Aruba Instant 8.12.0.0

Release Notes

a Hewlett Packard
Enterprise company

Copyright Information

This product includes code licensed under certain open source licenses which require source compliance. The corresponding source for these components is available upon request. This offer is valid to anyone in receipt of this information and shall expire three years following the date of the final distribution of this product version by Hewlett Packard Enterprise Company. To obtain such source code, please check if the code is available in the HPE Software Center at https://myenterpriselicense.hpe.com/cwp-ui/software but, if not, send a written request for specific software version and product for which you want the open source code. Along with the request, please send a check or money order in the amount of US $10.00 to:

Hewlett Packard Enterprise Company
Attn: General Counsel
WW Corporate Headquarters
1701 E Mossy Oaks Rd Spring, TX 77389
United States of America.

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 Aruba Instant release notes includes the following topics:

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*
- *Aruba Instant User Guide*
- *Aruba Instant CLI Reference Guide*
- *Aruba Instant REST API Guide*
- *Aruba Instant 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	arubanetworks.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

Chapter 2
What's New

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

New Features and Enhancements

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

Short Supported Release

Aruba Instant 8.12.0.0 is a Short Supported Release (SSR).

Enhancement for Configuring Non-DFS Channels

Starting with Aruba Instant 8.12.0.0, when configuring access point control settings for the 5 GHz radio, a new checkbox named **Check All Non-DFS Channels** is available to select all Non-DFS channels at once in order to remove them from the allow-channel list. In the WebUI, this new checkbox can be found under **Configuration > RF > ARM > Show advanced options > Customize valid channels > Valid 5 GHz channels> Edit > Check All Non-DFS Channels**.

SKU Number Added to the show activate status Command

Starting with Aruba Instant 8.12.0.0, APs will display their SKU number to identify themselves to Activate/Central if the SKU number is shipped in flash.

No Support for Air Slice in Instant AP Deployments

Starting with Aruba Instant 8.12.0.0, Air Slice support will not be available. If Air Slice is enabled prior to the upgrade, it will be displayed as enabled in the configuration, but it will not take effect internally. The following commands have been impacted:

- **show datapath session dpi**
- **show datapath ipv6 session**
- **show datapath acl**
- **show datapath acl-rule**
- **airslice-policy**
- **show ap debug airslice client-stats**
- **show ap bss-table**

External Antenna Provision Support for 6 GHz

In Aruba Instant 8.12.0.0, 6 GHz external antenna provision configuration is available in the radio settings of APs. The **external-antenna-6ghz** and **ant-pol-6ghz** commands have been included as a knob to properly configure 6 GHz external antenna gain.

Support for 6 GHz Configurations in REST APIs

Aruba Instant 8.12.0.0 supports 6 GHz in REST APIs, which includes the addition of radio-profile-6ghz, utb-filter-block and rf-zone APIs, as well as new JSON parameters in ssid, channel and radio-state APIs. It also adds Norma and Leo as platforms to the allowed list of API upgrades.

Support for Backup Central On-Premises Server IP Addresses in DHCP Option 43

DHCP option 43 will now support an alternate IP address for data center redundancy. This will help customers with multiple data centers set up a backup server IP address for APs to switch to in case of a localized failure. This configuration can be applied through the **ip dhcp pool option 43** CLI command.

Enhanced Debugging Experience in the Radio Profile

The **scheduler-mode** parameter is added to the radio profile in order to provide a better debugging experience. The parameter accepts two possible configurations, **fairness** and **latency**. The default parameter is set to **fairness**, which enables Traffic Allocation Framework (TAF) on the radio profile. The **latency** parameter disables TAF. Aruba Technical Support should be contacted in order to adjust the **scheduler-mode** configuration. Modifying this configuration without guidance from Aruba Technical Support could cause fairness issues on the network.

AP-584 Outdoor Operation is now Supported in France and Israel

The DRT information for AP-584 access points now complies with the regulatory guidelines that allow for outdoor operation in France and Israel.

Support for 670 Series Outdoor Access Points

The 670 Series access points (AP-675, AP-675EX, AP-677, AP-677EX, AP-679, and AP-679EX) are 802.11ax Wi-Fi 6E Outdoor Access Points that offer 2x2 MIMO radios, allowing for simultaneous tri-band operation. These APs also feature a wired 2.5 Gbps Smart Rate network interface and one SFP port for fiber support. If deployed with Aruba Instant, the Aruba670 Series access points will only operate as a dual-band AP in the 2.4 GHz and 5 GHz radios. For 6 GHz operation, the APs require ArubaOS 8.12.0.0 or later versions and deployments managed by a Mobility Conductor.

Additional features include:

- Data rates up to 2.4 Gbps
- Maximum Ratio Combining (MRC)
- Orthogonal Frequency Division Multiple Access (OFDMA)
- IoT-ready (integrated Bluetooth 5 and 802.15.4 radio for Zigbee support)
- Target Wake Time (TWT) for improved client power savings
- Advanced Cellular Coexistence (ACC)

For complete technical details and installation instructions, see the *Aruba 670 Series Access Points Installation Guide*.

Support for AP-605H Access Points

The AP-605H access point is a high-end dual-radio tri-band 2x2 MIMO 802.11ax WiFi 6E hospitality AP platform supporting concurrent operation in any two of the three supported bands (2.4 GHz, 5 GHz and 6 GHz). The mode of operation is configurable either manually or through AirMatch. Ideal for hospitality, branch, and teleworker use-cases, the AP-605H access points can be deployed in either controller-based (ArubaOS) or controller-less (Aruba Instant) network environments.

Additional features include:

- Flexible coverage across any two bands (2.4 GHz, 5 GHz, and 6 GHz) for up to 3.6 Gbps combined peak data rate.
- Up to seven 160 MHz channels in 6 GHz support low-latency, bandwidth-hungry applications like high-definition video and AR/VR applications.
- Combines wireless and wired access in compact desktop or wall mount model that can be PoE powered.
- Convenient wired connectivity and support for PoE with fast 2.5 GbE uplink port, two 1 GbE ports, and two 1 GbE PSE ports capable of supplying up to a total of 30W PoE.
- IoT-ready with integrated Bluetooth 5 and Zigbee.

For complete technical details and installation instructions, see the *Aruba 600H Series Hospitality Access Points datasheet* and the *Aruba 600H Series Hospitality Access Points Installation Guide*.

Enhanced LLDP Information for Neighbor Devices

This enhancement enables users to access more detailed information about neighboring devices. The output of the **show ap debug lldp info** command has been upgraded to provide a richer set of data regarding neighboring devices. A new **remote_system_description** field in the command output now includes device information such as device model information, software version information, among others.

Enhanced Telemetry with New Radio, Client, and VAP Statistics

This release broadens our telemetry capabilities with the addition of new statistics for radios, clients, and virtual APs (VAPs). These new metrics provide deeper visibility into network performance, user experience, and the wireless environment. These new statistics are visible in the output of the commands **show ap debug radio-stats**, **show ap debug client-stats**, and **show ap debug bss-stats**.

Enhancements to the show audit-trail Command Output

This release introduces improvements to the **show audit-trail** command output to assist users in better diagnosing and understanding system events. The command now provides a more detailed and comprehensive output, offering deeper insights into system operations and changes. New output details:

- Member Receive Full Config Events
- Conductor Receive Delta Events
- Config Init Event with Reason
- System Time Change Events
- Capture Fail Reason for Command Execution.
- Reboot Event Logging

Tracking of Randomized MAC Addresses

This feature enables the tracking of probe requests from clients using randomized MAC addresses, offering deeper insights into client presence within the network infrastructure. This update is pivotal for businesses seeking advanced analytics in environments where understanding visitor behavior and network usage patterns is essential. New commands **laa-counter-msg** and **laa-counter-msg-interval** are introduced. Counters are sent to ALE using **profile default-ale**.

Virtual Access Point Configuration for 6 GHz in MBSSID Groups

This release introduces support for up to 8 Virtual Access Points (VAPs) on the 6 GHz radio. This update significantly expands the possibilities for network customization and segmentation, particularly beneficial for complex or high-density environments. The commands **show mbssid-group-profile**, **show mbssid-group-profile <profile name>**, **mbssid-group-profile <profile name>**, and **no mbssid-group-profile <profile name>** are introduced for visualizing and configuring MBSSID group profiles and their references to SSID profiles.

Ability to Specify Key Type When Using EST

A new option to select RSA-4096 key length and ECDSA certificates is available. We support two types of ECDSA keys and three types of RSA keys. For each type of RSA keys, two key lengths 2048 and 4096 are available. Selecting any of the following certificates will override the default RSA-2048:

- csr-attribute ecdsa-prime256v1-with-sha256
- csr-attribute ecdsa-prime384r1-with-sha384
- csr-attribute rsa-with-sha256 key-length <INT:key_length:2048,4096>
- csr-attribute rsa-with-sha384 key-length <INT:key_length:2048,4096>
- csr-attribute rsa-with-sha512 key-length <INT:key_length:2048,4096>

For complete technical details, see the *Aruba Instant CLI Guide*.

New Counters for AP-Wired Client to Cloud

The feature reports the physical port's speed, duplex and error frames counter to the central in 8.12. In the output of show interface counters command, the following results are populated:

- CRC/FCS errors
- Collision errors
- Runts errors
- Giants errors

Auto-assign an EST Provisioned Certificate to the Wi-Fi Uplink

Aruba Instant8.12.0.0 introduces the ability to auto-assign an EST received certificate to the Wi-Fi Uplink features, such that it can be used to support an EAP-TLS authentication. This implementation automatically renews the digital certificate that is about to expire, which solves the problem where the wifi1x function is not available if the certificate is not manually uploaded after it expires. The process to configure this feature is outlined below:

1. Connect the AP to the network through eth or another Wifi-uplink connection.
2. Configure the EST service on CPPM For complete technical details and installation instructions, see the CPPM User Manual
3. Configure an accessible EST server on the AP
4. Obtain all certificates through the EST server.

For complete technical details, see the Instant User Guide.

Enhanced USB Dongle Firmware Upgrade for SES-Imagotag SCD

This release introduces an advanced feature for the SES-Imagotag SCD. This enhancement enables the capability for dongles to generate a Claim-ID, a critical component for establishing a secure connection

to V:Cloud. This feature addresses the need for enhanced security in data communication between retail management systems and V:Cloud.

Port Bounce for Wired Clients on Instant Access Points

This release introduces a new feature for Instant APs that automatically reinitiates DHCP requests following a VLAN change. This enhancement specifically affects wired non-802.1x clients in scenarios where there is a change in authorization events.

Deprecation of SHA-1 Cipher Suites for RadSec Server

The **radsec-ciphers-level <all|high>** parameter has been introduced under the **wlan auth-server** command. The parameter allows users to include or exclude SHA-1 cipher suites from the RadSec server.

Detection and Containment of Wi-Fi Direct Devices

The **detect-wifi-direct-p2p-groups**, **protect-wifi-direct-p2p-groups**, and **wifi-direct-network-quiet-time** commands have been introduced to detect and contain devices associated with Wi-Fi Direct groups under the IDS profile.

Vendor Specific IE based Containment

Aruba Instant allows users to configure exclusions for IDS containment based on vendor specific IE information. This feature allows APs to be exempted from containment even when the devices use randomized MAC addresses. To exempt APs from containment, users should configure the vendor OUI and OUI type in the IDS unauthorized device profile. A maximum of five vendor OUI and OUI types can be defined for confinement exclusion.

Support for NTP Authentication Mode

Aruba Instant allows users to configure Network Time Protocol (NTP) keys to authenticate servers. This feature can be configured through the CLI using the **ntp-authentication-key**, **ntp-trustedkey**, and **ntp-server-key** commands. The **show ntp authentication keys** and **show running-config | include ntp** commands list the details of the configured ntp authentication keys.

Enhancement to IDS Rogue Classification

Both wireless and wired MAC addresses are recorded for IDS rogue detection, thus ensuring that the Instant AP provides more details on IDS rogue classification to the user.

Support for SSL Throttling

SSL throttle can now be configured manually using the **set-sysctl ssl_throttle_table** command to a value between 1–32; the default value is 16. The **get-sysctl ssl_throttle_table** command can be used to view the configured SSL throttle value.

Firmware Synchronization Improvement in CoP for Instant AP Cluster with Different Models

Aruba Instant 8.12.0.0 improves firmware synchronization in CoP for Instant AP cluster with different models.

Enhancement to debug pkt dump for Enforce DHCP Violation

The output for **debug pkt dump** includes information regarding packets drops that occur due to enforce DHCP violations.

VAP Creation in 500 Series APs with New Toggle for GCM-256 Encryption

The **gcm-256-sw-encrypt-support** command has been introduced to enable/disable GCM-256 software encryption and allow for Virtual AP creation in both CNSA and non-CNSA SSIDs. This new configuration benefits those APs that do not support hardware encryption, like the 510 Series and 570 Series. By default, this configuration is **disabled**. So, it is important to note that if upgrading from Aruba Instant 8.11.x to Aruba Instant 8.12.x, GCM-256-based VAPs on the affected platforms will be disabled, and enabling the command will be required to configure them. Also, please be aware that software encryption has significantly lower performance than hardware encryption.

Behavioral Changes

This release does not introduce any changes in Aruba Instant behaviors, resources, or support that would require you to modify the existing system configurations after updating to 8.12.0.0.

Chapter 3
Supported Hardware Platforms

The following table displays the Instant AP platforms supported in Aruba Instant 8.12.0.x release.

Table 3: *Supported Instant AP Platforms*

Instant AP Platform	Minimum Required Instant Software Version
670 Series — AP-675, AP-675EX, AP-677, AP-677EX, AP-679, and AP-679EX	Instant 8.12.0.0
600 Series — AP-605H	Instant 8.12.0.0
503 Series — AP-503	Instant 8.11.1.0 or later
503 Series — AP-503	Instant 8.11.1.0 or later
610 Series — AP-615	Instant 8.11.0.0 or later
580 Series — AP-584, AP-585, and AP-587 580EX Series — AP-585EX and AP-587EX 650 Series — AP-655	Instant 8.10.0.0 or later
630 Series — AP-635	Instant 8.9.0.0 or later
500H Series — AP-503H 560 Series — AP-565 and AP-567	Instant 8.7.1.0 or later
500H Series — AP-505H 518 Series — AP-518 570 Series — AP-574, AP-575, and AP-577 570EX Series — AP-575EX and AP-577EX	Instant 8.7.0.0 or later
500 Series — AP-504 and AP-505	Instant 8.6.0.0 or later
530 Series — AP-534 and AP-535 550 Series — AP-555	Instant 8.5.0.0 or later
303 Series — AP-303P 510 Series — AP-514 and AP-515	Instant 8.4.0.0 or later
303 Series — AP-303 318 Series — AP-318 370 Series — AP-374, AP-375, and AP-377 370EX Series — AP-375EX and AP-375EX	Instant 8.3.0.0 or later
303H Series — AP-303H 360 Series — AP-365 and AP-367	Instant 6.5.2.0 or later
300 Series — IAP-304 and IAP-305	Instant 6.5.1.0-4.3.1.0 or later
310 Series — IAP-314 and IAP-315	Instant 6.5.0.0-4.3.0.0 or later

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 www.networkingsupport.hpe.com .

The following DRT file version is part of this release:

- DRT-1.0_89073

Chapter 5
Resolved Issues

The following issues are resolved in this release.

Table 4: *Resolved Issues in Instant 8.12.0.0*

Bug ID	Description	Reported Version
AOS-195769	In some Instant APs set up with dynamic VLAN assignment, ARP or GARP traffic was unexpectedly sent to wireless clients, even if they were connected to a different VLAN and VAP. This issue was observed in the following scenarios: ■ When the broadcast packets from VLAN 1 and all of the clients on the SSID were on VLAN 2, the packets were sent to all VAPs belonging to the same SSID. ■ When the SSID had two VAPs that belong to the same VLAN, but only one VAP had clients on that VLAN, the traffic was forwarded to both VAPs. ■ When all of the VAPs of a given SSID have clients on different VLANs, the packets were broadcasted to all VLANs. The fix ensures that GARP traffic function as expected. This issue was observed in Instant APs running Aruba Instant 8.6.0.0 or later versions.	Aruba Instant 8.6.0.0
AOS-215025	Information was missing from the output of the **show ap dot11k-beacon-report** and **show ap dot11k-stat** commands when the **dot11k** setting was enabled on an Instant AP. The fix ensures that the **show ap dot11k-beacon-report** and **show ap dot11k-stat** commands function as expected when the **dot11k** setting is enabled. This issue was observed in APs running Aruba Instant 8.4.0.0 or later versions.	Aruba Instant 8.6.0.6
AOS-225670 AOS-247530	Instant APs displayed incorrect **Role** information in the output of the **show clients** command. This issue occurred when the MPSK local key role was changed through the Central UI. The fix ensures the correct information is displayed in the command output. This issue was observed in Central-managed APs running Aruba Instant 8.6.0.0 or later versions.	Aruba Instant 8.10.0.0
AOS-230124 AOS-231165	Multiple core files were created for the **dpimgr** process on Instant APs in a cluster setup. The fix ensures the APs work as expected. This issue was observed in Central-managed APs running Aruba Instant 8.6.0.0 or later versions.	Aruba Instant 8.7.1.7
AOS-231129	Instant APs did not send the cold and warm SNMP traps when expected. THe fix ensures that the APs function as expected. This issue was observed in APs running Aruba Instant 8.0.0.0 or later versions.	Aruba Instant 8.6.0.8

Table 4: *Resolved Issues in Instant 8.12.0.0*

Bug ID	Description	Reported Version
AOS-231846	Wired clients connected to an Instant AP were not displayed in the **Clients > Wired** page of the Aruba Central UI. This issue occurred with wired clients whose MAC address ended with the characters **FF** (**xx:xx:xx:xx:xx:FF**). The fix ensures that connected wired clients are displayed in the **Clients > Wired** page as expected. This issue was observed in Aruba Central-managed Instant APs running Aruba Instant 8.6.0.16 or later versions.	Aruba Instant 8.6.0.9
AOS-234042 AOS-234060 AOS-236584	Some Instant APs in a cluster crashed and rebooted unexpectedly. The log file listed the reason for reboot as: **Reboot Time and Cause: AP Reboot reason: Some Crash Warm-reset**. The fix ensures that the APs function as expected. This issue was observed in AP-345 access points running Aruba Instant 8.6.0.16 or later versions.	Aruba Instant 8.6.0.16
AOS-234532 AOS-246059	Some Central-managed APs triggered multiple alerts stating **Radio frames retry percent for AP has been above 90% for about 15 minutes**, under the **Analyze > Alerts & Events > Critical > OPEN ALERTS** section of Central. The issue was related to a miscalculation in the **Radio Frames Retry Percent** process, due to a miscount of the Tx MPDU values. The fix includes an enhancement to the total Tx MPDU transmitted counter, resolving the issue and eliminating the alerts. The issue was observed in APs running Aruba Instant 8.9.0.0 or later versions.	Aruba Instant 8.9.0.0
AOS-235218 AOS-235584	Instant APs in a cluster reported high CPU and memory utilization. This issue occurred due to a memory leak in the **dpimgr** process. The fix ensures that the APs function as expected. This issue was observed in Central-managed APs running Aruba Instant 8.6.0.18 or later versions.	Aruba Instant 8.6.0.18
AOS-235685	Users experienced delay or dropped voice calls while roaming between Instant APs. The fix ensures that the AP functions as expected without delays or dropped voice calls. This issue was observed in Central-managed AP-515 and AP-575 access points running Aruba Instant 8.6.0.20 or later versions.	Aruba Instant 8.7.1.9
AOS-236052	An Instant AP did not update its IP address and retained its original IP address. This issue occurred when the AP switched to a different VLAN using ClearPass. The fix ensures the IP address of the AP is updated as expected. This issue was observed in APs running Aruba Instant 8.7.1.3 or later versions.	Aruba Instant 8.7.1.3
AOS-237132	The MSS value did not change when the data packets were routed through the IAP-VPN tunnel. This issue occurred when PPPoE uplink was configured. The fix ensures that the correct MSS value is displayed. This issue was observed in APs running Aruba Instant 6.4.3.4-4.2.1.0 or later versions.	Aruba Instant 6.4.3.4-4.2.1.0
AOS-237413	High memory utilization was observed in a cluster consisting of APs. The issue occurred in environments where the SNMP server did not have **username** field in trap inform response message, which caused the process memory leak. This issue was observed in Instant AP clusters running Aruba Instant 8.6.0.18 or later versions.	Aruba Instant 8.6.0.18

Table 4: *Resolved Issues in Instant 8.12.0.0*

Bug ID	Description	Reported Version
AOS-237750 AOS-239650	An Instant AP crashed and rebooted when pre-auth roles was not configured and DPI was enabled. The log file listed the reason for the reboot as **BadPtr: 00000000 PC: strncpy+0xc/0x28 Warm-reset**. The fix ensures that the AP does not crash when pre-auth roles are not configured. This issue was observed in APs running Aruba Instant 8.10.0.0 or later versions.	Aruba Instant 8.10.0.4
AOS-237859 AOS-237874	Instant APs experienced connectivity issues in an environment where both wifi-uplink and mesh links coexisted in the same radio. The fix ensures the mesh link moves to a non-interfering band in this scenario. For example: ■ wifi-uplink on band **a** and mesh link operates in 5 GHz or 6 GHz bands. Mesh link will connect to the 6 GHz band. ■ wifi-uplink on 6 GHz, and mesh link operates in 5 GHz or 6 GHz bands. Mesh link will connect to the 5 GHz band. ■ wifi-uplink and mesh -band are on 6 GHz , mesh will go to 5 GHz This issue was observed in access points running Aruba Instant 8.11.0.0 or later versions.	Aruba Instant 8.11.0.0
AOS-237965 AOS-237699	View-only users were unable to perform debug operations. This issue occurred when the user was able to log in while the Instant AP was in a degraded state. The fix ensures that view-only users are able to perform debug operations. This issue was observed in APs running Aruba Instant 8.10.0.2 or later versions.	Aruba Instant 8.10.0.2
AOS-238137	The **traceroute** command returned the following error message: **Can't find tsgw src ip**. This issue occurred when the Instant AP had multiple routing entries in the routing profile. The fix ensures that the **traceroute** command functions as expected. This issue was observed in APs running Aruba Instant 8.10.0.3 or later versions.	Aruba Instant 8.10.0.3
AOS-238155	Member Instant APs were unable to broadcast an SSID when connected to the Ethernet 1 port through fiber link. This issue occurred when **out-of-service internet-down** setting was enabled. The fix ensures that the **internet-down** status is displayed only on the conductor AP. This issue was observed in Central-managed APs running Aruba Instant 8.6.0.17 or later versions.	Aruba Instant 8.6.0.17
AOS-238198	Some Instant APs took longer than expected to apply uplink band configurations. The fix ensures the Instant APs work as expected. This issue was observed in Instant APs running Aruba Instant 8.11.0.0 or later versions.	Aruba Instant 8.11.0.0
AOS-238228	Client devices experienced network connectivity issues intermittently. This issue occurred when: ■ An Instant AP was in Wi-Fi uplink dot1x mode. ■ The AP attempted to connect with a device having a reauthentication configuration. The fix ensures that the clients can connect to the network seamlessly. This issue was observed in AP-303H access points running Aruba Instant 8.7.1.8 or later versions.	Aruba Instant 8.7.1.8

Table 4: *Resolved Issues in Instant 8.12.0.0*

Bug ID	Description	Reported Version
AOS-238326	An Instant AP crashed and rebooted due to high memory utilization. The log file listed the reason for the event as **Reboot caused by kernel panic: MemLeak: mem low for 60 seconds, under 0MB 10 times, MB free 11 (4%), total 247**. The fix ensures that the AP functions as expected. This issue was observed in APs with less than 256 MB RAM and AP-203H access points running Aruba Instant 8.6.0.18 or later versions.	Aruba Instant 8.6.0.18
AOS-238369	The **Devices > Access Points > Overview > RF** tab of the Aruba Central UI displayed 100% error for multiple Instant AP due to incorrect statistics. The fix ensures that the UI displays correct RF values. This issue was observed in Central-managed APs running Aruba Instant 8.6.0.17 or later versions.	Aruba Instant 8.6.0.17
AOS-238393	HE clients were unable to pass traffic when the SSID was configured with WPA3 enterprise encryption. The fix ensures that HE clients are able to pass traffic when WPA3 enterprise encryption is configured for the SSID. This is issue was observed in 500 Series and 510 Series access points running Aruba Instant 8.11.0.0 or later versions.	Aruba Instant 8.11.0.0
AOS-238447	Some AP-303Haccess points crashed when a USB LTE modem was connected. The fix ensures the AP works as expected in this scenario. This issue was observed in APs running Aruba Instant 8.11.1.0 or later versions.	Aruba Instant 8.11.1.0
AOS-238535 AOS-240748	The output of the **show dpi-app stats full** command displayed incorrect values when the command was executed after a 15 minute interval. The fix ensures that the correct values are displayed when the **show dpi-app stats full** command is executed. This issue was observed in APs running Aruba Instant 8.6.0.19 or later versions.	Aruba Instant 8.11.0.0
AOS-238808	An Instant AP was unable to form a mesh link at the 60 GHz and was denylisted. The fix ensures that the 60 GHz connection was formed by default. This issue was observed in AP-387 access points running Aruba Instant 8.6.0.19 or later versions.	Aruba Instant 8.6.0.19
AOS-239368	Instant APs in a cluster did not retain the configured CPPM username and password. This issue occurred when the APs were rebooted while the password exceeded 23 characters. The fix ensures that the APs retain the configured CPPM username and password. This issue was observed in APs running Aruba Instant 8.9.0.2 or later versions.	Aruba Instant 8.9.0.2
AOS-239411	Instant APs did not accept the serial number of the device as the default password after a factory reset. This issue occurred when the AP was reset using the **factory reset** command in AP boot mode. The fix ensures that the AP accepts the serial number as the default password after a factory reset. This issue was observed in APs running Aruba Instant 8.9.0.0 or later versions.	Aruba Instant 8.10.0.0
AOS-239419 AOS-238100	The eth0 link of an Instant AP appeared offline in the AirWave UI. The fix ensures that the eth0 link status is displayed correctly in the AirWave UI. This issue was observed in AirWave-managed APs running Aruba Instant 8.6.0.18 or later versions.	Aruba Instant 8.6.0.18

Table 4: *Resolved Issues in Instant 8.12.0.0*

Bug ID	Description	Reported Version
AOS-239575 AOS-243208 AOS-244929	Users were unable to configure RTLS or VC DNS IP address when FIPS mode was enabled. The fix ensures that users are able to configure RTLS and VC DNS IP address when FIPS mode is enabled. This issue was observed in Central-managed APs running Aruba Instant 8.10.0.3 or later versions.	Aruba Instant 8.10.0.3
AOS-239586	An Instant AP name was displayed incorrectly in the **Live Events** tab of the Central UI, after the name is updated. This issue was observed in Central-managed APs running Aruba Instant 8.10.0.4 or later versions.	Aruba Instant 8.10.0.4
AOS-239682	Some WLAN networks were created randomly in the **Overview** > **Summary** > **WLANs** page of the WebUI, and the network name appeared as Unicode symbols. The fix ensures the WebUI works as expected. This issue was observed in Aruba Central managed AP-315 access points running Aruba Instant 8.7.1.10 or later versions.	Aruba Instant 8.7.1.10
AOS-239919	An Instant AP connected to a switch port with single stack IPv6 VLAN was unable to obtain DHCPv6 addresses. This caused the AP to revert to IAP mode. The fix ensures that the IPv6 process for obtaining the DHCPv6 addresses is restarted if the AP fails to obtain the addresses. This issue was observed in APs running Aruba Instant 8.10.0.1 or later versions.	Aruba Instant 8.10.0.2
AOS-240080 AOS-245100	After configuring multiple DNS IP servers by using a separating comma, the **Overview > Summary > DNS NAME SERVERS** section of the Central UI showed an incorrect number of DNS servers. The fix ensures the saved configuration is displayed accurately in the UI. This issue was observed in Instant APs managed by Central running Aruba Instant 8.11.1.0 or later versions.	Aruba Instant 8.11.1.0
AOS-240096	Clients were unable to connect to the SSID when: ▪ Two SSID profiles had the same ESSID. ▪ Both **time range profile** and **SSID Zone** were configured on the Instant AP. This issue was observed in Central-managed APs running Aruba Instant 8.7.0.0 or later versions.	Aruba Instant 8.7.1.9
AOS-240114	Client traffic was not forwarded by an Instant AP. This issue occurred when the **deny-intra-vlan-traffic** was enabled and VRRP was configured on the upstream default router. This issue was observed in Instant APs running Aruba Instant 8.10.0.6 or later versions. The fix ensures that users are able to pass client traffic.	Aruba Instant 8.11.0.0
AOS-240139	An Instant AP in a cluster did not generate an SNMP trap when rogue APs were detected. The fix ensures that the AP generates SNMP traps when rogue APs are present. This issue was observed in APs running Aruba Instant 8.7.0.0 or later versions.	Aruba Instant 8.10.0.4
AOS-240176	Users were unable to configure the **Quality of Service** and **DSCP TAG** type of an Instant AP when application-based ACL was configured for ICMP. The fix ensures that users are able to configure the **Quality of Service** and **DSCP TAG** type for the ICMP application. This issue was observed in Central-managed APs running Aruba Instant 8.6.0.0 or later versions.	Aruba Instant 8.6.0.0

Table 4: *Resolved Issues in Instant 8.12.0.0*

Bug ID	Description	Reported Version
AOS-240180	An Instant AP was unable to resolve the FQDN. This issue occurred when the AP DNS packet failed to skip the default tunnel route when **Dynamic DNS** was enabled in the DHCP profile. The fix ensures that the AP DNS packet does not skip the default tunnel route even if **Dynamic DNS** was enabled. This issue was observed in APs running Aruba Instant 8.10.0.3 or later versions.	Aruba Instant 8.10.0.3
AOS-240266	An Instant AP rejected association requests. The log file listed the reason as: **AP is resource constrained-Max Clients Associated**. This issue occurred even though there were no clients associated with the AP. The fix ensures that the AP functions as expected. This issue was observed in APs running Aruba Instant 8.6.0.0 or later versions.	Aruba Instant 8.10.0.3
AOS-240398	Wireless users did not receive IP addresses from the DHCP server when the software version of Instant APs was upgraded to Aruba Instant 8.6.0.19 or later. The fix ensures that users receive IP addresses from the server when the AP boots up. This issue was observed in APs running Aruba Instant 8.6.0.19 or later versions.	Aruba Instant 8.6.0.19
AOS-240459	Static IP addresses of locally managed Instant APs were changed to DHCP IP addresses if the configured default gateway was unreachable. The fix ensures that the IP address configuration does not change when the default gateway is unreachable. This issue was observed in APs running Aruba Instant 6.5.0.0 or later versions.	Aruba Instant 6.5.4.20
AOS-240507	The output of the **iftype** command displayed incorrect SNMP values. The fix ensures that the **iftype** command displays the correct SNMP values. This issue was observed in APs running Aruba Instant 8.6.0.0 or later versions.	Aruba Instant 8.7.1.11
AOS-240530	Instant APs returned the following error message **auth_cppm_ instant.c, auth_cppm_transform:1859: Dldb Role pf_iap_dur-3008-26: Buffer too large**. This issue occurred when the buffer size of the downloadable user role sent from the ClearPass Policy Manager exceeded 16 KB. The fix ensures that the AP functions as expected. This issue was observed in APs running Aruba Instant 8.10.0.0 or later versions.	Aruba Instant 8.10.0.4
AOS-240727	The DHCP server failed to start with the correct interface. The server also did not issue IPv4 or IPv6 addresses in the guest or DHCP scope defined VLANs. The fix ensures that the DHCP server starts with the correct interface. This issue was observed in APs running Aruba Instant 8.10.0.0 or later versions.	Aruba Instant 8.11.0.1
AOS-240805	Users were unable to upgrade the software version of AP-635 and AP-655 access points using REST API. The fix ensures that the software upgrades using REST API are successful for AP-635 and AP-655 access points. This issue was observed in APs running Aruba Instant 8.10.0.0 or later versions.	Aruba Instant 8.11.0.0

Table 4: *Resolved Issues in Instant 8.12.0.0*

Bug ID	Description	Reported Version
AOS-241109	The backup SSID was enabled when internet connectivity went down. However, the backup SSID was still enabled when the internet connectivity was restored. This issue occurred as the device statistics were not cleared automatically. The fix ensures that the backup SSID is disabled when internet connectivity is restored. This issue was observed in APs running Aruba Instant 8.10.0.5 or later versions.	Aruba Instant 8.10.0.5
AOS-241197	An Instant AP generated **sapd** core during boot up. The fix ensures that the APs work as expected. This issue was observed in AP-575 access points running Aruba Instant 8.10.0.5 or later versions.	Aruba Instant 8.10.0.5
AOS-241203	High memory utilization was reported on some Instant APs because the AWC process was consuming high memory. This caused the APs to become unresponsive. The fix ensures that the APs function as expected. This issue was observed in APs running Aruba Instant 8.10.0.0 or later versions.	Aruba Instant 8.10.0.0
AOS-241395	Some Instant APs repeatedly formed a connection with PAN firewall despite there being no user connected to the APs. The fix ensures that the APs function as expected. This issue was observed in APs running Aruba Instant 8.6.0.0 or later versions.	Aruba Instant 8.6.0.0
AOS-241743 AOS-242212 AOS-244549	Users were unable to connect to the cloud guest SSID, and were being redirected to the Captive Portal page. The log file listed the following reason for the error: **Internal Error while getting request ID in radsec server**. The fix ensures that users are able to connect to cloud guest SSID without issues. This issue was observed in APs running Aruba Instant 8.10.0.5 or later versions.	Aruba Instant 8.10.0.6
AOS-242008	Instant APs crashed and rebooted unexpectedly. The log file listed the reason for reboot as **Reboot caused by kernel panic: assert**. The fix ensures that the APs function as expected. This issue was observed in AP running Aruba Instant 8.10.0.0 or later versions.	Aruba Instant 8.10.0.5
AOS-242056	A delay in IDS to classify Instant APs as rogue was observed in AP-535 access points running Aruba Instant 8.10.0.5 or later versions. This issue occurred because the time taken to detect the rogue AP included the scanning duration time. This issue was fixed by changing the rogue classification delay from monitored time to discovered time.	Aruba Instant 8.10.0.5
AOS-242249 AOS-244271	Multiple client devices connected to IAP-315 access points were not obtaining an IP address. After rebooting the Instant APs, the client's devices obtained the IP address. This was caused by a memory leak when DMO was enabled and air-time-fairness-mode config preferred-access. The fix ensures the Instant APs perform as expected. This issue was observed in IAP-315 access points running Aruba Instant 8.9.0.2 or later versions.	Aruba Instant 8.10.0.5
AOS-242271	Multiple DHCP server connection errors were reported on the **AI Insights** dashboard of the Central UI. The fix ensures that the process works as expected. This issue was observed in Central-managed APs running Aruba Instant 8.7.1.0 or later versions.	Aruba Instant 8.7.1.0
AOS-242512	The dynamic TACACS proxy authentication process did not work as expected in APs running Aruba Instant 8.11.0.1 or later versions. The fix ensures this process works as intended.	Aruba Instant 8.11.0.1

Table 4: *Resolved Issues in Instant 8.12.0.0*

Bug ID	Description	Reported Version
AOS-242628	The **MIB_WLAN_INDEX** entry displayed an incorrect value in **MIB_WAP_TABLE**. As a result, the correct ESSID of the Instant APs were not displayed in the AirWave WebUI. The fix ensures that the correct ESSID names are displayed. This issue was observed in AirWave managed Instant AP clusters running Aruba Instant 8.3.0.0 or later versions.	Aruba Instant 8.3.0.0
AOS-242654	Instant APs were caught in a reboot loop when the user attempted to upgrade the software version to Aruba Instant 8.8.0.0 or later. The log file listed the reason for this event as **Current uplink down, no useable uplink**. The fix ensures that the APs function as expected when the user upgrades the software version. This issue was observed in Central-managed AP-303H access points running Aruba Instant 8.8.0.0 or later versions.	Aruba Instant 8.10.0.6
AOS-242732	Instant 802.11ax access points experienced a noticeable performance drop when the **air-time-fairness** setting was set to **fair-access** instead of **default-access**. The issue was related to the **air-time-fairness** feature not being compatible with modern APs. The fix ensures this configuration does not impact newer APs negatively. This issue was observed in APs running Aruba Instant 8.10.0.0 or later versions.	Aruba Instant 8.10.0.0
AOS-242779	In some APs running Aruba Instant 8.10.0.6 or later versions, a **Check sum mismatch** error was displayed. The issue occurred when the MPSK key name included a space. The fix ensures the correct checksum value is displayed.	Aruba Instant 8.10.0.6
AOS-242841 AOS-250716 AOS-247907	In some cases, AppRF displayed unreliable aggregated statistics after a long period of time. The fix ensures the AppRF aggregated statistics are accurate. This issue was observed in APs running Aruba Instant 8.6.0.0 or later versions.	Aruba Instant 8.11.1.0
AOS-243125 AOS-245986	Instant APs reported high memory utilization when the Central connection was unstable. This issue occurred after the software was upgraded to Aruba Instant 8.11.1.0 or later versions. The fix ensures that the APs function as expected. This issue was observed in Central-managed APs running Aruba Instant 8.11.1.0 or later versions.	Aruba Instant 8.11.1.1
AOS-243184	An Instant AP displayed incorrect country codes in the air captured packet, although the correct country code was configured on the AP. The fix ensures that the configured country codes are displayed in the air capture packet. This issue was observed in APs running Aruba Instant 8.10.0.5 or later versions.	Aruba Instant 8.10.0.5
AOS-243414	Instant APs did not send updated DNS parameters to Central. The fix ensures the APs send the accurate information to Central. This issue was observed in APs running Aruba Instant 8.7.1.5 or later versions.	Aruba Instant 8.7.1.5
AOS-244068	The containment feature was not effectively functioning for clients connected across various channels. The fix ensures the feature works as expected. This issue was observed in IAP-505 running Aruba Instant 8.10.0.0 or later versions.	Aruba Instant 8.10.0.0
AOS-244395	An Instant AP failed to establish TLS connection with the RADIUS server . The fix ensures that the AP is able to establish TLS connection with the RADIUS server. This issue was observed in Central-managed APs running Aruba Instant 8.6.0.0 or later versions.	Aruba Instant 8.10.0.6

Table 4: *Resolved Issues in Instant 8.12.0.0*

Bug ID	Description	Reported Version
AOS-244640	Users were unable to perform EAP-TLS authentication when a custom certificate was used. The fix ensures that the AP established TLS connections using the custom certificate. This issue was observed in APs running Aruba Instant 8.6.0.2 or later versions.	Aruba Instant 8.11.1.0
AOS-244876	The output of the **show ap regulatory** command was missing from the tech-support supplemental. The fix ensures that the output of the **show ap regulatory** command is included in the tech-support supplemental. This issue was observed in APs running Aruba Instant 8.6.0.0 or later versions.	Aruba Instant 8.11.0.1
AOS-245417	Some access points configured as a mesh portal transmitted at reduced power levels despite being set to full power. The issue was observed after the APs were rebooted and powered up with the 5 GHz band disabled under all WLAN profiles. The fix ensures the APs work as expected. This issue was observed in AP-575 access points running Aruba Instant 8.10.0.6 or later versions.	Aruba Instant 8.10.0.6
AOS-245804	Instant APs incorrectly resolved the device connectivity URL to the firewall IP address. This issue occurred because the AP cached the DNS query result into the hosts file. The fix removes the cache entry before the AP connected to Aruba Central. This issue was observed in Central-managed APs running Aruba Instant 8.10.0.0 or later versions.	Aruba Instant 8.10.0.6
AOS-245899	The **AI Insights** dashboard incorrectly showed high CPU usage for APs on the Central UI. The fix ensures that **AI Insights** does not show incorrect CPU data. This issue was observed in Central-managed AP-615 access points running Aruba Instant 8.11.0.0 or later versions.	Aruba Instant 8.11.0.0
AOS-246255	Some Instant APs were unable to join a Virtual Controller cluster. The Central UI did not display such APs within their group. This issue was related to the Virtual Controller failing to upgrade its DRT. The fix ensures that the APs can join Virtual Controller clusters and groups in Central. This issue was seen in APs running Aruba Instant 8.10.0.2 or later versions.	Aruba Instant 8.10.0.2
AOS-246337	For some Instant APs in a cluster, 5 GHz radio band was intermittently down on the Central UI. The fix ensures that the 5 GHz radio functions as expected. This issue was observed in Central-managed APs running Aruba Instant 8.10.0.6 or later versions.	Aruba Instant 8.10.0.6
AOS-246408	The **aiRadioChannel** parameter of the MIB node did not include details about the 40 MHz, 80 MHz, and 160 MHz channels. The fix ensures that the information appears as expected. This issue was observed in APs running Aruba Instant 8.6.0.2 or later versions.	Aruba Instant 8.6.0.2
AOS-246493	Fake SSIDs were displayed for Instant APs in the Aruba Central UI. The fix ensures that only real SSIDs are displayed under the **AP > Overview > Summary** page of the Central UI. This issue was observed in Central-managed APs running Aruba Instant 8.11.1.1 or later versions.	Aruba Instant 8.11.1.1

Table 4: *Resolved Issues in Instant 8.12.0.0*

Bug ID	Description	Reported Version
AOS-246548	Multiple wireless clients experienced cloud authentication failure after upgrading the software version. The logs listed the reason for the error as **Internal Error while getting request ID in radsec server.** The fix ensures that the clients do not experience cloud authentication failure after upgrading the software version. This issue was observed in Central-managed APs running Aruba Instant 8.6.0.0 or later versions.	Aruba Instant 8.11.1.0
AOS-246591	Some Central-managed APs did not generate the output of the **show tech-support** command. The logs displayed the message **Waiting for response for command show tech-support...**, and eventually displayed the error **No response was received for command show tech-support**. The fix ensures the command works as expected. This issue was observed in Central-managed APs running Aruba Instant 8.10.0.1 or later versions.	Aruba Instant 8.10.0.1
AOS-246617	After upgrading to Aruba Instant 8.10.0.7, some Instant APs crashed and rebooted unexpectedly, disconnecting every 2-3 hours due to IPv6 packet synchronization problems. The crash logs listed the reason for the error as **Panic:Ktrace core monitor: cpu3 hung for 45 seconds, hung cpu count: 1 Warm-reset.** The fix ensures that the APs work as expected. This issue was observed in AP-515 access points running Aruba Instant 6.5.4.0 or later versions.	Aruba Instant 8.10.0.7
AOS-246735 AOS-246633 AOS-247461	Some access points crashed with reason **BadAddr:ffffffc133b1e424 PC:memcmp+0xd0/0x1c0 Warm-reset.** The fix ensures Instant APs work as expected. This issue was observed in AP-515 and AP-575 access points running Aruba Instant 8.10.0.0 or later versions.	Aruba Instant 8.10.0.0
AOS-247151	The output of the **show backup-config** command did not include configuration details for AP-635 access points. The fix ensures that the output of the **show backup-config** command includes the configuration details. This issue was observed in AP-635 access points running Aruba Instant 6.5.4.0 or later versions.	Aruba Instant 8.11.1.0
AOS-247318 AOS-249944	Instant APs crashed unexpectedly when the **show ap debug radius-statistics** command was executed. The command returned the following error message: **Module AP STM Low Priority is busy**. The fix ensures that the **show ap debug radius-statistics** command functions as expected. This issue was observed in APs running Aruba Instant 8.10.0.0 or later versions.	Aruba Instant 8.10.0.8
AOS-247394	While running the **show auth-survivability cache-info** command, the username displayed random characters for strings longer than 16 characters. The fix ensures the usernames are displayed correctly. This issue was observed in some Instant APs runningAruba Instant 6.5.4.0 or later versions.	Aruba Instant 6.5.4.0
AOS-248170 AOS-205658	Some APs became virtual controllers after experiencing a power outage. The issue occurred when the uptime beacon protocol was designed in 32 bits instead of 64 bits, and the uptime was less than 300 seconds. The fix ensures the APs work as expected. This issue was observed in access points running Aruba Instant 8.10.0.6 or later versions.	Aruba Instant 8.10.0.6

Table 4: *Resolved Issues in Instant 8.12.0.0*

Bug ID	Description	Reported Version
AOS-248634	Instant APs randomly generated the following error message: **An internal system error has occurred at file cli_swarm.c function get_user_acct_counters_ctx line 34902**. The fix ensures that the APs do not generate random error messages. This issue was observed in APs running Aruba Instant 8.11.2.0 or later versions.	Aruba Instant 8.11.2.0
AOS-249004	The **Cellular Status** and **USB Modem Information** tables were missing from the output of the **show cellular status** command. The fix ensures that the output includes the **Cellular Status** and **USB Modem Information** tables. This issue was observed in Instant APs running Aruba Instant 8.10.0.0 or later versions.	Aruba Instant 8.11.2.0
AOS-249437 AOS-250853	Mesh point Instant APs failed to connect to the portal and the portal failed to update the channel bandwidth to the configured value. This issue occurred when: ▪ **no 80mhz-support** was configured under the ARM profile. ▪ **mesh-band 6ghz** was configured. The fix ensures that the mesh point APs function as expected. This issue was observed in APs running Aruba Instant 8.10.0.0 or later versions.	Aruba Instant 8.11.2.1
AOS-249817	The AP BLE antenna was not able to scan. The issue occurred if the AP was broadcasting the SSID on Wi-Fi channel 11 or Wi-Fi channel 1. The fix ensures the AP works as expected. This issue was observed in AP-635 access points running Aruba Instant 8.11.2.0 or later versions.	Aruba Instant 8.11.2.0
AOS-250160 AOS-250315	The **Non-DTLS Members** parameter changed to **Deny** on the **Configuration > System** page when the WebUI was refreshed. However, the output of the **show cluster-security** command indicated that the Non-DTLS members parameter was set to **Allow**. The fix ensures the values match correctly. This issue was observed in APs running Aruba Instant 8.10.0.1 or later versions.	Aruba Instant 8.10.0.1
AOS-250362	Some Instant AP members failed to join the cluster after upgrading the software version. This issues occurred when the DRT download failed. The fix ensures that the APs join the cluster after the software upgrade. This issue was observed in Central-managed APs running Aruba Instant 8.10.0.0 or later versions.	Aruba Instant 8.10.0.9

Chapter 6
Known Issues and Limitations

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

Known Issues

Following are the known issues observed in this release.

Table 5: *Known Issues in Instant 8.12.0.0*

Bug ID	Description	Reported Version
AOS-239482	Some Instant APs with Wi-Fi configuration and a 5 GHz radio connectivity are unable to setup a mesh topology. This issue is observed in AP-635 and AP-655 Instant APs running Aruba Instant 8.12.0.0.	Aruba Instant 8.12.0.0

Chapter 7
Upgrading an Instant AP

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

While upgrading an Instant 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 Aruba Instant 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 Aruba Instant 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 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.