HPE Aruba Networking Instant Operating System 8.10.0.16

Release Notes

Hewlett Packard Enterprise

Contents

The following table provides the revision history of this document.

Table 1: *Revision History*

Revision	Change Description
Revision 01	Initial release.

This Instant AOS-8 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 Aruba user-centric network:

- *Aruba AP Software Quick Start Guide*
- *Instant AOS-8 User Guide*
- *Instant AOS-8 CLI Reference Guide*
- *Instant AOS-8 REST API Guide*
- *Instant AOS-8 Syslog Messages Reference Guide*
- *Aruba Instant AP Troubleshooting Guide*

Supported Browsers

The following browsers are officially supported for use with the 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, Aruba will replace racially insensitive terms and instead use the following new language:

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

Contacting Support

Table 2: *Contact Information*

Main Site	arubanetworking.hpe.com
Support Site	networkingsupport.hpe.com
Airheads Social Forums and Knowledge Base	community.arubanetworks.com
North American Telephone	1-800-943-4526 (Toll Free) 1-408-754-1200
International Telephone	arubanetworks.com/support-services/contact-support
Software Licensing Site	lms.arubanetworks.com
End-of-life Information	arubanetworks.com/support-services/end-of-life
Security Incident Response Team	Site: arubanetworks.com/support-services/security-bulletins Email: aruba-sirt@hpe.com

There are no new features, enhancements, or behavioral changes introduced in this release.

This section displays the supported platforms in Instant AOS-8.x. The **minimum version supported** column displays the minimum Instant AOS-8.x version that can be run on a platform. The **latest version supported** column displays the newest Instant AOS-8.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			Instant AOS-8 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	8.12.0.x
	650 Series	AP-655	8.10.0.x	8.12.0.x
		AP-654	8.11.2.x	8.12.0.x
	630 Series	AP-635	8.9.0.x	8.12.0.x
		AP-634	8.11.2.x	8.12.0.x
	610 Series	AP-615	8.11.0.x	8.12.0.x
	600 Series	AP-605H	8.12.0.x	8.12.0.x

Access Points			Instant AOS-8 Versions Supported	
AP Family	AP Series	AP Model	Minimum	Latest
5xx	580 Series	AP-584, AP-585, AP-585EX, AP-587, AP-587EX	8.10.0.x	8.12.0.x
	570 Series	AP-574, AP-575, AP-577	8.7.0.x	8.12.0.x
	560 Series	AP-565, AP-567	8.7.1.x	8.12.0.x
	550 Series	AP-555	8.5.0.x	8.12.0.x
	530 Series	AP-534, AP-535	8.5.0.x	8.12.0.x
	510 Series	AP-518	8.7.0.x	8.12.0.x
		AP-514, AP-515	8.4.0.x	8.12.0.x
	500 Series	AP-504, AP-505	8.6.0.x	8.12.0.x
		AP-505H	8.7.0.x	8.12.0.x
		AP-503H	8.7.1.x	8.12.0.x
		AP-503	8.11.1.x	8.12.0.x

Access Points			Instant AOS-8 Versions Supported	
AP Family	AP Series	AP Model	Minimum	Latest
3xx	380 Series	AP-387	8.4.0.x	8.10.0.x
	370 Series	AP-374, AP-375, AP-377, AP-375EX, AP-377EX, AP-375ATEX	8.3.0.x	8.12.0.x
	360 Series	AP-365, AP-367	8.3.0.x	8.12.0.x
	340 Series	AP-344, AP-345	8.3.0.x	8.10.0.x
	330 Series	AP-334, AP-335	8.1.0.x	8.10.0.x
	320 Series	AP-324, AP-325	8.0.0.x	8.10.0.x
	310 Series	AP-318	8.3.0.x	8.12.0.x
		AP-314, AP-315	8.1.0.x	8.12.0.x
	300 Series	AP-304, AP-305	8.1.0.x	8.12.0.x
		AP-303H, AP-303HR	8.2.0.x	8.12.0.x
		AP-303P	8.4.0.x	8.12.0.x
		AP-303	8.3.0.x	8.12.0.x
2xx	270 Series	AP-274, AP-275, AP-277	8.0.0.x	8.6.0.x
	220 Series	AP-224, AP-225, AP-228	8.0.0.x	8.6.0.x
	210 Series	AP-214, AP-215	8.0.0.x	8.6.0.x
	200 Series	AP-207	8.1.0.x	8.6.0.x
		AP-203H, AP-203R, AP-203RP	8.2.0.x	8.10.0.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 Instant AP 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.com.

The following DRT file version is part of this release:

- DRT-1.0_91868

The following issues are resolved in this release.

Table 3: *Resolved Issues in Instant 8.10.0.16*

Bug ID	Description	Reported Version
AOS-247307 AOS-261131 AOS-251985	Some AP-635 access points running Instant AOS-8.0.0.0 or later versions crashed unexpectedly. The log files listed the reason for the event as **Reboot caused by kernel panic: Take care of the TARGET ASSERT**. The fix ensures that the APs work as expected.	Instant AOS-8.0.0.0
AOS-250092 AOS-251675 AOS-261384 AOS-247174	WPA3 SAE clients failed to reauthenticate while roaming to a previous AP. This issue occurred since PMK cache lifetime was not set and **11r** functionality was disabled. The fix ensures SAE clients are able to roam as expected by setting a PMK cache lifetime of 8 hours. This issue was observed in AP running Instant AOS-8.10.0.0 or later versions.	Instant AOS-8.10.0.0
AOS-250255 AOS-260110	Users encountered connectivity issues and high memory utilization on AP-335 and AP-345 access points running Instant AOS-8.10.0.8 or later versions. The fix ensures APs work as expected.	Instant AOS-8.10.0.8
AOS-256659	Some APs displayed an incorrect hostname when clients had IPv6 enabled, which in turn displayed incorrect information on Central. The fix ensures that the correct hostname is displayed. This issue was observed in APs running Instant AOS-8.0.0.0 or later versions.	Instant AOS-8.0.0.0
AOS-257872	Upgrading DRT via HTTPS failed due to **DRT stuck download**, which caused some APs to appear offline in the Central UI. The fix ensures APs will not be stuck in DRT downloading, maintaining AP connectivity and visibility in the Central UI. This issue was observed in APs running Instant AOS-8.10.0.12 or later versions.	Instant AOS-8.10.0.12
AOS-258287	Multiple false alerts were observed on access points after enabling IDS. The fix ensures that the alerts are genuine. This issue was observed in AP-635 access points running Instant AOS-8.10.0.0 or later versions.	Instant AOS-8.10.0.0
AOS-258406	Wireless clients connected to APs were randomly assigned **default_wired_port_profile** role. This happened because different roles had the same index in the STM process. The fix ensures that the index values are unique for each role. This issue was observed in AP-515 access points running Instant AOS-8.10.0.0 or later versions.	Instant AOS-8.10.0.0
AOS-259401 AOS-260943 AOS-260631 AOS-262043	Some access points crashed and rebooted unexpectedly. The log files listed the reason for the event as **Reboot caused by kernel panic: Fatal exception in interrupt**. The issue occurred because of a crash in the AP datapath. The fix ensures access points work as expected. This issue was observed in 500 Series and 600 Series APs running Instant AOS-8.10.0.14 or later versions.	Instant AOS-8.10.0.14

Table 3: *Resolved Issues in Instant 8.10.0.16*

Bug ID	Description	Reported Version
AOS-259527	Multiple APs with **IDS detection** enabled were incorrectly detecting Power Save DoS attacks. An excessive number of alerts was seen in the log files. The fix ensures that alerts for Power Save DoS attacks are accurate and not triggered excessively. This issue was observed in APs running Instant AOS-810.0.0 or later versions.	Instant AOS-8.10.0.0
AOS-259710 AOS-257465 AOS-259633 AOS-259858 AOS-259922 AOS-260134 AOS-260177 AOS-260385 AOS-260559 AOS-260680 AOS-260958 AOS-261675 AOS-259322	Several UCM crashes were observed on APs with UCC due to memory corruption. The fix resolves the memory corruption issue in APs with UCC. This issue was observed on APs running Instant AOS-8.10.0.0 or later versions.	Instant AOS-8.10.0.0
AOS-260232 AOS-258711	In the **show ap monitor rogue-ap <mac>** command output, some APs failed to display a value for **Match MAC**, even though **Match Eth MAC** displayed a value. The issue occurred because when dealing with the rogue classification of similar BSSID detection, a null value was assigned to **Match MAC**. The fix ensures both values are displayed as expected. This issue was observed in APs running Instant AOS-8.10.0.0 or later versions.	Instant AOS-8.10.0.0
AOS-260258 AOS-260383	The output of the **show ap arm neighbors** and **show ap monitor ap-list** commands did not show information for neighboring 5 GHz BSSIDs. This issue was caused by a hardware buffer getting stuck, preventing the AP monitor list from being updated correctly. The fix ensures APs accurately report 5 GHz neighbor information. This issue was observed in APs running Instant AOS-8.10.0.0 or later versions.	Instant AOS-8.10.0.0
AOS-260393	Some AirWave-managed APs did not display show command outputs. The command execution resulted in a **No output for this command** message. The fix ensures that APs display show command outputs. This issue was observed in APs running Instant AOS-8.10.0.14 or later versions.	Instant AOS-8.10.0.14
AOS-260884 AOS-261200	Some virtual controllers generated core files frequently. This issue occurred because the **dnsmasq** process was crashing. The fix ensures that the virtual controllers work as expected. The issue was observed in APs running Instant AOS-8.10.0.14 or later versions.	Instant AOS-8.10.0.14
AOS-260983	AP-655 access points that were installed on Windows 11 incorrectly displayed Windows 10 in both the SSH and WebUI. This issue occurred because the DHCP fingerprinting is the same for Windows 10 and Windows 11. The fix ensures that AP-655 access points display Windows 11 when applicable. The issue was observed in AP-655 access points running Instant AOS-8.10.0.4 or later versions.	Instant AOS-8.10.0.4

HPE Aruba Networking Instant Operating System 8.10.0.16 | Release Notes

Table 3: *Resolved Issues in Instant 8.10.0.16*

Bug ID	Description	Reported Version
AOS-261039	Some Instant Access Point crashed and rebooted unexpectedly due to a memory overrun in the **AWC** process. The fix applies data validation to ensures access points perform as expected. This issue was observed in access points running Instant AOS-8.10.0.16 or later versions.	Instant AOS-8.10.0.16
AOS-261065	Some guest clients could not connect to the guest SSID. The issue occurred because the guest clients failed to transition from the pre-authenticated role to post-authentication role. The fix ensures that the guest clients successfully connect to the guest SSID. The issue was observed in AP-505 access points running Instant AOS-8.10.0.12.	Instant AOS-8.10.0.12
AOS-261284	Downloaded roles were not propagated from conductor APs to member APs in some scenarios, such as when member APs reloaded. The fix ensures that the download roles are propagated correctly to the member AP. This issue was observed on APs running Instant AOS-8.10.0.15 or later versions.	Instant AOS-8.10.0.15
AOS-261317	Some APs crashed unexpectedly due to a missing **NULL** check in the authentication library when the MDNS module called the **rc_pack_list** API without providing an authentication secret. The fix ensures APs work as expected. This issue was observed in APs running Instant AOS-8.10.0.14 or later versions.	Instant AOS-8.10.0.14
AOS-261623 AOS-261987 AOS-261992 AOS-262042	Some AP-555 access points randomly crashed and rebooted. The log files listed the reason for the crash as **Kernel panic - not syncing: Take care of the TARGET ASSERT**. The fix ensures APs work as expected. This issue was observed in APs running Instant AOS-8.10.0.12 or later versions.	Instant AOS-8.10.0.12
AOS-262403 AOS-261409 AOS-261914	Some clients connected to 500 Series access points experienced latency and performance issues. The fix brings back the latency and performance to the expected level for these clients. This issue was observed in access points running Instant AOS-8.10.0.14 or later versions.	Instant AOS-8.10.0.14

This chapter describes the known issues observed in this release.

Limitations

This section describes the limitations in Instant AOS-8.10.0.16.

AP-635 and AP-655 Access Points

AP-635 and AP-655 access points have the following limitations:

- All radios for AP-635 and AP-655 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 500 Series and 510 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 Instant AP hostname is increased from 32 to 128 characters. The following configuration settings do not support the new limit of 128 ASCII characters in 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

Instant AOS-8 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 Instant AOS-8.10.0.11. TAA SKUs running Instant AOS-8.10.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 Instant AOS-8.11.0.0 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 Instant AP 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 Instant 8.10.0.16*

Bug ID	Description	Reported Version
AOS-195769	In some Instant APs 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 Instant APs running Instant AOS-8.6.0.0 or later versions.	Instant AOS-8.6.0.0
AOS-204171	Clients intermittently experience high latency when the Instant AP is connected to the backup controller after a failover event. This issue occurs under the following scenarios: ■ The AP attempts to reconnect to the primary controller. ■ Fast failover is enabled on the AP. This issue is observed in 203R Series access points running Instant AOS-8.3.0.0 or later versions.	Instant AOS-8.3.0.0

Table 4: *Known Issues in Instant 8.10.0.16*

Bug ID	Description	Reported Version
AOS-220890	MPSK-Local SSID is broadcasted as Open SSID in Instant APs when the software version is downgraded to Instant AOS-8 versions lower than 8.7.0.0. This issue is observed in APs running Instant AOS-8.6.0.8 or later versions.	Instant AOS-8.6.0.8
AOS-225601 AOS-224170	Some member APs in a cluster appear as **down** in the AirWave UI. This issue is observed in AirWave-managed APs running Instant AOS-8.6.0.0 or later versions.	Instant AOS-8.6.0.0
AOS-228967	Users are unable to configure the **Station Ageout Time** to a value over 3600 seconds. This issue is observed in APs running Instant AOS-8.7.1.4 or later versions.	Instant AOS-8.6.0.8
AOS-231129	Instant APs do not send cold and warm SNMP traps when expected. This issue is observed in APs running Instant AOS-8.0.0.0 or later versions.	Instant AOS-8.6.0.8
AOS-232833	Member APs ignore the proxy configuration when trying to download firmware with the image URL provided by the virtual controller. This issue is observed in APs running Instant AOS-8.9.0.0 or later versions.	Instant AOS-8.9.0.0
AOS-233095	In AP clusters that are configured with a static IP address, the system log is populated with multiple **arping ongoing got central rollback** messages. The APs are managed locally and are not managed by Central. This issue is observed in APs running Instant AOS-8.7.1.3 or later versions.	Instant AOS-8.7.1.3
AOS-233149 AOS-235164	The Instant AP 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 Instant AOS-8.7.1.9 or later versions.	Instant AOS-8.7.1.9
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 Instant AOS-8.9.0.3 or later versions.	Instant AOS-8.9.0.3
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 Instant AOS-8.9.0.2 or later versions.	Instant AOS-8.9.0.2
AOS-234828	Instant APs 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 Instant AOS-8.9.0.3 or later versions.	Instant AOS-8.9.0.3
AOS-235428	Instant APs in a cluster intermittently disconnect from the VPN and Central. The output of the **show ap debug cloud-server** command returns the **Master failover** error message, despite the conductor being stable. This issue is observed in APs running Instant AOS-8.6.0.17 or later versions.	Instant AOS-8.6.0.17
AOS-238137	The **traceroute** command returns the following error message: **Can't find tsgw src ip**. This issue occurs when the Instant APs have multiple routing entries in the routing profile. This issue is observed in APs running Instant AOS-8.10.0.3 or later versions.	Instant AOS-8.10.0.3

Table 4: *Known Issues in Instant 8.10.0.16*

Bug ID	Description	Reported Version
AOS-239411	Instant APs 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 Instant AOS-8.9.0.0 or later versions.	Instant AOS-8.9.0.0
AOS-239419	The **eth0** link of an AP appears offline in the AirWave UI. This issue is observed in AirWave-managed APs running Instant AOS-8.6.0.18 or later versions.	Instant AOS-8.6.0.18
AOS-240530	Instant APs 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 Instant AOS-8.10.0.0 or later versions.	Instant AOS-8.10.0.4
AOS-241316	The output of the **show ap debug lldp** command displays incorrect information. This issue is observed in APs running Instant AOS-8.6.0.0 or later versions.	Instant AOS-8.6.0.20
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 Instant AOS-8.10.0.5 or later versions.	Instant AOS-8.10.0.5
AOS-249946 AOS-247154	Some APs crash and reboot unexpectedly due to a UCM segmentation issue, which affects different VoIP applications. This issue is observed in access points running Instant AOS-8.10.0.2 or later versions.	Instant AOS-8.10.0.2
AOS-252434 AOS-252435	Some Instant APs experience unexpected UCM crashes several times a day due to duplicate MAC addresses in the hash table. This issue is observed in APs running Instant AOS-8.10.0.2 or later versions.	Instant AOS-8.10.0.2
AOS-261701	Some APs managed under a Central template group become preferred Conductors, overwriting the **per-ap-settings** variable. This issue arises from two factors: first, the absence of conditions configured in lowercase and case-sensitive format, which prevents the **per-ap-settings** from being correctly applied to the APs. And second, the APs failing to report the correct configuration when the preferred Conductor is set as a member AP in swarm mode, even though it is successfully pushed in Central. This issue is observed in APs running Instant AOS-8.10.0.14 or later versions.	Instant AOS-8.10.0.14

This chapter describes the Instant software upgrade procedures and the different methods for upgrading the image on the Instant AP.

> While upgrading anInstant AP, you can use the image check feature to allow the Instant AP to find new software image versions available on a cloud-based image server hosted and maintained by Aruba. 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 Instant software.

Topics in this chapter include:

Upgrading an Instant AP and Image Server

Instant supports mixed Instant AP class Instant deployment with all Instant APs as part of the same virtual controller cluster.

Image Management Using AirWave

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

> The virtual controller communicates with the AirWave server if AirWave is configured. If AirWave is not configured on the Instant AP, the image is requested from the Image server.

Image Management Using Cloud Server

If the multi-class Instant AP network is not managed by AirWave, image upgrades can be done through the Cloud-Based Image Check feature. If a new Instant AP joining the network needs to synchronize its software version with the version on the virtual controller and if the new Instant AP belongs to a different class, the image file for the new Instant AP is provided by the cloud server.

Configuring HTTP Proxy on an Instant AP

If your network requires a proxy server for Internet access, ensure that you configure the HTTP proxy on the Instant AP to download the image from the cloud server. The **Username** and **Password**

configuration is supported only for cloud services. After setting up the HTTP proxy settings, the Instant AP connects to the Activate server, AMP, Central, OpenDNS, or web content classification server through a secure HTTP connection. The proxy server can also be configured and used for cloud services. You can also exempt certain applications from using the HTTP proxy (configured on an Instant AP) by providing their host name or IP address under exceptions.

The following procedure describes how to configure the HTTP proxy settings using the webUI:

1. Navigate to **Configuration** > **System** > **Proxy**.
2. Enter the HTTP proxy server IP address in the **Auth Server** text box.
3. Enter the port number in the **Port** text box.
4. If you want to set an authentication username and password for the proxy server, enable the **Proxy requires authentication** toggle switch.
5. Enter a username in the **Username** text box.
6. Enter a password in the **Password** text box.
7. If you do not want the HTTP proxy to be applied for a particular host, click **+** to enter that IP address or domain name of that host in the **Exceptions** section.
8. Click **Save**.

The following procedure describes how to configure the HTTP proxy settings using the CLI:

```
(Instant AP)(config)# proxy server 192.0.2.1 8080 example1 user123
(Instant AP)(config)# proxy exception 192.0.2.2
(Instant AP)(config)# end
(Instant AP)# commit apply
```

HTTP Proxy Support through Zero Touch Provisioning

Instant APs experience issues when connecting to AirWave, Central, 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 Instant AP through a DHCP server.

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

In order for the factory default Instant AP to automatically discover the proxy server, you need to configure the HTTP proxy information in the DHCP server option. The Instant AP 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 Instant APs with AirWave

Starting from Instant AOS-8.4.0.0, Rolling Upgrade for Instant APs in standalone mode is supported with AirWave. The upgrade is orchestrated through NMS and allows the Instant APs 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 *AirWave 8.2.8.2 Instant Deployment Guide* and *AirWave 8.2.8.2 Release Notes*.

Upgrading an Instant AP Using the Automatic Image Check

You can upgrade an Instant AP by using the Automatic Image Check feature. The automatic image checks are performed once, as soon as the Instant AP boots up and every week thereafter.

If the image check locates a new version of the Instant software on the image server, the New version available link is displayed on the Instant main window.

| | If AirWave is configured, the automatic image check is disabled. |

The following procedure describes how to check for a new version on the image server in the cloud using the webUI:

1. Go to **Maintenance** > **Firmware**.
2. In the **Automatic** section, click **Check for New Version**. After the image check is completed, one of the following messages is displayed:
   - No new version available—If there is no new version available.
   - Image server timed out—Connection or session between the image server and the Instant AP is timed out.
   - Image server failure—If the image server does not respond.
   - A new image version found—If a new image version is found.
3. If a new version is found, the **Upgrade Now** button becomes available and the version number is displayed.
4. Click **Upgrade Now**.

The Instant AP downloads the image from the server, saves it to flash, and reboots. Depending on the progress and success of the upgrade, one of the following messages is displayed:

- Upgrading—While image upgrading is in progress.
- Upgrade successful—When the upgrade is successful.
- Upgrade failed—When the upgrade fails.

If the upgrade fails and an error message is displayed, retry upgrading the Instant AP.

Upgrading to a New Version Manually Using the WebUI

If the Automatic Image Check feature is disabled, 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 Instant APs.
      ii. Click on **Browse** and select the image file from your local system. The following table describes the supported image file format for different Instant AP models:

Access Points	Image File Format
AP-635 and AP-655	Aruba Instant_Norma_8.10.0.x_xxxx
AP-344, AP-345, AP-514, AP-515, AP-518, AP-574, AP-575, AP-575EX, AP-577, and AP-577EX	Aruba Instant_Draco_8.10.0.x_xxxx
AP-503H, AP-504, AP-505, AP-505H, AP-565, and AP-567.	Aruba Instant_Gemini_8.10.0.x_xxxx
IAP-314, IAP-315, IAP-324, IAP-325, AP-374, AP-375, AP-377, AP-318, and AP-387	Aruba Instant_Hercules_8.10.0.x_xxxx
IAP-334 and IAP-335	Aruba Instant_Lupus_8.10.0.x_xxxx
AP-534, AP-535, AP-555, AP-584, AP-585, AP-585EX, AP-587, AP-587EX	Aruba Instant_Scorpio_8.10.0.x_xxxx
AP-303, AP-303H, 303P Series, IAP-304, IAP-305, AP-365, and AP-367	Aruba Instant_Ursa_8.10.0.x_xxxx
AP-203H, AP-203R, AP-203RP, and IAP-207	Aruba 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>/ArubaInstant_Hercules_8.10.0.x_xxxx
         - TFTP - tftp://<IP-address>/<image-file>. For example, tftp://<IP-address>/Aruba Instant_Hercules_8.10.0.x_xxxx
         - FTP - ftp://<IP-address>/<image-file>. For example, ftp://<IP-address>/Aruba Instant_Hercules_8.10.0.x_xxxx
         - FTP - ftp://<user name:password>@<IP-address>/<image-file>. For example, ftp://<aruba :123456>@<IP-address>/ArubaInstant_Hercules_8.10.0.x_xxxx

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

Multiclass Instant APs 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 Instant APs to reboot automatically after a successful upgrade. To reboot the Instant AP at a later time, clear the **Reboot all APs after upgrade** check box.

5. Click **Upgrade Now** to upgrade the Instant AP to the newer version.

6. Click **Save**.

Upgrading an Instant AP Image 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/ArubaInstant_Hercules_8.10.0.x_xxxx
```

The following procedure describes how to upgrade an image without rebooting the Instant AP:

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

The following is an example to upgrade an image without rebooting the Instant AP:

```
(Instant AP)# upgrade-image2-no-reboot ftp://192.0.2.7/Aruba 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 Instant 6.4.x.x-4.2.x.x to Instant 8.10.0.x

Before you upgrade an Instant AP running Instant 6.5.4.0 or earlier versions to Instant 8.10.0.x, follow the procedures mentioned below:

1. Upgrade from Instant 6.4.x.x-4.2.x.x or any version prior to Instant 6.5.4.0.
2. Refer to the *Field Bulletin AP1804-1* at asp.arubanetworks.com.
3. Verify the affected serial numbers of the Instant AP units.