Aruba Instant 8.6.0.22

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.

Contents

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:

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	https://asp.arubanetworks.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.

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.

Enhancements to Technical Support Logs

The **show tech-support** command has been modified to reduce response time and improve customer experience. This change adds **show ap regular** and **show drt status** in **show tech-support supplemental** command.

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.

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 8.6.0.22.

Chapter 3
Supported Hardware Platforms

The following table displays the Instant AP platforms supported in Aruba Instant 8.6.x release.

Table 3: *Supported Instant AP Platforms*

Instant AP Platform	Minimum Required Instant Software Version
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 387 Series — AP-387 510 Series — AP-514 and AP-515	Instant 8.4.0.0 or later
303 Series — AP-303 318 Series — AP-318 340 Series — AP-344 and AP-345 370 Series — AP-374, AP-375, and AP-377 370EX Series — AP-375EX and AP-377EX	Instant 8.3.0.0 or later
203H Series — AP-203H	Instant 6.5.3.0 or later
203R Series — AP-203R and AP-203RP 303H Series — AP-303H and AP-303HR 360 Series — AP-365 and AP-367	Instant 6.5.2.0 or later
207 Series — IAP-207 300 Series — IAP-304 and IAP-305	Instant 6.5.1.0-4.3.1.0 or later
310 Series — IAP-314 and IAP-315 330 Series — IAP-334 and IAP-335	Instant 6.5.0.0-4.3.0.0 or later
320 Series — IAP-324 and IAP-325	Instant 6.4.4.3-4.2.2.0 or later
228 Series — IAP-228 270 Series — IAP-277	Instant 6.4.3.1-4.2.0.0 or later
210 Series — IAP-214 and IAP-215	Instant 6.4.2.0-4.1.1.0 or later
270 Series — IAP-274 and IAP-275	Instant 6.4.0.2-4.1.0.0 or later
220 Series — IAP-224 and IAP-225	Instant 6.3.1.1-4.0.0.0 or later
RAP 155 Series — RAP-155 and RAP-155P	Instant 6.2.1.0-3.3.0.0 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 asp.arubanetworks.com.

The following DRT file version is part of this release:

- DRT-1.0_87407

Chapter 5
Resolved Issues

This chapter describes the issues resolved in this release.

Table 4: *Resolved Issues in Instant 8.6.0.22*

Bug ID	Description	Reported Version
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 during AP bootup. This issue was observed in APs running Aruba Instant 8.6.0.0 or later versions. The fix ensures that the Instant AP updates its IP address as expected.	Aruba Instant 8.6.0.0
AOS-237413	High memory utilization was observed in some AP-515 access point clusters, running Aruba Instant 8.6.0.18 or later versions. The issue occurred when the **snmpd_sap** process did not get a valid response from the SNMP server, causing the memory leak. The fix ensures responses from the SNMP server are handled correctly.	Aruba Instant 8.6.0.18
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-242628	The **MIB_WLAN_INDEX** entry displayed an incorrect value in **MIB_WAP_TABLE**. As a result, the correct ESSID of the Instant APs was not displayed in the AirWave WebUI. The fix ensures that the correct ESSID is 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-244068	Rogue Instant AP containment did not function as expected when detecting rogue APs with different channels. The fix ensures that the rogue AP containment is attempted on detected rogue APs with different channels. This issue was observed in Instant APs running Aruba Instant 6.5.4.0 or later versions.	Aruba Instant 8.11.0.1
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
AOS-245753	An Instant AP was unable to establish a RadSec connection with the cloud CPPM server. The output of the **show radius state** command displays the status of the RadSec server as **INIT**. The fix ensures that the AP connects to the cloud server as expected. This issue was observed in APs running Aruba Instant 8.6.0.0 or later versions.	Aruba Instant 8.6.0.20

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

Limitations

Airtime Fairness Mode

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

Important Update on Deprecated Access Points

The 210 Series, 220 Series, AP-228, and 270 Series access points will be deprecated for future releases and include the following limitations in Instant 8.6.0.x, which is the last supported software version for these access points:

- No support for BLE interface (with USB).
- The DPI engine used for AppRF will have limitations in terms of enhancements and fixes in the future.
- These APs use WolfSSL libraries in Instant 8.6.0.0 and not OpenSSL.
- No support for WPA3 security.

All of these platforms have already been marked as end-of-sale. Please review the end-of-sale and end-of-support dates for these platforms here.

Known Issues

Following are the known issues observed in this release.

Table 5: *Known Issues in Instant 8.6.0.22*

Bug ID	Description	Reported Version
AOS-192469 AOS-207381	An Instant AP does not tag voice and video traffic with the WMM values defined in the SSID profile. Instead, the AP uses the default DSCP tags of 48 and 40 for voice and video traffic respectively. This issue is observed in APs running Aruba Instant 8.3.0.0 or later versions.	Aruba Instant 8.6.0.0
AOS-192604 AOS-207381	An Instant AP does not tag voice and video traffic with the WMM values defined in the SSID profile. Instead, the AP uses the default DSCP tags of 48 and 40 for voice and video traffic respectively. This issue is observed in Instant APs running Aruba Instant 8.3.0.0 or later versions.	Aruba Instant 8.6.0.0
AOS-195769 AOS-234168	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	Aruba Instant 8.6.0.0

Table 5: *Known Issues in Instant 8.6.0.22*

Bug ID	Description	Reported Version
	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 Aruba Instant 8.6.0.0 or later versions.	
AOS-197400	An Instant AP fails to switch uplink interfaces during an uplink failover event. This issue occurs when the Instant AP is configured with two Ethernet uplinks. This issue is observed in Instant APs running Aruba Instant 8.6.0.1 or later versions.	Aruba Instant 8.6.0.1
AOS-201901	An Instant AP changes all access rules to **deny** when the configuration is restored through the CLI from a Windows TFTP server. This issue occurs when the Windows configuration retrieved from the TFTP server includes newline (\n) and carriage return (\r) characters. This issue is observed in APs running Aruba Instant 8.5.0.0 or later versions.	Aruba Instant 8.5.0.0
AOS-202248 AOS-210095	The Instant AP logs are flooded with **awc: wsc: callback_central** messages. These logs are displayed when the **sapd** module of the AP processes messages from Aruba Central. This issue is observed in Aruba Central-managed APs running Aruba Instant 8.5.0.10 or later versions.	Aruba Instant 8.5.0.10
AOS-203766	An Instant AP fails to commit AirGroup settings configured using the Instant WebUI. This issue occurs under the following conditions: ■ When the number of **AirGroup services** exceeds 16. ■ When the number of **service IDs** exceeds 32. This issue is observed in APs running Aruba Instant 8.6.0.0 or later versions.	Aruba Instant 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 Aruba Instant 8.3.0.0 or later versions.	Aruba Instant 8.3.0.0
AOS-209051	Clients are unable to send traffic when the Instant clusters are configured with L3 mobility. This issue occurs under the following scenarios: ■ The client is connected to a cluster other than the home cluster. ■ The network experiences high latency due to an overload caused by a broadcast storm. This issue is observed in APs running Aruba Instant 8.6.0.4 or later versions.	Aruba Instant 8.6.0.4

Table 5: *Known Issues in Instant 8.6.0.22*

Bug ID	Description	Reported Version
AOS-210440	Administrator authentication fails when accessing the Instant AP through the WebUI. This issue occurs when the administrator password includes special characters such as **"** or **'**. This issue is observed in APs running Aruba Instant 8.6.0.5 or later versions. **Workaround:** Create a different administrator password without special characters.	Aruba Instant 8.6.0.5
AOS-210635	Some 530 Series access points report only a small margin of Rx errors in the AP BSS table. This issue is observed in Aruba Central-managed 530 Series access points running Aruba Instant 8.6.0.4 or later versions.	Aruba Instant 8.6.0.4
AOS-213641 AOS-239097	An Instant AP fails to resolve DNS properly for control and management traffic. This issue occurs under the following scenarios: ▪ After the client switches from cellular modem to Ethernet uplink. ▪ When IPv6 DNS fails in a dual stack network. This issue is observed in APs running Aruba Instant 8.3.0.11 or later versions.	Aruba Instant 8.3.0.11
AOS-215571	An Instant AP recommends an 80 MHz channel in ARM when 80 MHz channels are disabled in the cluster. This blocks the AP from selecting a different channel. This issue is observed in Aruba Central-managed APs running Aruba Instant 8.6.0.5 or later versions.	Aruba Instant 8.6.0.5
AOS-218704 AOS-220857	Some VoIP calls are not sent to the server to be recorded. This issue occurs when: ▪ The server recording the calls is behind the controller. ▪ Some APs in the cluster are rebooted. This issue is observed in APs running Aruba Instant 8.6.0.4 or later versions.	Aruba Instant 8.6.0.4
AOS-218974	iPhone clients running iOS 14 or later versions are unable to connect to SSIDs when a Hotspot 2.0 profile is mapped to it. This issue occurs when a Hotspot 2.0 profile is not configured on the iOS device. This issue is observed in APs running Aruba Instant 8.6.0.4 or later versions. **Workaround:** Configure a Hotspot 2.0 profile in the iOS device.	Aruba Instant 8.6.0.4
AOS-219576	Clients connected to an Instant AP are randomly disconnecting from the network with the reason: **internal only**. Clients rejoin the network immediately after the disconnection. This issue is observed in APs running Aruba Instant 8.6.0.8 or later versions.	Aruba Instant 8.6.0.8
AOS-219592	Clients receive router advertisement packets from VLANs other than their assigned VLAN. This issue is observed in SSIDs configured with Dynamic VLAN assignment. This issue is observed in APs running Aruba Instant 8.6.0.7 or later versions.	Aruba Instant 8.6.0.7
AOS-220890	MPSK-Local SSID is broadcasted as Open SSID in Instant APs when the software version is downgraded to Aruba Instant versions lower than 8.7.0.0. This issue is observed in APs running Aruba Instant 8.6.0.8 or later versions.	Aruba Instant 8.6.0.8

Table 5: *Known Issues in Instant 8.6.0.22*

Bug ID	Description	Reported Version
AOS-220896	An Instant AP generates internal system error messages. The output of the **show log system** command displays: **An internal system error has occurred at file rc_acct_instant.c function clear_client_stats_ by_mac line 238**. This issue is observed in APs running Aruba Instant 8.6.0.7 or later versions.	Aruba Instant 8.6.0.7
AOS-220990	An Instant AP fails to download firmware when a destination NAT rule for incoming HTTP traffic is applied in the inbound firewall rule and loses connectivity with Aruba Central when the AP reloads after a destination NAT rule for incoming HTTPS traffic is applied in the inbound firewall rule. This issue is observed in Aruba Central-managed Instant APs running Aruba Instant 8.6.0.9 or later versions.	Aruba Instant 8.6.0.9
AOS-224170 AOS-225601	Some member Instant APs in a cluster appear as down in the AirWave UI. This issue is observed in AirWave-managed APs running Aruba Instant 8.6.0.0 or later versions.	Aruba Instant 8.6.0.0
AOS-225567	Clients connected to a member AP disconnect with the deauthentication reason: **Internal only**. Clients reconnect to the Instant APs immediately after disconnection. When this issue occurs the status of clients in the Instant AP is shown as **disconnected**. This issue occurs when a large number of SNMP requests are sent to the Virtual Controller. This issue is observed in APs running Aruba Instant 8.6.0.8 or later versions.	Aruba Instant 8.6.0.8
AOS-225757	An Instant AP displays the AirWave URL in the **Aruba Central server** field in the output of **show debug cloud-server** command despite being managed by Aruba Central. This issue occurs when the AP management is changed to Central from AirWave. This issue is observed in APs running Aruba Instant 8.6.0.11 or later versions.	Aruba Instant 8.6.0.11
AOS-229903	The **Match MAC** information is not displayed in the **Rogue Device Info** page of the AirWave UI. This issue occurs when the Instant AP fails to send the match MAC information to AirWave. This issue is observed in APs running Aruba Instant 8.6.0.4 or later versions.	Aruba Instant 8.6.0.4
AOS-231019 AOS-232063	An Instant AP fails to reconnect after an LTE outage. The output of the **show cell status** command is missing information. This issue is observed in APs running Aruba Instant 8.6.0.16 or later versions.	Aruba Instant 8.7.1.7
AOS-231846	Wired clients connected to an Instant AP are not displayed in the **Clients > Wired** page of the Aruba Central UI. This issue occurs with wired clients whose MAC address end with the characters **FF** (**xx:xx:xx:xx:xx:FF**). This issue is observed in Aruba Central-managed Instant APs running Aruba Instant 8.6.0.16 or later versions.	Aruba Instant 8.6.0.9
AOS-238100 AOS-239419	The eth0 link of an Instant AP appears offline in the AirWave UI. This issue is observed in AirWave-managed APs running Aruba Instant 8.6.0.18 or later versions.	Aruba Instant 8.6.0.18

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 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.

In the Old WebUI

To configure the HTTP proxy settings:

1. Navigate to **System** > **Proxy**. The **Proxy configuration** window is displayed.
2. Enter the HTTP proxy server IP address in the **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, select the **Proxy requires authentication** checkbox.
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 **New** to enter that IP address or domain name of that host in the **Exceptions** section.

In the New WebUI

To configure the HTTP proxy settings:

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**.

In the CLI

To configure the HTTP proxy settings:

```
(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.

In the Old WebUI

To check for a new version on the image server in the cloud:

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.

In the New WebUI

To check for a new version on the image server in the cloud:

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.

In the Old WebUI

To manually check for a new firmware image version and obtain an image file:

1. Navigate to **Maintenance** > **Firmware**.
2. Under **Manual** section, perform the following steps:
   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-344, AP-345, AP-514, AP-515, AP-518, AP-574, AP-575, AP-575EX, AP-577, and AP-577EX	ArubaInstant_Draco_8.6.0.x_xxxx
AP-503H, AP-504, AP-505, AP-505H, AP-565, and AP-567.	ArubaInstant_Gemini_8.6.0.x_xxxx
IAP-314, IAP-315, IAP-324, IAP-325, AP-374, AP-375, AP-377, AP-318, and AP-387	ArubaInstant_Hercules_8.6.0.x_xxxx
IAP-334 and IAP-335	ArubaInstant_Lupus_8.6.0.x_xxxx
AP-534, AP-535, and AP-555	ArubaInstant_Scorpio_8.6.0.x_xxxx
AP-303, AP-303H, 303P Series, IAP-304, IAP-305, AP-365, and AP-367	ArubaInstant_Ursa_8.6.0.x_xxxx
AP-203H, AP-203R, AP-203RP, and IAP-207	ArubaInstant_Vela_8.6.0.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_8.6.0.x_xxxx
      - TFTP - tftp://<IP-address>/<image-file>. For example, tftp://<IP-address>/ArubaInstant_Hercules_8.6.0.x_xxxx
      - FTP - ftp://<IP-address>/<image-file>. For example, ftp://<IP-address>/ArubaInstant_Hercules_8.6.0.x_xxxx
      - FTP - ftp://<user name:password>@<IP-address>/<image-file>. For example, ftp://<aruba:123456>@<IP-address>/ArubaInstant_Hercules_8.6.0.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.

3. Clear the **Reboot all APs after upgrade** check box if required. This check box is selected 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.
4. Click **Upgrade Now** to upgrade the Instant AP to the newer version.

In the New WebUI (Instant 8.4.0.0 or later versions)

To manually check for a new firmware image version and obtain an image file:

1. Navigate to **Maintenance** > **Firmware**.
2. 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-344, AP-345, AP-514, AP-515, AP-518, AP-574, AP-575, AP-575EX, AP-577, and AP-577EX	ArubaInstant_Draco_8.6.0.x_xxxx
AP-503H, AP-504, AP-505, AP-505H, AP-565, and AP-567.	ArubaInstant_Gemini_8.6.0.x_xxxx
IAP-314, IAP-315, IAP-324, IAP-325, AP-374, AP-375, AP-377, AP-318, and AP-387	ArubaInstant_Hercules_8.6.0.x_xxxx
IAP-334 and IAP-335	ArubaInstant_Lupus_8.6.0.x_xxxx
AP-534, AP-535, and AP-555	ArubaInstant_Scorpio_8.6.0.x_xxxx
AP-303, AP-303H, 303P Series, IAP-304, IAP-305, AP-365, and AP-367	ArubaInstant_Ursa_8.6.0.x_xxxx
AP-203H, AP-203R, AP-203RP, and IAP-207	ArubaInstant_Vela_8.6.0.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_8.6.0.x_xxxx
         - TFTP - tftp://<IP-address>/<image-file>. For example, tftp://<IP-address>/ArubaInstant_Hercules_8.6.0.x_xxxx
         - FTP - ftp://<IP-address>/<image-file>. For example, ftp://<IP-address>/ArubaInstant_Hercules_8.6.0.x_xxxx
         - FTP - ftp://<user name:password>@<IP-address>/<image-file>. For example, ftp://<aruba:123456>@<IP-address>/ArubaInstant_Hercules_8.6.0.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

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_8.6.0.x_xxxx
```

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/ArubaInstant_Hercules_
8.6.0.x_xxxx
```

To view the upgrade information:

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

Upgrade from Instant 6.4.x.x-4.2.x.x to Instant 8.6.0.x

Before you upgrade an Instant AP running Instant 6.5.4.0 or earlier versions to Instant 8.6.0.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.