAP315 ■ OAW-AP330 Series — OAW-IAP334 and OAW-IAP335	AOS-W Instant 6.5.0.0-4.3.0.0 or later
■ OAW-AP320 Series — OAW-IAP324 and OAW-IAP325	AOS-W Instant 6.4.4.3-4.2.2.0 or later
■ OAW-IAP228 ■ OAW-AP270 Series — 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-AP220 Series — OAW-IAP224 and OAW-IAP225	AOS-W Instant 6.3.1.1-4.0.0.0 or later
■ OAW-RAP155 Series — OAW-RAP155 and OAW-RAP155P	AOS-W Instant 6.2.1.0-3.3.0.0 or later

Chapter 4
Regulatory Updates

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_79055

This release includes fixes for vulnerabilities documented in **CVE-2020-11022**, **CVE-2020-11023**, **CVE-2020-25705**, and the following CVEs referenced in ARUBA-PSA-2021-007:

- CVE-2019-5317
- CVE-2019-5319
- CVE-2020-24635
- CVE-2020-24636
- CVE-2021-25143
- CVE-2021-25144
- CVE-2021-25145
- CVE-2021-25146
- CVE-2021-25148
- CVE-2021-25149
- CVE-2021-25150
- CVE-2021-25155
- CVE-2021-25156
- CVE-2021-25157
- CVE-2021-25158
- CVE-2021-25159
- CVE-2021-25160
- CVE-2021-25161
- CVE-2021-25162

Additionally, the following issues are resolved in this release.

Table 4: *Resolved Issues in AOS-W Instant 8.5.0.12*

Bug ID	Description	Component	Platform	Reported Version
AOS-153932 AOS-211583	**Symptom:** A OAW-AP303H Series access point crashed and rebooted unexpectedly. The log file listed the reason for reboot as: **Reboot caused by kernel panic: Fatal exception**. The fix ensures that the AP works as expected. **Scenario:** This issue occurred when the AP used a 3G/4G modem for uplink connection. This issue was observed in OAW-AP303H Series access points running AOS-W Instant 8.5.0.10 or later versions.	3G/4G Management	OAW-AP303H Series access points	AOS-W Instant 8.5.0.10
AOS-190340	**Symptom:** An OAW-IAP failed to receive **banner text**, **terms-of-use**, and **use-policy** configurations for captive portal from the OmniVista 3600 Air Manager server. The fix ensures that the AP receives the captive portal configurations as expected. **Scenario:** This issue occurred when special characters were used to define **banner text**, **terms-of-use**, and **use-policy**. This issue was observed in APs running AOS-W Instant 8.5.0.0 or later versions.	Captive Portal	All platforms	AOS-W Instant 8.6.0.0
AOS-199744	**Symptom:** The output of the **show iap table long** command did not display any values under the **BID (Subnet Name)** column, when the command was executed on the Switch. Upgrade the Switch to AOS-W 8.5.0.12 to resolve the issue. The fix ensures that the Switch works as expected. **Scenario:** This issue occurred in backup Switchs when an IAP branch failed over from the primary Switch in an IAP-VPN deployment. This issue was observed in IAP-VPN deployments that had Switches running AOS-W 8.3.0.0 or later versions.	IAPMgr	All platforms	AOS-W Instant 8.5.0.7
AOS-205389	**Symptom:** A few APs in an AOS-W Instant cluster intermittently reported **config checksum** errors. The fix ensures that APs sync configurations from the master AP without any checksum errors. **Scenario:** This issue occurred in OmniVista 3600 Air Manager-managed AOS-W Instant networks. This issue was observed in APs running AOS-W Instant 8.5.0.7 or later versions.	VC Management	All platforms	AOS-W Instant 8.5.0.7
AOS-205932	**Symptom:** Some client devices were disconnected from the network when roaming from one AP to another. The fix ensures that APs sync GTK successfully and clients can roam without any interruption in connection. **Scenario:** This issue occurred when broadcast and multicast traffic for clients was blocked due to Group Transient Key (GTK) sync failure between the neighboring APs. This issue was observed in 802.11r enabled APs running AOS-W Instant 8.4.0.2 or later versions.	Authentication	All platforms	AOS-W Instant 8.4.0.2

Table 4: *Resolved Issues in AOS-W Instant 8.5.0.12*

Bug ID	Description	Component	Platform	Reported Version
AOS-206840	**Symptom:** The checksum ID and radio information of an AP were not updated on the Virtual Switch. The fix ensures that the AP updates checksum ID and radio information on the Virtual Switch. **Scenario:** This issue occurs in APs that are configured with a static channel. This issue was observed in OAW-AP300 Series, OAW-AP315, OAW-AP320 Series, OAW-AP330 Series, OAW-AP360 Series, and OAW-AP370 Series access points running AOS-W Instant 8.4.0.6 or later versions.	Wi-Fi Driver	OAW-AP300 Series, OAW-AP315, OAW-AP320 Series, OAW-AP330 Series, OAW-AP360 Series, and OAW-AP370 Series access points	AOS-W Instant 8.4.0.6
AOS-207602	**Symptom:** An OAW-AP200 Series access point failed to complete 802.1X authentication when **Validate server** option was selected in the **Configuration > System > Show advanced options > Uplink > AP1X** section. The debug log listed the following reason: **Server validation failed**. The fix ensures that the AP completes 802.1X authentication and works as expected. **Scenario:** This issue was observed in OAW-AP200 Series access points running AOS-W Instant 8.6.0.4 or later versions.	Authentication	OAW-AP200 Series access points	AOS-W Instant 8.6.0.4
AOS-209148	**Symptom:** Some clients were unable to reach the splash page for captive portal authentication. The fix ensures that captive portal clients reach the splash page and join the network as expected **Scenario:** This issue occurred when the AP failed to process DNS queries from captive portal clients. This issue was observed in APs running AOS-W Instant 8.3.0.0 or later versions.	Captive Portal	All platforms	AOS-W Instant 8.3.0.0
AOS-210059	**Symptom:** An OAW-IAP failed to install CA certificate for 802.1X authentication. The OAW-IAP displays the error message: **Validate certificate file failed**. The fix ensures that CA certificate is installed on the AP as expected. **Scenario:** This issue was observed in APs running AOS-W Instant 8.5.0.9 or later versions.	Authentication	All platforms	AOS-W Instant 8.5.0.9
AOS-210224	**Symptom:** Two member APs in a cluster broadcasted on the same channel when other free channels were available. The fix ensures that the member APs broadcast on different channels as expected. **Scenario:** This issue was observed in APs running AOS-W Instant 8.5.0.5 or later versions.	ARM	All platforms	AOS-W Instant 8.5.0.5

Table 4: *Resolved Issues in AOS-W Instant 8.5.0.12*

Bug ID	Description	Component	Platform	Reported Version
AOS-210855	**Symptom:** The master AP in an AOS-W Instant cluster randomly encountered a CLI core crash that reset the **Age** for APs in the output of **show aps** command. The fix ensures that the AP works as expected. **Scenario:** This issue was observed in APs running AOS-W Instant 8.5.0.0 or later versions.	VC Management	All platforms	AOS-W Instant 8.6.0.5
AOS-211407	**Symptom:** Clients connected to an OAW-IAP were unable to send and receive traffic. The fix ensures that clients can send and receive traffic in OAW-IAP clusters as expected. **Scenario:** This issue was observed in networks configured with **Deny intra VLAN traffic** and the client IP assignment was set to **Virtual Switch** managed. This issue occurred after a Master AP failover event in the AOS-W Instant cluster. This issue was observed in APs running AOS-W Instant 8.5.0.0 or later versions.	Datapath	All platforms	AOS-W Instant 8.6.0.4
AOS-213257	**Symptom:** An OAW-IAP failed to remove the domain name suffix when logging username entries in the AirGroup users table. The fix ensures that the AP logs the username entry in the AirGroup table as expected. **Scenario:** This issue occurred when **Enforce ClearPass registration** was enabled in the **Configuration > Services >AirGroup** section of the WebUI. This issue was observed in APs running AOS-W Instant 8.3.0.0 or later versions.	AirGroup	All platforms	AOS-W Instant 8.3.0.0
AOS-214199	**Symptom:** An OAW-IAP failed to establish an SSL connection with OpenDNS servers. The fix ensures that the AP connects to OpenDNS servers as expected. **Scenario:** This issue occurred due to an incompatibility with the **content-header** message sent by the OpenDNS server. This issue was observed in APs running AOS-W Instant 8.5.0.11 or later versions.	Authentication	All platforms	AOS-W Instant 8.5.0.11

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 8.5.0.12*

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	**Symptom:** An OAW-IAP reboots unexpectedly. The log file lists the reason for the event as **Reboot caused by kernel panic: softlockup: hung tasks.** **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.	Datapath	All platforms	AOS-W Instant 8.3.0.0
AOS-185064	—	**Symptom:** An OAW-IAP fails to stop clients from connecting to a rogue AP. **Scenario:** This issue is observed in APs running AOS-W Instant 8.3.0.0 or later versions. **Workaround:** Reboot the AP working as the Spectrum Monitor.	IDS	All platforms	AOS-W Instant 8.3.0.0
AOS-186192	—	**Symptom:** Clients experience connectivity issues when configured to receive its IP address from the Local or Distributed, L3 DHCP scope. **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. **Workaround:** Clear the ARP entry for the default gateway in the master OAW-IAP.	Datapath	All platforms	AOS-W Instant 8.4.0.1
AOS-189484 AOS-189491	—	**Symptom:** Wired clients experience connectivity issues with OAW-IAPs using Wi-Fi uplink. **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. **Workaround:** Reconfigure the wired port profile on the OAW-IAP in the **Configuration > Networks** page of the WebUI.	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 8.5.0.12*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-190089	—	**Symptom:** An OAW-IAP classifies YouTube application traffic as UDP traffic and not YouTube app traffic. **Scenario:** This issue is observed in APs running AOS-W Instant 8.4.0.3 or later versions.	AppRF	All platforms	AOS-W Instant 8.4.0.3
AOS-190211	—	**Symptom:** Wired clients of an Ethernet interface experience connectivity issues when other Ethernet ports are shut down because of loop protection. **Scenario:** This issue is observed in OAW-AP303H access points running AOS-W Instant 8.3.0.0 or later versions.	Datapath	OAW-AP303H access points	AOS-W Instant 8.3.0.0
AOS-191329	—	**Symptom:** The output of **show running-configuration** command does not include IPM configuration logs. **Scenario:** This issue is observed in APs running AOS-W Instant 8.5.0.1 or later versions.	Configuration	All platforms	AOS-W Instant 8.5.0.1
AOS-192469	—	**Symptom:** An OAW-IAP does not tag voice and video traffic with the WMM values defined in the SSID profile. Instead, the AP uses the default DSCP tags of 48 and 40 for voice and video traffic respectively. **Scenario:** This issue is observed in APs running AOS-W Instant 8.3.0.0 or later versions.	Datapath	All platforms	AOS-W Instant 8.3.0.0
AOS-193088	—	**Symptom:** The client list registers the device name as the user name for some users in the post authentication role. **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.	Authentication	All platforms	AOS-W Instant 8.5.0.0
AOS-201901	—	**Symptom:** An OAW-IAP changes all access rules to **deny** when the configuration is restored through the CLI from a Windows TFTP server. **Scenario:** This issue occurs when the Windows configuration retrieved from the TFTP server includes newline (\n) and carriage return (\r) characters. This issue is observed in APs running AOS-W Instant 8.5.0.0 or later versions.	Configuration	All platforms	AOS-W Instant 8.5.0.0

Table 5: *Known Issues in AOS-W Instant 8.5.0.12*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-204171	—	**Symptom:** Clients intermittently experience high latency when the AP is connected to the backup Switch after a failover event. **Scenario:** This issue occurs when, ■ the AP attempts to connect to the primary controller. ■ when fast failover is enabled on the AP. This issue is observed in OAW-AP203R Series access points running AOS-W Instant 8.3.0.0 or later versions.	VPN	OAW-AP203R Series access points	AOS-W Instant 8.5.0.8
AOS-207415	—	**Symptom:** The access requests of some clients are rejected by the RADIUS server. **Scenario:** This issue occurs when the client's access request sent from the AP to the RADIUS server was missing the **State** attribute. This issue is observed in APs running AOS-W Instant 8.4.0.0 or later versions.	Authentication	All platforms	AOS-W Instant 8.4.0.0
AOS-211525 AOS-212652	—	**Symptom:** An OAW-IAP inherits the gateway IP of the layer 2 switch during a switch outage and causes an IP address conflict when the switch is back online. **Scenario:** This issue is observed in APs running AOS-W Instant 8.5.0.5 or later versions.	Firewall	All platforms	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

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. 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.