# HPE Aruba Networking Instant Operating System 8.12.0.5 Release Notes

Hewlett Packard Enterprise

**Open Source Code**

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


## Revision History

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 Instant AOS-8 release notes includes the following topics:

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

For the list of terms, refer to the Glossary.

## Related Documents

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

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

## Supported Browsers

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

| Web Browser | Operating System |
|---|---|
| Microsoft Edge (Microsoft Edge 92.0.902.62 and Microsoft EdgeHTML 18.19041) or later | ■ Windows 10 or later<br>■ macOS |
| Firefox 107.0.1 or later | ■ Windows 10 or later<br>■ 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<br>■ macOS |

# Terminology Change

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

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

# Contacting Support

**Table 2:** *Contact Information*

| | |
|---|---|
| Main Site | arubanetworking.hpe.com |
| Support Site | networkingsupport.hpe.com |
| Airheads Social Forums and Knowledge Base | community.arubanetworks.com |
| North American Telephone | 1-800-943-4526 (Toll Free)<br>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<br>Email: aruba-sirt@hpe.com |

# Chapter 2
# What's New

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

# Chapter 3
# Supported Platforms

This section displays the supported platforms in Instant AOS-8.x. The **minimum version supported** column displays the minimum Instant AOS-8.x version that can be run on a platform. The **latest version supported** column displays the newest Instant AOS-8.x version that can be run on a certain device. Patch releases do not affect platform support. For example, a device which **latest supported version** is 8.10.0.x can run on any 8.10.0.x version, such as 8.10.0.2 or 8.10.0.10.

## Access Point Platforms

| Access Points | | | Instant AOS-8 Versions Supported | |
|---|---|---|---|---|
| **AP Family** | **AP Series** | **AP Model** | **Minimum** | **Latest** |
| 6xx | 670 Series | AP-675, AP-675EX, AP-677, AP-677EX, AP-679, AP-679EX | 8.12.0.x | 8.13.0.x |
| | 650 Series | AP-655A, AP-654A | 8.13.0.x | 8.13.0.x |
| | | AP-655 | 8.10.0.x | 8.13.0.x |
| | | AP-654 | 8.11.2.x | 8.13.0.x |
| | 630 Series | AP-635A, AP-634A | 8.13.0.x | 8.13.0.x |
| | | AP-635 | 8.9.0.x | 8.13.0.x |
| | | AP-634 | 8.11.2.x | 8.13.0.x |
| | 610 Series | AP-615 | 8.11.0.x | 8.13.0.x |
| | 600 Series | AP-605H | 8.12.0.x | 8.13.0.x |

| Access Points | | | Instant AOS-8 Versions Supported | |
|---|---|---|---|---|
| **AP Family** | **AP Series** | **AP Model** | **Minimum** | **Latest** |
| 5xx | 580 Series | AP-584, AP-585, AP-585EX, AP-587, AP-587EX | 8.10.0.x | 8.13.0.x |
| | 570 Series | AP-574, AP-575, AP-577 | 8.7.0.x | 8.13.0.x |
| | 560 Series | AP-565, AP-567 | 8.7.1.x | 8.13.0.x |
| | 550 Series | AP-555 | 8.5.0.x | 8.13.0.x |
| | 530 Series | AP-534, AP-535 | 8.5.0.x | 8.13.0.x |
| | 510 Series | AP-518 | 8.7.0.x | 8.13.0.x |
| | | AP-514, AP-515 | 8.4.0.x | 8.13.0.x |
| | 500 Series | AP-504, AP-505 | 8.6.0.x | 8.13.0.x |
| | | AP-505H | 8.7.0.x | 8.13.0.x |
| | | AP-503H | 8.7.1.x | 8.13.0.x |
| | | AP-503 | 8.11.1.x | 8.13.0.x |

| Access Points | | | Instant AOS-8 Versions Supported | |
|---|---|---|---|---|
| **AP Family** | **AP Series** | **AP Model** | **Minimum** | **Latest** |
| 3xx | 380 Series | AP-387 | 8.4.0.x | 8.10.0.x |
| | 370 Series | AP-374, AP-375, AP-377, AP-375EX, AP-377EX, AP-375ATEX | 8.3.0.x | 8.13.0.x |
| | 360 Series | AP-365, AP-367 | 8.3.0.x | 8.13.0.x |
| | 340 Series | AP-344, AP-345 | 8.3.0.x | 8.10.0.x |
| | 330 Series | AP-334, AP-335 | 8.1.0.x | 8.10.0.x |
| | 320 Series | AP-324, AP-325 | 8.0.0.x | 8.10.0.x |
| | 310 Series | AP-318 | 8.3.0.x | 8.13.0.x |
| | | AP-314, AP-315 | 8.1.0.x | 8.13.0.x |
| | 300 Series | AP-304, AP-305 | 8.1.0.x | 8.13.0.x |
| | | AP-303H, AP-303HR | 8.2.0.x | 8.13.0.x |
| | | AP-303P | 8.4.0.x | 8.13.0.x |
| | | AP-303 | 8.3.0.x | 8.13.0.x |
| 2xx | 270 Series | AP-274, AP-275, AP-277 | 8.0.0.x | 8.6.0.x |
| | 220 Series | AP-224, AP-225, AP-228 | 8.0.0.x | 8.6.0.x |
| | 210 Series | AP-214, AP-215 | 8.0.0.x | 8.6.0.x |
| | 200 Series | AP-207 | 8.1.0.x | 8.6.0.x |
| | | AP-203H, AP-203R, AP-203RP | 8.2.0.x | 8.10.0.x |

# Chapter 4
# Regulatory Updates

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

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

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

The following DRT file version is part of this release:

- DRT-1.0_92117

# Chapter 5
# Resolved Issues

The following issues are resolved in this release.

**Table 3:** *Resolved Issues in Instant 8.12.0.5*

| Bug ID | Description | Reported Version |
|---|---|---|
| AOS-250092<br>AOS-251675<br>AOS-261384<br>AOS-247174 | WPA3 SAE clients failed to reauthenticate while roaming to a previous AP. This issue occurred since PMK cache lifetime was not set and **11r** functionality was disabled. The fix ensures SAE clients are able to roam as expected by setting a PMK cache lifetime of 8 hours. This issue was observed in AP running Instant AOS-8.10.0.0 or later versions. | Instant AOS-8.10.0.0 |
| AOS-255852 | The Live Packet Capture (LPCAP) feature was not working as expected due to the OpenFlow agent failing to establish a connection with Central over OpenFlow. The fix ensures the feature works as expected. This issue was observed in APs running AOS-8.12.0.3 or later versions | Instant AOS-8.10.0.16 |
| AOS-257921 | Some APs crashed and rebooted unexpectedly. The log files listed the error as **ASSERT((uke)->ua_idx)**. The fix ensures the APs work as expected. This issue was observed in APs running Instant AOS-8.12.0.1 or later versions. | Instant AOS-8.12.0.1 |
| AOS-260223 | A gaming console could not connect to a WPA3 pre-shared key SSID on 600 Series APs. The authentication failed due to a message integrity check failure. This issue occurred due to a timing issue within the station management module. The fix ensures that the timing event does not occur and the gaming console connects as expected. | Instant AOS-8.12.0.0 |
| AOS-260258<br>AOS-260383 | The output of the **show ap monitor ap-list** command did not show information for neighboring 5 GHz BSSIDs. This issue was caused by a hardware monitor buffer ring getting stuck, and it also led to APs crashing with the reason **wal_soc_dev_hw.c:918 Assertion !(panic_mask & WHAL_UMCMN_WBM0_ASSERT_INT_MASK) failed**. The fix ensures APs do not experience these issues. This issue was observed in APs running Instant AOS-8.10.0.0 or later versions. | Instant AOS-8.10.0.0 |
| AOS-260790 | Some issues were seen in the **RF Health** report. This occurred because the average error value in the health report was greater than 100%. The fix ensures that the issues are resolved. This issue was observed in AP-655 access points running Instant AOS-8.10.0.14 or later versions. | Instant AOS-8.10.0.14 |
| AOS-261039 | Some Instant Access Point crashed and rebooted unexpectedly due to a memory overrun in the **AWC** process. The fix applies data validation to ensure access points perform as expected. This issue was observed in access points running Instant AOS-8.10.0.16 or later versions. | Instant AOS-8.10.0.16 |

**Table 3:** *Resolved Issues in Instant 8.12.0.5*

| Bug ID | Description | Reported Version |
|---|---|---|
| AOS-261065 | Some guest clients could not connect to the guest SSID. The issue occurred because the guest clients failed to transition from the pre-authenticated role to post-authentication role. The fix ensures that the guest clients successfully connect to the guest SSID. The issue was observed in AP-505 access points running Instant AOS-8.10.0.12 or later versions. | Instant AOS-8.10.0.12 |
| AOS-261317 | Some APs crashed unexpectedly due to a missing **NULL** check in the authentication library when the MDNS module called the **rc_pack_list** API without providing an authentication secret. The fix ensures APs work as expected. This issue was observed in APs running Instant AOS-8.10.0.14 or later versions. | Instant AOS-8.10.0.14 |
| AOS-261578 | Some APs remained on old channel even after detecting radar. The fix ensures that the APs work as expected. This issue was observed in AP-515 running Instant AOS-8.10.0.14 or later versions. | Instant AOS-8.10.0.14 |
| AOS-261623<br>AOS-261987<br>AOS-261992<br>AOS-262042 | Some AP-555 access points randomly crashed and rebooted. The log files listed the reason for the crash as **Kernel panic - not syncing: Take care of the TARGET ASSERT**. The fix ensures APs work as expected. This issue was observed in APs running Instant AOS-8.10.0.12 or later versions. | Instant AOS-8.10.0.12 |
| AOS-261672 | Some AP-535 access points rebooted unexpectedly. The log file listed the reason for the reboot as **mini_httpd core is generated**. The fix ensures APs work as expected. This issue was observed in APs running Instant AOS-8.12.0.4 or later versions. | Instant AOS-8.12.0.4 |
| AOS-261677 | Hidden SSIDs responded incorrectly to probe requests. The fix ensures the hidden SSIDs do not respond in this scenario. This issue was observed in AP-635 and AP-655access points running Instant AOS-8.12.0.0 or later versions. | Instant AOS-8.12.0.0 |
| AOS-261701 | Some APs managed under a Central template group become preferred Conductors, overwriting the **per-ap-settings** variable. This issue arises from two factors: first, the absence of conditions configured in lowercase and case-sensitive format, which prevents the **per-ap-settings** from being correctly applied to the APs. Second, the APs failing to report the correct configuration when the preferred Conductor is set as a member AP in swarm mode, even though it is successfully pushed in Central. This issue is observed in APs running Instant AOS-8.10.0.14 or later versions. | Instant AOS-8.10.0.14 |
| AOS-262040 | The STM module for some APs crashed unexpectedly. The log files listed the crash signature as **handle_assoc_req**. The fix ensures that the STM module does not crash and that APs work as expected. This issue was observed in APs running Instant AOS-8.10.0.0 or later versions. | Instant AOS-8.12.0.3 |
| AOS-262274 | Some mesh APs display the eth0 interface as **DOWN** in the SNMP server. The fix ensures the APs work as expected. This issue is observed in APs running Instant AOS-8.12.0.5 or later versions. | Instant AOS-8.12.0.2 |
| AOS-262315 | When authentication failed in APs, ClearPass Policy Manager has an option to return a custom message; however, this message was not being displayed. The fix ensures the correct message is displayed. This issue was observed in APs running Instant AOS-8.12.0.0 or later versions. | Instant AOS-8.10.0.0 |

**Table 3:** *Resolved Issues in Instant 8.12.0.5*

| Bug ID | Description | Reported Version |
|---|---|---|
| AOS-262403<br>AOS-261409<br>AOS-261914 | Some clients connected to 500 Series access points experienced latency and performance issues. The fix brings back the latency and performance to the expected level for these clients. This issue was observed in access points running Instant AOS-8.10.0.14 or later versions. | Instant AOS-8.10.0.14 |

# Chapter 6
# Known Issues and Limitations

This chapter describes the known issues observed in this release.

**Table 4:** *Known Issues in Instant 8.12.0.5*

| Bug ID | Description | Reported Version |
|---|---|---|
| AOS-249946 | Some AP-515 access points running Instant AOS-8.10.0.2 or later versions crash unexpectedly. This issue occurs due to a **Segmentation** fault in the **ucm** process. | Instant AOS-8.10.0.2 |
| AOS-250574<br>AOS-252921 | A few AP-655 access points crash and reboot with an alert as **Critical**. The log file lists the reason for the reboot as **Reboot after internal watchdog dump saved**. This issue is observed in APs running Instant AOS-8.10.0.0 or later versions. | Instant AOS-8.10.0.7 |
| AOS-253435 | In some AP-315 and AP-375 access points, clients are able to access torrent sites and other applications despite having ACL entries configured to block such traffic. This issue is observed in access points running Instant AOS-8.6.0.19 or later versions. | Instant AOS-8.6.0.19 |
| AOS-258275 | Blocked traffic is observed in Central in the **Applications > Visibility > Blocked Traffic** page, although no ACLs are configured to block this traffic. This issue is observed in access points running Instant AOS-8.10.0.13 or later versions. | Instant AOS-8.10.0.13 |
| AOS-260232<br>AOS-258711 | In the **show ap monitor rogue-ap <mac>** command output, some APs fail to display a value for **Match MAC**, even though **Match Eth MAC** displays a value. The issue occurs because when dealing with the rogue classification of similar BSSID detection, a null value is assigned to **Match Mac**. This issue is observed in APs running Instant AOS-8.10.0.0 or later versions. | Instant AOS-8.10.0.0 |
| AOS-260983 | AP-655 access points installed on Windows 11 incorrectly display Windows 10 in both the SSH and WebUI. This issue occurs because the DHCP fingerprinting is the same for Windows 10 and Windows 11. The issue is observed in AP-655 access points running Instant AOS-8.10.0.4 or later versions. | Instant AOS-8.10.0.4 |

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

In order for the factory default Instant AP to automatically discover the proxy server, you need to configure the HTTP proxy information in the DHCP server option. The Instant AP will receive the proxy information and store it in a temporary file.

To retrieve the port and the proxy server information, you need to first configure the DHCP **option 60** to **ArubaInstantAP** as shown below:

```
(Instant AP)(config)# ip dhcp <profile_name>
(Instant AP)("IP DHCP profile-name")# option 60 ArubaInstantAP
```

Secondly, use the following command to configure the proxy server:

```
(Instant AP)(config)# proxy server <host> <port> [<username> <password>]
```

Use the text string **option 148 text server=host_ip,port=PORT,username=USERNAME,password=PASSWORD** to retrieve the details of the proxy server.

## Rolling Upgrade on Instant APs with AirWave

Starting from Instant AOS-8.4.0.0, Rolling Upgrade for Instant APs in standalone mode is supported with AirWave. The upgrade is orchestrated through NMS and allows the Instant APs deployed in standalone mode to be sequentially upgraded such that the APs upgrade and reboot one at a time. With Rolling Upgrade, only one AP is affected at a 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, and AP-587EX | Aruba Instant_Scorpio_8.10.0.x_xxxx |
| AP-303, AP-303H, 303P Series, IAP-304, IAP-305, AP-365, and AP-367 | Aruba Instant_Ursa_8.10.0.x_xxxx |
| AP-203H, AP-203R, AP-203RP, and IAP-207 | Aruba Instant_Vela_8.10.0.x_xxxx |

   b. To upgrade firmware using the URL of an image file:
      i. Select the **Image URL** option to obtain an image file from a HTTP, TFTP, or FTP URL.
      ii. Enter the image URL in the **URL** text field. The syntax to enter the URL is as follows:
      - HTTP - http://<IP-address>/<image-file>. For example, http://<IP-address>/ArubaInstant_Hercules_8.10.0.x_xxxx
      - TFTP - tftp://<IP-address>/<image-file>. For example, tftp://<IP-address>/Aruba Instant_Hercules_8.10.0.x_xxxx
      - FTP - ftp://<IP-address>/<image-file>. For example, ftp://<IP-address>/Aruba Instant_Hercules_8.10.0.x_xxxx
      - FTP - ftp://<user name:password>@<IP-address>/<image-file>. For example, ftp://<aruba :123456>@<IP-address>/ArubaInstant_Hercules_8.10.0.x_xxxx


- The FTP server supports both **anonymous** and **username:password** login methods.
- Multiclass Instant APs can be upgraded only in the URL format, not in the local image file format.

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

# Upgrading an Instant AP Image Using CLI

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

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

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

```
(Instant AP)# upgrade-image ftp://192.0.2.7/ArubaInstant_Hercules_8.10.0.x_xxxx
```

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

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

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

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

The following command describes how to view the upgrade information:

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

# Upgrade from Instant 6.4.x.x-4.2.x.x to Instant 8.10.0.x

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

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