

# Aruba Instant 6.1.3.1-3.0.0.1

## Release Notes

Aruba Instant 6.1.3.1-3.0.0.1 is a patch software release that introduces fixes to many previously outstanding issues. For details on all of the features described in the following sections, see the *Aruba Instant 6.1.3.1-3.0.0.0 User Guide*.

### In Previous Aruba Instant 6.1.3.1-3.0.0.0 Release

The following new features were added in the previous Aruba Instant 6.1.3.1-3.0.0.0 Release.

### What's New in this Release

This section provides a brief summary of the new features included in this release of Aruba Instant.

#### New Platforms

The following table lists the new Instant devices supported by Aruba:

**Table 1** *New Platforms*

Part Number	Description
IAP-104	Aruba Instant IAP-104 Wireless Access Point. Unrestricted Regulatory Domain. These products should be considered as 'Rest of World' products and <b>must not</b> be used for deployments in the United States, Japan or Israel.
IAP-104-US/JP	Aruba Instant IAP-104 Wireless Access Point. Restricted Regulatory Domain - US/JP
IAP-175P	Aruba Instant AP-175P, 802.11n dual 2x2 320mW; POE
IAP-175P-US/JP	Aruba Instant IAP-175P, 802.11n dual 2x2 320mW; POE. Restricted Regulatory Domain - US/JP
IAP-175AC	Aruba Instant IAP-175AC Outdoor Access Point, 802.11n 2x2 dual radio 320mW; AC powered (with PSE)
IAP-175AC-US/JP	Aruba Instant IAP-175AC Outdoor Access Point, 802.11n 2x2 dual radio 320mW; AC powered (with PSE). Restricted Regulatory Domain - US/JP
RAP-3WN	Aruba RAP-3WN Wireless Access Point. Unrestricted Regulatory Domain. These products should be considered as 'Rest of World' products and <b>must not</b> be used for deployments in the United States, Japan or Israel.
RAP-3WN-US/IL/JP	Aruba RAP-3WN Wireless Access Point with POE support. Restricted Regulatory Domain - US/IL/JP
RAP-3WNP	Aruba RAP-3WNP Wireless Access Point with POE support. Unrestricted Regulatory Domain. These products should be considered as 'Rest of World' products and <b>must not</b> be used for deployments in the United States, Japan or Israel
RAP-3WNP-US/IL/JP	Aruba RAP-3WNP Wireless Access Point with POE support. Restricted Regulatory Domain - US/IL/JP



---

IAP-104, IAP-175, and RAP-3WN will be available in a future price list.

---

## Multiclass Upgrade using AirWave and Cloud Server

Aruba Instant supports mixed AP class deployment with IAP-92/93, IAP-104, IAP-105, IAP-175P/175AC, RAP-3WN/3WNP, and IAP-134/135 as part of the same Virtual Controller cluster.

**Table 2** Instant Image File format

AP Type	Supported Instant Version	Image Name
RAP-3WN/3WNP	6.1.2.3-2.0.0.0 or later	ArubaInstant_Orion_6.1.2.3-2.0.0.0_xxxxx
IAP-104		
IAP-175P/175AC		
IAP-92/93		
IAP-105	6.1.2.3-2.0.0.0 or later	ArubaInstant_Cassiopeia_6.1.2.3-2.0.0.0_xxxxx
IAP-134/135		



---

Multiclass AP feature does not support IAP upgrade using a local image file. You can use an AirWave server or the cloud image server to upgrade a multiclass Instant AP.

---

## Upgrade using Image Server

The Automatic Image Check in the WebUI allows Instant APs in a Virtual Controller cluster to discover new software image versions on a cloud-based image server hosted by Aruba Networks. See the *Aruba Instant 6.1.3.1-3.0.0.0 User Guide* for more information.

## Upgrade using Airwave

If the multi-class IAP network is managed by AirWave, then image upgrades can only be done through the AirWave UI. Users must upload IAP images for both classes on the AMP server. When new IAPs joining the network need to synchronize its software with that of the virtual controller, and that the new IAP is of a different class, the image file for the new IAP will be provided by airwave. If the AMP does not have the proper image file, the new AP will not be able to join the network. See the *Aruba Instant 6.1.3.1-3.0.0.0 User Guide* for more information.

## Improved Network Scalability

The AP limits on IAP-104, IAP-105, IAP-134, IAP-135, and IAP-175 have been removed. IAP -92/93 continues to support 16 IAPs.

## IAP to ArubaOS AP Conversion

An Instant AP can now be provisioned as a Campus AP (CAP) or a Remote AP (RAP) in a controller-based network. Use the **Maintenance > Convert** tab in the Instant WebUI and enter the IP address of the mobility controller to convert the IAP to work in RAP mode.



---

An IAP can be converted to an ArubaOS Campus AP only if the controller is running ArubaOS 6.1 or later and to an ArubaOS Remote AP only if the controller is running ArubaOS 6.1.4 or later.

---

The following steps describe the RAP conversion process:

1. The user points the IAP to a physical controller (local or remote)
2. The IAP automatically downloads the RAP image
3. The IAP reboots itself and comes up as a RAP

After conversion, the Instant AP will be managed by the Aruba mobility controller which has been specified in the Instant WebUI. See the *Aruba RAP-3WN Installation Guide* for more information.



---

In order for the RAP conversion to work, ensure that you configure the Instant AP in the controller white-list and enable the FTP service on the controller.

---

## Instant AP Standalone Mode

This feature allows you to deploy an Instant AP as an autonomous AP which is a separate entity from the existing Virtual Controller cluster in the same Layer 2 domain.

## UI-based Backup/Restore Configuration

Instant WebUI supports backup and restore configuration for local backup and restore.

## OpenDNS Integration

Instant now supports OpenDNS business solutions which requires an OpenDNS (<http://www.opendns.com>) account comprising a username and a password.

## Support for Turkish language

Aruba Instant WebUI now supports Turkish language.

## Mesh Portal Enhancement

The mesh portal will now reboot after 5 minutes (instead of 30 seconds) when it loses Ethernet connectivity to a wired network to facilitate troubleshooting.

## Certificate Management using AirWave

You can now manage Instant AP certificates using the Airwave Management server (AMP). To upload a certificate in AirWave, go to **Device Setup > Certificate** and then click **Add** to add a new certificate.

Instant supports the following certificates for EAP authentication:

- CA certificates: PEM or DER formats.
- Server certificates: PEM or PKCS#12 formats, with passphrase (PSK)

## 3G Support

Aruba Instant supports 3G USB modems for the corporate Instant network. The 3G USB modems can be used to extend the connectivity to places where Ethernet uplink is not feasible. With this support, the client traffic can reach the Internet and the corporate network. To use 3G modem, plug it into the USB port of

RAP3 while it is powered OFF and then power ON the RAP3. In most cases, the RAP3 automatically recognizes the modem and configures it. The detected modem type will be displayed under **Settings > Advanced > Uplink** tab. If the modem cannot be detected appropriately then the user has to manually select the country and ISP settings of the modem in the UI. If the modem used does not belong to any of the countries and ISPs available in the UI drop-down list, you can manually set up the modem by entering low-level settings of the modem individually.



---

RAP-3WN and RAP-3WNP, which will be available soon, support 3G.

---

## Uplink Manager

Instant AP now supports Ethernet uplink and 3G uplink. In Instant UI, you can select the preferred uplink using Uplink preference drop down under **Uplink** tab in **Settings**.

## Ethernet Downlink

The downlink ports allow third party devices such as VOIP phones or printers (which support only wired connection) to connect to the wireless network. Additionally, an Access Control List (ACL) can be configured for added security on the ethernet downlink. Only the OpenAuth mechanism is supported for this release.

## Enable/Disable Firewall ALG Configuration

You can now enable or disable SIP, VOCERA, Alcatel NOE, and Cisco Skinny protocols for ALG in Aruba Instant.

## Firewall based Logging

Instant firewall now supports firewall based logging function. The firewall logs on the Instant APs are generated as syslog messages.

## Client Blacklisting

The client blacklisting feature denies connectivity to the blacklisted clients. When a client is blacklisted in a Virtual Controller, the client is not allowed to associate with the Instant AP in the network. If a client is connected to the network when it is blacklisted, a de-authentication message is sent to force the client to disconnect.

The following types of client blacklisting are generated in Instant:

- Manual Blacklisting
- Authentication Failure Blacklisting
- Session Firewall Based Blacklisting

## User VLAN Derivation

Instant now allows you to assign user VLAN through user attributes. When external RADIUS authentication server is used for authentication, the user VLAN can be derived from Vendor Specific Attributes (VSA).

The user VLAN can be derived from the following rules:

- VSA
- VLAN derivation rule
- User role
- SSID Profile

## VPN Features

The next generation of remote APs integrates features of a RAP and an Instant AP into a single Instant AP device.



---

VPN support on IAP will require a future release of ArubaOS on Mobility controller.

---

VPN features are ideal for:

- enterprises with many branches that do not have a dedicated VPN connection to the HQ.
- branch offices that require multiple APs.
- individuals working from home, connecting to the VPN.

This new architecture and form factor seamlessly adds the survivability feature of Instant APs with the VPN connectivity of RAPs — providing corporate connectivity to non-corporates.

The following VPN features are briefly described:

### VPN Configuration

This feature enables you to create a single VPN tunnel from the Virtual Controller to a Aruba mobility controller in your corporate office. Here, the VPN tunnels from the Instant APs terminate on the Aruba mobility controller. The controller solely acts as a VPN end-point and does not supply the Instant AP with any configuration.

### Routing Profile Configuration

Instant can terminate VPN connections on Aruba mobility controllers. The Routing profile defines the corporate subnets which need to be tunneled through the IPSec tunnel.

### DHCP Server Configuration

The Virtual Controller (VC) on an Instant AP enables different DHCP pools (various deployment models) in addition to allocating IP subnets to each branch. The following modes of DHCP server are supported:

- Local Subnet — In this mode, the VC assigns an IP address from a configured subnet and forwards traffic to both **corporate** and **non-corporate** destinations. This is achieved by appropriately translating the network address (NAT) and forwarding the packet through the IPSec tunnel or through the uplink.
- L2 Switching Mode — In this mode, Instant supports the following two types to support L2 switching mode of connection to corporate:
  - Distributed L2: In this mode, the VC assigns an IP address from a configured subnet and forwards traffic to both **corporate** and **non-corporate** destinations. Instant adds the VLAN configured in this subnet to the controller VLAN multicast table enabling the L2 subnet to act as an extension of the VLAN on the controller. Corporate traffic is sent on the IPSec tunnel and non-corporate traffic is sent on the uplink.
  - Centralized L2: In this mode, the VC does not assign an IP address to the client, but the DHCP traffic is directly forwarded to the controller over the IPSec tunnel and gets an IP address from either the controller or a DHCP server behind the controller serving the VLAN of the client. However, Instant AP does forward client traffic in the same way as the **Distributed L2** mode.
- L3 Routing Mode— In this mode, Instant supports L3 routing mode of connection to corporate. VC assigns an IP addresses from the configured subnet and forwards traffic to both **corporate** and **non-corporate** destinations. Instant AP takes care of routing on the subnet and also adds a route on the controller after the VPN tunnel is set up during the registration of the subnet.

## Fixed Issues

This release contains all fixes up to and including those in Aruba Instant 6.1.3.1-3.0.0.0 release. The following issues have been fixed in the Aruba Instant 6.1.3.1-3.0.0.1 patch release.

**Table 3** Fixed Issues for Instant 6.1.3.1-3.0.0.1

Bug ID	Description
67270	The source IP for the radius request was invalid when the AP was booted with the Dynamic Radius Proxy (DRP) enabled. This issue has been fixed.
67450	The issue that the driver message "asap_user_station_add" was displayed in the console when the clients associate to an AP has been fixed.
67770	The Dynamic Radius Proxy (DRP) issue that the Instant UI being inconsistent with the backend has been fixed.
67769	When the administrator created a new SSID profile by selecting the <b>Assign pre-authentication role</b> option in the Instant UI, the configuration was not saved successfully. This issue has been fixed.

The following issues are fixed in the Aruba Instant 6.1.3.1-3.0.0.0 release.

**Table 4** Fixed Issues for Instant 6.1.3.1-3.0.0.0

Bug ID	Description
58940	The Accounting terminations caused by the RFC 3576 disconnect, Admin Reset, Idle Timeout, and Session Timeout in the Instant AP have been fixed.
58938	The Instant AP now sends RADIUS Accounting Start packets on successful authentications.
61375	Intermittent reboot by IAP-105 has been resolved.
61277	The Web UI can now be configured after connecting to AirWave.
61736	The Usage graphs in the Instant WebUI now display current time.
60913	All forms in the WebUI can now be submitted using the keyboard.
64754	The WebUI no longer freezes when the clock is changed in the Instant AP.
65780	You can now include spaces while specifying Admin-DN and Base-DN fields in the LDAP Server window of the WebUI.
62069	Instant now supports passphrases that are 32 characters long while uploading certificates.
63953	Microsoft Vista clients running 6.1.2.3-2.0.0.3 can now receive IP address via DHCP server.

## Known Issues and Limitations

The following are the known issues and limitations for Aruba Instant 6.1.3.1-3.0.0.0 release.

**Table 5** *Known Issues*

Bug ID	Description
65626	IAPs configured with the country codes QA, MA, CO, and GT may not function properly.
67131	The automatic wireless network configuration on windows 7 does not work with static-wep. However the manual wireless network configuration works correctly.
67280	The Instant WebUI redirects all user entries to the <b>Search</b> dialog when you click <b>Upload certificate</b> link before clicking the <b>Users</b> link. This occurs when you create or edit a Guest Network using the internal database. To avoid this issue configure the users before uploading the certificate to the IAP.
—	When you deploy a network with both Ethernet and 3G uplink, do not configure the Ethernet uplink in the 192.168.11.0/24 and 172.16.11.0/24 subnets.

## Contacting Support

**Table 6** *Web Sites and Emails*

Web Site	
• Main Site	<a href="http://www.arubanetworks.com">http://www.arubanetworks.com</a>
• Support Site	<a href="https://support.arubanetworks.com">https://support.arubanetworks.com</a>
• Wireless Security Incident Response Team (WSIRT)	<a href="http://www.arubanetworks.com/support/wsirt.php">http://www.arubanetworks.com/support/wsirt.php</a>
Support Emails	
Americas and APAC	support@arubanetworks.com
EMEA	emea_support@arubanetworks.com
WSIRT Email Please email details of any security problem found in an Aruba product.	wsirt@arubanetworks.com

**Table 7** *Contact Phone Numbers*

Telephone Numbers	
• Aruba Corporate	+1 (408) 227-4500
• FAX	+1 (408) 227-4550
Support	
United States	800-WI-FI-LAN (800-943-4526)
Universal Free Phone Service Number (UIFN): Australia, Canada, China, France, Germany, Hong Kong, Ireland, Israel, Japan, Korea, Singapore, South Africa, Taiwan, and the UK	+800-4WIFI-LAN (+800-49434-526)
All other countries	+1 (408) 754-1200