Aruba Instant 8.7.1.1

aruba

a Hewlett Packard
Enterprise company

Copyright Information

© Copyright 2020 Hewlett Packard Enterprise Development LP.

Open Source Code

This product includes code licensed under the GNU General Public License, the GNU Lesser General Public License, and/or certain other open source licenses. A complete machine-readable copy of the source code corresponding to such code 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, send a check or money order in the amount of US $10.00 to:

Hewlett Packard Enterprise Company
6280 America Center Drive
San Jose, CA 95002
USA

Contents

Revision History

The following table provides the revision history of this document.

Table 1: *Revision History*

Revision	Change Description
Revision 01	Initial release.

This Aruba Instant release notes includes the following topics:

For the list of terms, refer to the Glossary.

Supported Browsers

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

- Microsoft Internet Explorer 11 on Windows 7 and Windows 8
- Microsoft Edge (Microsoft Edge 38.14393.0.0 and Microsoft EdgeHTML 14.14393) on Windows 10
- Mozilla Firefox 48 or later on Windows 7, Windows 8, Windows 10, and macOS
- Apple Safari 8.0 or later on macOS
- Google Chrome 67 or later on Windows 7, Windows 8, Windows 10, and macOS

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*

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

This chapter describes the features and enhancements introduced in Aruba Instant 8.7.1.1.

Datapath

A new command, **clear datapath dns-id-map**, is introduced to enable deletion of DNS ID mappings in the Instant AP. The command has two new parameters:

Parameter	Description
`all`	Deletes all DNS ID mappings in the Instant AP
`<domain-name>`	Deletes DNS ID mappings linked to the specified domain name.

Executing this command on the master AP in a cluster will remove DNS ID mappings in all slave APs. Whereas, executing the command on a slave AP will only remove mappings in the slave AP.

Supported Instant APs

The following table displays the Instant AP platforms supported in Aruba Instant 8.7.1.0 release.

Table 3: *Supported Instant AP Platforms*

Instant AP Platform	Minimum Required Instant Software Version
■ 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 ■ 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

Table 3: *Supported Instant AP Platforms*

Instant AP Platform	Minimum Required Instant Software Version
■ 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

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 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_78105

This release includes an update to JQuery, which has been upgraded to version 3.5.1 to address **CVE-2020-11022** and **CVE-2020-11023**.

Additionally, the following issues are resolved in this release.

Table 4: *Resolved Issues in Aruba Instant 8.7.1.1*

Bug ID	Description	Reported Version
AOS-196842	Clients connected to a mesh point AP failed to authenticate to a WLAN guest network. This issue occurred in cloud guest networks configured with the authentication type as **Anonymous**. The fix ensures that clients can authenticate to the WLAN guest networks as expected. This issue was observed in Aruba Central managed AP-375 access points running Aruba Instant 8.5.0.5 or later versions.	Aruba Instant 8.5.0.5
AOS-199744	The output of the **show iap table long** command did not display any values under the **BID (Subnet Name)** column, when the command was executed on the controller. This issue was observed in backup controllers when an IAP branch failed over from the primary controller in an IAP-VPN deployment. The fix ensures that the controller works as expected. Upgrade the Controller to ArubaOS 8.7.1.1 to resolve the issue. This issue was observed in IAP-VPN deployments that had in controllers running ArubaOS 8.3.0.0 or later versions.	Aruba Instant 8.5.0.7
AOS-200633	Users were unable to view the Instant webUI in Internet Explorer browser. A **Certificate Invalid** error message was displayed. The fix ensures that the Instant WebUI works as expected in Internet Explorer. This issue was observed in APs running Aruba Instant 8.6.0.5 or later versions.	Aruba Instant 8.7.0.0
AOS-205389	A few APs in an Instant cluster intermittently reported **config checksum** errors. The fix ensures that APs sync configurations from the master AP without any checksum errors. This issue occurred in AirWave managed Instant networks. This issue was observed in APs running Aruba Instant 8.5.0.7 or later versions.	Aruba Instant 8.5.0.7
AOS-205932	Some client devices were disconnected from the network when roaming from one AP to another. This issue occurred when broadcast and multicast traffic for clients was blocked due to Group Transient Key (GTK) sync failure between the neighboring APs. The fix ensures that APs sync GTK successfully and clients can roam without any interruption in connection. This issue was observed in 802.11r enabled APs running Aruba Instant 8.4.0.2 or later versions.	Aruba Instant 8.4.0.2

Table 4: *Resolved Issues in Aruba Instant 8.7.1.1*

Bug ID	Description	Reported Version
AOS-207070	Clients were unable to authenticate into the network using captive portal authentication when it was configured with an external RADIUS server. This issue occurred when the duration of TCP handshake process with the RADIUS server exceeded 400ms due to WAN issues. The fix ensures that clients can connect to networks using captive portal authentication configured with an external RADIUS server as expected. This issue was observed in APs running Aruba Instant 8.5.0.0 or later versions.	Aruba Instant 8.5.0.5
AOS-207415	The access requests for some clients were rejected by the RADIUS server. This issue occurred when the access request sent from the AP to the RADIUS server was missing the **State** attribute. The fix ensures that clients can authenticate with the RADIUS server as expected. This issue was observed in APs running Aruba Instant 8.4.0.0 or later versions.	Aruba Instant 8.4.0.0
AOS-207756	The system status LED of a 340 Series access point showed solid amber instead of solid green when powered with an 802.3at PoE supply. The fix ensures that the AP displays the solid green when powered with 802.3at power supply. This issue was observed in 340 Series access points running Aruba Instant 8.6.0.0 or later versions.	Aruba Instant 8.6.0.4
AOS-207781	An Instant AP learnt wrong IP addresses for certain domain names. The fix ensures that the AP learns the correct IP address. This issue was observed in APs running Aruba Instant 8.5.0.0 or later versions.	Aruba Instant 8.6.0.4
AOS-208681	The Instant webUI gets stuck on the uploading screen during firmware upgrade. This issue occurred when Internet Explorer was used to access the webUI. The fix ensures that the Instant AP webUI responds as expected in Internet Explorer. This issue was observed in access points running Aruba Instant 8.6.0.5 or later versions.	Aruba Instant 8.6.0.5
AOS-208783	Some GUI elements in the new WebUI were not visible when accessed through Internet Explorer. This issue occurred when the system used to access the WebUI had the font download option disabled in the firewall settings. The fix ensures that the new WebUI is rendered as expected. This issue was observed in APs running Aruba Instant 8.6.0.0 or later versions.	Aruba Instant 8.6.0.5
AOS-209148	Clients were unable to reach the splash page for captive portal authentication. This issue occurred when the AP fails to process DNS queries from captive portal clients. The fix ensures that captive portal clients join the network as expected. This issue was observed in 8.6.0.0 or later versions.	Aruba Instant 8.7.0.0
AOS-209707 AOS-210108 AOS-211758	APs in an cluster reported high memory usage and rebooted randomly. The log file lists the reason for reboot as: **Reboot caused by kernel panic: MemLeak**. The fix ensures that the APs work as expected. This issue was observed in APs running Aruba Instant 8.7.0.0 or later versions.	Aruba Instant 8.7.0.0

Table 4: *Resolved Issues in Aruba Instant 8.7.1.1*

Bug ID	Description	Reported Version
AOS-209855 AOS-210214 AOS-211809 AOS-214704 AOS-212823 AOS-212590	An Instant AP crashed and rebooted unexpectedly. The log file lists the reason for the event as **Kernel panic - not syncing: Fatal exception in interrupt**. The fix ensures that the AP works as expected. This issue is observed in APs running Aruba Instant 8.7.0.0 or later versions.	Aruba Instant 8.7.0.0
AOS-210141	An Instant AP sent RADIUS accounting messages with incorrect IP information. This issue occurred when the client moved from one user role to another after connecting to the network. The fix ensures that the AP sends the correct IP information in RADIUS accounting messages. This issue was observed in APs running Aruba Instant 8.6.0.2 or later versions.	Aruba Instant 8.6.0.2
AOS-210224	Two member APs in a cluster broadcasted on the same channel when other free channels were available. The fix ensures that the member APs broadcast on different channels as expected. This issue was observed in APs running Aruba Instant 8.5.0.6 or later versions.	Aruba Instant 8.5.0.5
AOS-210855	The master AP in an Instant cluster randomly encountered a CLI core crash and reset the **Age** for APs in the output of **show aps** command. The fix ensures that the AP works as expected. This issue was observed in APs running Aruba Instant 8.5.0.0 or later versions.	Aruba Instant 8.6.0.5
AOS-211394	An Instant AP dropped clients and did not allow new clients to join the network. During this period the AP reported a high memory usage warning in Aruba Central. This issue occurred when **ARP Poison Check** and **Deny Intra VLAN Traffic** was enabled in the AP. The fix ensures that the AP works as expected. This issue was observed in Aruba Central managed Instant APs running Aruba Instant 8.6.0.6 or later versions.	Aruba Instant 8.6.0.6
AOS-211407	Clients connected to an Instant AP were unable to send and receive traffic. This issue was observed in networks configured with **Deny intra VLAN traffic** and the client IP assignment was set to **Virtual Controller managed**. This issue occurred after a Master AP failover event in the Instant cluster. The fix ensures that clients can send and receive traffic in Instant AP clusters as expected. This issue was observed in APs running Aruba Instant 8.6.0.4 or later versions.	Aruba Instant 8.6.0.4
AOS-212652	An Instant AP inherits the gateway IP of the layer 2 switch in the event of a switch outage and causes an IP address conflict when the switch is back online. The fix ensures that the AP does not inherit the gateway IP of the layer 2 switch in the event of a switch outage. This issue was observed in APs running Aruba Instant 8.5.0.5 or later versions.	Aruba Instant 8.5.0.5

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

Limitations

This section describes the limitations in Aruba Instant 8.7.1.1.

AP Hostname Character Limit Extension

The number of ASCII characters allowed in the Instant AP hostname is increased from 32 to 128 characters. The following configuration settings do not support the new limit of 128 ASCII characters in Instant 8.7.1.1:

- The AP Name field in Role Derivation or VLAN Derivation.
- The AP Name field in beacon and probe response frames.
- The AP Name field in the **show ap mesh link** and **ap mesh neighbor** commands.

Unified Communications Manager

UCM does not prioritize NAT traffic.

Known Issues

Following are the known issues observed in this release.

Table 5: *Known Issues in Aruba Instant 8.7.1.1*

Bug ID	Description	Reported Version
AOS-181197 AOS-208313	A 303H Series access point crashes due to kernel panic and reboots. This issue occurs when the AP uses a 3G/4G modem for uplink connection. This issue is observed in 303H Series access points running Aruba Instant 8.4.0.0 or later versions.	Aruba Instant 8.4.0.0
AOS-190757	An Instant AP fails to classify YouTube UDP traffic as **webcategory Streaming-media** and allows users access to YouTube when **webcategory Streaming-Media** is denied by an access rule. This issue is observed in APs running Aruba Instant 8.5.0.1 or later versions.	Aruba Instant 8.6.0.0
AOS-192604	Traffic between clients within the same subnet VLAN is subject to source NAT. This issue occurs because the master AP performs source NAT on local traffic. This issue is observed in APs running Aruba Instant 8.6.0.0 or later versions.	Aruba Instant 8.6.0.0
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 APs running Aruba Instant 8.6.0.1 or later versions.	Aruba Instant 8.6.0.1
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 Central. This issue is observed in Central-managed APs running Aruba Instant 8.5.0.10 or later versions.	Aruba Instant 8.5.0.10
AOS-203279	An AP-565 access point crashes and fails to reboot when software version prior to Aruba Instant 8.7.1.0 is installed. This issue is observed when a software version prior to Aruba Instant 8.7.1.0 is installed on AP-565 access points.	Aruba Instant 8.7.1.0
AOS-203311	An AP-565 access point reboots and disables FIPS mode. This issue is observed in AP-565 access points running Aruba Instant 8.7.1.0 or later versions.	Aruba Instant 8.7.1.0
AOS-204171	Clients intermittently experience high latency when the AP is connected to the backup controller after a failover event. This issue occurs under the following scenarios: ■ The AP attempts to re-connect 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-206840 AOS-209687	The checksum ID and radio information of an AP is not updated on the Virtual Controller. This issue occurs in APs that are configured with a static channel. This issue is observed in 300 Series, AP-315, 320 Series, 330 Series, 360 Series, and 370 Series access points running Aruba Instant 8.4.0.6 or later versions.	Aruba Instant 8.4.0.6

Table 5: *Known Issues in Aruba Instant 8.7.1.1*

Bug ID	Description	Reported Version
AOS-207602	An Instant AP fails to complete 802.1X authentication when **Validate server** option is selected in **Configuration > System > Show advanced options> Uplink > AP1X** section. The debug log lists the reason for failure as: **Server validation failed.** This issue is observed in 200 Series access points running Aruba Instant 8.6.0.4 or later versions.	Aruba Instant 8.6.0.4
AOS-208450	An AP-503H access point operating as a mesh point sends incorrect source MAC address in LLDP messages. This issue is observed in AP-503H access points running Aruba Instant 8.7.1.0 or later versions.	Aruba Instant 8.7.1.0
AOS-208474	An Instant AP frequently disconnects itself from the cluster and then rejoins it. The log file lists the reason for the event as: **stm	PAPI_Send failed, send_papi_message_with_args, 1215: Resource temporarily unavailable**. This issue is observed in APs running Aruba Instant 8.6.0.5 or later versions.	Aruba Instant 8.6.0.5
AOS-208648	The system log of an Instant AP has a lot of **Swarm quit factory default status by : ssid_config** messages. This issue is observed in APs running Aruba Instant 8.7.0.0 or later versions.	Aruba Instant 8.7.0.0
AOS-208969	An AP-503H access point experiences high volume of radio resets which affects the quality of the network. This issue is observed in AP-503H access points running Aruba Instant 8.7.1.0 or later versions.	Aruba Instant 8.7.1.0
AOS-209002	An AP-503H access point denies re-association requests and sends the message **Denied; MFP - Try Later** to clients reconnecting to the network. This issue is observed in AP-503H access points running Aruba Instant 8.7.1.0.	Aruba Instant 8.7.1.0
AOS-209051	Clients are unable to send and receive 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
AOS-210290	An Instant AP fails to update the service ID of AirGroup services when the service ID is configured through the Instant WebUI and Central. This issue occurs when the name of the service ID contains a "**.**" character. This issue is observed in APs running Aruba Instant 8.7.0.0 or later versions.	Aruba Instant 8.7.0.0
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 an administrator password without special characters.	Aruba Instant 8.6.0.5

Table 5: *Known Issues in Aruba Instant 8.7.1.1*

Bug ID	Description	Reported Version
AOS-210717 AOS-212956	The **Client-view heatmap** window in **Dashboard > Clients** page of the Instant WebUI does not display any data. This issue occurs when the number of client match history record exceeds 300. This issue is observed in APs running Aruba Instant 8.7.0.0 or later versions.	Aruba Instant 8.7.0.0
AOS-211665	An Instant AP is unable to connect to Central using a proxy server. The output of **show ap debug cloud-server** command lists the reason as **HTTPS proxy error**. This issue occurs when FreeProxy is used as the proxy server. This issue is observed in APs running Aruba Instant 8.5.0.7 or later versions.	Aruba Instant 8.5.0.7
AOS-212238	An Instant AP fails to update **device-owner** and **shared-user-list** attributes sent from the ClearPass Policy Manager server in the AirGroup CPPM entries table. This issue is observed in APs running 8.7.0.0 or later versions.	Aruba Instant 8.7.1.0
AOS-213257	An Instant AP fails to remove the domain name suffix when logging username entries in the AirGroup users table. This issue occurs when **Enforce ClearPass registration** is enabled in the **Configuration > Services > Airgroup** section. This issue is observed in APs running Aruba Instant 8.3.0.0 or later versions.	Aruba Instant 8.3.0.0
AOS-213941	An Instant AP stops broadcasting and reboots unexpectedly. The log file lists the reason for reboot as: **Reboot due to trigger the cooldown event**. This issue is observed in APs running Aruba Instant 8.7.1.0 or later versions.	Aruba Instant 8.7.1.0
AOS-214199	An Instant AP fails to establish an SSL connection with OpenDNS servers. This issue occurs due to an incompatibility with the **content-header** message sent by the OpenDNS server. This issue is observed in APs running Aruba Instant 8.5.0.11 or later versions.	Aruba Instant 8.5.0.11

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

> **NOTE:** 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.

> **NOTE:** 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.

NOTE

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

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:
- Select the **Image file** option. This method is only available for single-class Instant APs.

    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_8.7.1.x_xxxx
AP-504, AP-505, 500H Series, and 560 Series	ArubaInstant_Gemini_8.7.1.x_xxxx
IAP-314, IAP-315, IAP-324, IAP-325, AP-374, AP-375, AP-377, AP-318, and AP-387	ArubaInstant_Hercules_8.7.1.x_xxxx
IAP-334 and IAP-335	ArubaInstant_Lupus_8.7.1.x_xxxx
AP-534, AP-535, and AP-555	ArubaInstant_Scorpio_8.7.1.x_xxxx
AP-303, AP-303H, 303P Series, IAP-304, IAP-305, AP-365, and AP-367	ArubaInstant_Ursa_8.7.1.x_xxxx
AP-203H, AP-203R, AP-203RP, and IAP-207	ArubaInstant_Vela_8.7.1.x_xxxx

- Select the **Image URL** option. Select this option to obtain an image file from a HTTP, TFTP, or FTP URL.
  - HTTP - http://<IP-address>/<image-file>. For example, http://<IP-address>/ArubaInstant_Hercules_8.7.1.x_xxxx
  - TFTP - tftp://<IP-address>/<image-file>. For example, tftp://<IP-address>/ArubaInstant_Hercules_8.7.1.x_xxxx
  - FTP - ftp://<IP-address>/<image-file>. For example, ftp://<IP-address>/ArubaInstant_Hercules_8.7.1.x_xxxx

- FTP - ftp://<user name:password>@<IP-address>/<image-file>. For example, ftp://<aruba:123456>@<IP-address>/ArubaInstant_Hercules_8.7.1.x_xxxx

NOTE	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. Under **Manual** section, perform the following steps:

- Select the **Image file** option. This method is only available for single-class Instant APs.

    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_8.7.1.x_xxxx
AP-504, AP-505, 500H Series, and 560 Series	ArubaInstant_Gemini_8.7.1.x_xxxx
IAP-314, IAP-315, IAP-324, IAP-325, AP-374, AP-375, AP-377, AP-318, and AP-387	ArubaInstant_Hercules_8.7.1.x_xxxx
IAP-334 and IAP-335	ArubaInstant_Lupus_8.7.1.x_xxxx
AP-534, AP-535, and AP-555	ArubaInstant_Scorpio_8.7.1.x_xxxx
AP-303, AP-303H, 303P Series, IAP-304, IAP-305, AP-365, and AP-367	ArubaInstant_Ursa_8.7.1.x_xxxx
AP-203H, AP-203R, AP-203RP, and IAP-207	ArubaInstant_Vela_8.7.1.x_xxxx

- Select the **Image URL** option. Select this option to obtain an image file from a HTTP, TFTP, or FTP URL.

    - HTTP - http://<IP-address>/<image-file>. For example, http://<IP-address>/ArubaInstant_Hercules_8.7.1.x_xxxx

- TFTP - tftp://<IP-address>/<image-file>. For example, tftp://<IP-address>/ArubaInstant_Hercules_8.7.1.x_xxxx
- FTP - ftp://<IP-address>/<image-file>. For example, ftp://<IP-address>/ArubaInstant_Hercules_8.7.1.x_xxxx
- FTP - ftp://<user name:password>@<IP-address>/<image-file>. For example, ftp://<aruba:123456>@<IP-address>/ArubaInstant_Hercules_8.7.1.x_xxxx

NOTE	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. 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.
4. Click **Upgrade Now** to upgrade the Instant AP to the newer version.
5. 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_8.7.1.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_8.7.1.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 8.7.1.x

Before you upgrade an Instant AP running Instant 6.5.4.0 or earlier versions to Instant 8.7.1.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 support.arubanetworks.com.

3. Verify the affected serial numbers of the Instant AP units.