Aruba Instant 6.1.3.4-3.1.0.0

ARUBA networks

Release Notes

Open Source Code

Certain Aruba products include Open Source software code developed by third parties, including software code subject to the GNU General Public License (GPL), GNU Lesser General Public License (LGPL), or other Open Source Licenses. The Open Source code used can be found at this site:

http://www.arubanetworks.com/open_source

Legal Notice

The use of Aruba Networks, Inc. switching platforms and software, by all individuals or corporations, to terminate other vendors' VPN client devices constitutes complete acceptance of liability by that individual or corporation for this action and indemnifies, in full, Aruba Networks, Inc. from any and all legal actions that might be taken against it with respect to infringement of copyright on behalf of those vendors.

Warranty

This hardware product is protected by the standard Aruba warranty of one year parts/labor. For more information, refer to the ARUBACARE SERVICE AND SUPPORT TERMS AND CONDITIONS.

Altering this device (such as painting it) voids the warranty.

www.arubanetworks.com

1344 Crossman Avenue
Sunnyvale, California 94089

Phone: 408.227.4500
Fax 408.227.4550

Contents

Chapter 1

Release Overview

Aruba Instant 6.1.3.4-3.1.0.0 is a major software release that introduces new features, and lists fixed and known issues pertinent to the Aruba Instant 6.1.3.4-3.1.0.0 release. For details on all of the features described in the following sections, see the *Aruba Instant 6.1.3.4-3.1.0.0 User Guide*.

Chapter Overview

- "New Features and Enhancements" on page 7 describes the new features introduced in this release.
- "Bugs Fixed in this Release" on page 14 describes the issues that have been fixed in this release.
- "New Known Issues and Limitations" on page 16 provides descriptions for outstanding issues in this release.
- "Fixed in 6.1.3.1-3.0.0.2" on page 17 describes the issues that have been previously fixed in the Aruba Instant 6.1.3.1-3.0.0.2 release.

Contacting Support

Main Site	arubanetworks.com
Support Site	support.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 Telephones	arubanetworks.com/support-services/aruba-support-program/contact-support/
Software Licensing Site	licensing.arubanetworks.com/login.php
Wireless Security Incident Response Team (WSIRT)	arubanetworks.com/support/wsirt.php
Support Email Addresses	
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

Web Site Support	
Main Website	dell.com
Support Website	support.dell.com
Documentation Website	support.dell.com/manuals

This chapter provides a list of all the bugs fixed and new known issues identified in this release, as well as a brief summary of the new features included in this version of Aruba Instant.

New Features and Enhancements

4G LTE Modem Support

Instant AP now supports use of 4G USB modems to provide internet backhaul to an Instant network. Previously, Instant only supported 3G modems. 4G USB modems extend client connectivity to places where an Ethernet uplink is not feasible. This feature enables RAP-3 to automatically choose a network that is available in an area. 4G takes precedence over 3G when RAP-3 tries to auto-select the network.

The 3G and 4G USB modems can be provisioned only on RAP-3.

This release of Instant supports only the Pantech UML 290 4G card.

To use a UML290 4G modem:

1. Power off the RAP-3.
2. Plug the 4G modem into the USB port of the RAP-3.
3. Power on the RAP-3.

The RAP-3 is designed to automatically recognize the UML290 4G modem. Once recognized, the modem appears under **Settings > Advanced > Uplink** tab. In cases where the modem is not recognized, the modem can be manually configured by selecting the country and ISP settings in the Instant WebUI. If the modem used does not belong to any of the countries and ISPs available in the UI drop-down list, you can manually configure the modem by entering low-level settings of the modem individually, under **Settings > Advanced > Uplink > 3G/4G** tab in the Instant WebUI.

Mobility Access Switch (MAS) Integration

With this release, the Instant AP can be integrated with a MAS by plugging the Instant AP directly to the MAS port.To enable this integration, go to **Settings > General** and select **Enabled** in the Instant WebUI.

For more information on MAS, see the ***ArubaOS 7.1.3 User Guide***.

The two major MAS integration features are as follows:

PoE Prioritization - When an Instant AP is plugged directly into the MAS port, the MAS should increase the PoE priority of the port. This is done only if the PoE priority is set by default in the MAS.

Rogue AP Containment - When a rogue AP is detected by Instant, it sends the MAC Address of the rogue AP to the MAS. The MAS blacklists the MAC address of the rogue AP and turns off the PoE on the port.

NOTE

The PoE Prioritization and Rogue AP Containment features will be available for ArubaOS 7.2 release on **Aruba's Mobility Access Switches**.

GRE Tunnel Enhancements

A new parameter, **Per-AP tunnel** is now available while configuring the GRE tunnel. The IAPs can create GRE tunnels from all the APs instead of creating only from the AP that is acting as the virtual controller. The traffic going to the corporate is send via the L2 GRE tunnel from the AP itself and does not have to be forwarded through the virtual controller. A new parameter, **GRE type** is now available to enable a configurable GRE protocol type.

NOTE

By default, the **Per-AP tunnel** option is disabled in the Instant WebUI.

To configure the **GRE type** parameter, go to **VPN > Tunneling > Controller**, select **GRE** from the **Protocol** drop-down list, and enter the value for GRE type in the **GRE type** text box.

To enable the **Per-AP tunnel** parameter, go to **VPN > Tunneling > Controller** and select **Enabled** from the **Per-AP tunnel** drop-down list.

Disable Provisioning SSID

Instant now allows you to disable the instant provisioning SSID. This SSID is enabled by default, and can only be disabled or reenabled through an AP console connection. Use the `factory_reset` command to reset an IAP to its factory-default settings, and then use the `setenv disable_prov_ssid 1` and `saveenv` commands to disable the provisioning SSID. To enable the provisioning SSID, use the `factory_reset` command.

DHCP Based Role Derivation

Instant now allows you to assign user roles based on attributes communicated in the DHCP exchange or 802.1X authentication types. The newly added attributes are:

- DHCP-Option
- 802.1X-Authentication-Type

Video Dynamic Multicast Optimization (DMO)

Instant now supports Dynamic Multicast Optimization for video. With DMO enabled, the IAP converts multicast traffic into unicast over the wireless link. DMO enhances the quality and reliability of streaming video, while preserving the bandwidth available to non-video clients.

To enable this feature, go to **New WLAN> WLAN Settings > Dynamic multicast optimization**.

For more information on Video DMO, see the Aruba Instant 6.1.3.4-3.1.0.0 User Guide.

Multimedia ALG (Facetime, OCS)

Instant now has the added ability to identify and prioritize voice and video traffic from applications like Microsoft Office Communications Server (OCS) and Apple Facetime.

To configure these settings, go to **PEF > Roles > New > Classify media** in the Instant WebUI.

AirWave Primary/Backup

Instant now allows you to define the IP address of a backup AirWave server in the Instant WebUI. The backup server provides connectivity when the primary server is down. If the IAP cannot send data to the primary server, the virtual controller switches to the backup server automatically.

To configure this feature, go to **Settings > Admin > AirWave** in the Instant WebUI.

Deny Inter User Bridging and Deny Local Routing

- **Deny Inter User Bridging**— This feature allows you to deny traffic between two clients which are directly connected to the same IAP or are on the same Instant network.
- **Deny Local Routing**— This feature allows you to deny local routing traffic between clients which are connected to the same IAP or are on the same Instant network.

To enable or disable these features, go to **Settings > General** in the Instant WebUI.

DHCP Relay Agent and Option 82

Instant now includes DHCP Relay Agent and DHCP Option 82 enhancements to the L2 Centralized mode. When a DHCP server is configured with a DHCP Relay agent, the client's Broadcast DHCP Discover packet is not sent to the corporate network, instead the virtual controller acts as the DHCP Relay and unicasts DHCP packets to the corporate DHCP server. Enable DHCP Option 82 to allow clients to send DHCP packets with the Option 82 string.

The Option 82 string is available only in the Alcatel (ALU) format. The ALU format for the Option 82 string consists of the following:

- Remote Circuit ID— AP-MAC; SSID; SSID-Type
- Remote Agent— IDUE-MAC

The Option 82 is specific to Alcatel and is not configurable in this version of Instant.

The following table describes the behavior of the DHCP Relay Agent and Option 82 in the IAP.

Table 1 *DHCP Relay and Option 82*

DHCP Relay	Option 82	Behavior
Enabled	Enabled	DHCP packet relayed with the ALU-specific Option 82 string
Enabled	Disabled	DHCP packet relayed without the ALU-specific Option 82 string
Disabled	Enabled	DHCP packet not relayed, but broadcasted with the ALU-specific Option 82 string
Disabled	Disabled	DHCP packet not relayed, but broadcasted without the ALU-specific Option 82 string

To enable these features, go to **VPN > DHCP Server > New** in the Instant WebUI.

Enhancements to Internal DHCP Server for Clients

For networks using virtual controller IP assignment, the default size of the IP address pool has been increased to 512. You can also customize the DHCP pool's subnet and address range. The largest address pool supported is 2048.

Captive Portal Redirect URL

With this release, users can be redirected to a specific URL (instead of the original URL) after successful captive portal authentication.

To specify the URL, go to **New WLAN > Security > Redirect URL** in the Instant WebUI.

Uplink Switching based on VPN Status

Instant now supports switching uplinks based on the VPN status when deploying mixed uplinks (eth0, 3G, etc). This feature is automatically enabled when a VPN is configured in the IAP.

Image URL Upgrade Support

Aruba Instant now allows you to obtain the image file [(Orion (IAP-105/92/93) and/or Cassiopeia (IAP-134/135)] from a TFTP, FTP and HTTP URL.

To obtain the image file from a TFTP, FTP or HTTP URL, go to **Maintenance > Firmware > Image URL** in the Instant WebUI.

The following examples describe the image file format for two different classes of IAPs:

TFTP:

- URL for IAP-135/134: tftp://10.64.147.8/ArubaInstant_Cassiopeia_6.1.3.4-3.1.0.0_xxxx
- URL for IAP-105/92/93: tftp://10.64.147.8/ArubaInstant_Orion_6.1.3.4-3.1.0.0_xxxx

FTP:

- ftp://10.64.147.8/ArubaInstant_Cassiopeia_6.1.3.4-3.1.0.0_xxxx
- ftp://10.64.147.8/ArubaInstant_Orion_6.1.3.4-3.1.0.0_xxxx

HTTP:

- http://10.64.160.42/ArubaInstant_Cassiopeia_6.1.3.4-3.1.0.0_xxxx
- http://10.64.160.42/ArubaInstant_Orion_6.1.3.4-3.1.0.0_xxxx

Wired Bridging on Ethernet 0 of an Instant AP

Instant now supports wired bridging on the Ethernet 0 port of an Instant AP. Enabling wired bridging on this port of the IAP makes the port available as a downlink wired bridge and allows client access via the port. You can also use the port to connect a wired device when a 3G uplink is used.

To configure this feature, in the Instant WebUI, select the IAP in the **Access Point** window. Click on the **edit** link to open the **Edit Access Point** window. The parameter **Eth0 Bridging** is available in the **Uplink** tab.

Reboot the IAP after the bridging is set for the configuration to take effect.

Uplink Management VLAN

Instant now supports a management VLAN for the uplink traffic on an IAP. After an IAP is provisioned with this parameter, all management traffic sent from the IAP is tagged with the management VLAN.

To configure this feature, in the Instant WebUI, select the IAP in the **Access Point** window. Click the **edit** link to open the **Edit Access Point** window. The parameter **Uplink Management VLAN** is available in the **Uplink** tab.

This configuration requires an IAP reboot to take effect.

Instant AP Wired Authentication

Instant now supports wired authentication on the Ethernet uplink (Ethernet 0) and downlink (Ethernet 1/ Ethernet 2) ports of an Instant AP.

Instant supports the following authentication methods:

- MAC Authentication
- Captive Portal Authentication

To configure wired authentication, click the **Wired** link on the upper right corner of the Instant WebUI, then click on the **Network assignments** drop-down lists to apply an existing Ethernet downlink profile to the Ethernet ports.

Configure bridging on the Ethernet uplink (Ethernet 0) port before you apply a profile.

The devices (SIP phone / printer) connected to the wired ports are now authenticated using the profile that is applied to the port. A list of all the wired users is available in the **Wired** window.

Wired authentication does not support WEP, WPA, and WPA2 encryption.

Captive Portal Localization of the Instant AP

Instant now supports captive portal customization using double-byte characters. Traditional Chinese, Simplified Chinese, and Korean are a few languages that use double-byte characters.

In the Instant WebUI, use the **Networks** window to edit an existing SSID for guest access or click on the **New** link to create a new SSID. In the **Security** tab, select the option **Internal-Authenticated** or **Internal-Acknowledged** for the **Splash page type** to display a preview of the splash page for the captive portal. Click on the banner, term, or policy in the splash page preview to modify the text in the red box. This field accepts double-byte characters or a combination of English and double-byte characters.

Layer-3 Mobility

Layer-3 mobility is now supported on Aruba Instant AP. This allows a client to roam between APs on the same network but different client subnets, while preserving its IP address and existing data sessions.

To configure the L3 mobility settings, go to **Settings > Advanced > L3 Mobility** in the Instant WebUI.

Spectrum Monitor for IAP

Additional modes of operation are now available for an IAP:

- Spectrum Monitor: IAP gathers spectrum data but does not service clients
- Hybrid IAP: The IAP performs spectrum analysis and serves clients

The Instant WebUI allows you to view the spectrum data gathered by an IAP such as device list, channel metrics, and channel details. Alerts are sent to the Virtual Controller when a new non Wi-Fi device is found or when a non Wi-Fi device is deleted from the spectrum data.

You can convert an IAP into a spectrum monitor by performing the following steps:

1. In the Instant WebUI, select the **Access Point** and click **edit**.
2. In the **Radio** tab, select **Spectrum Monitor** from the **Mode** drop-down list.

You can convert the IAPs in an Instant network into hybrid IAPs by performing the following steps:

1. Click the **RF** link at the upper right corner of the WebUI.
2. Click **Show advanced options** to view the **Radio** tab.
3. To enable a spectrum monitor on the 802.11g radio band, in the **2.4 GHz radio** profile, select **Enabled** from the **Background Spectrum Monitoring** drop-down list.
4. To enable a spectrum monitor on the 802.11a radio band, in the **5 GHz radio** profile, select **Enabled** from the **Background Spectrum Monitoring** drop-down list.

The spectrum monitor feature is available only for IAP-104, IAP-105, IAP-134, and IAP-135. The spectrum mode does not work with mesh.

New Options in ACL Configuration

While creating a new ACL rule, in addition to the log and blacklist options, you can now specify the following options in the Instant WebUI:

- Disable scanning: Pause ARM scanning on the IAP when a session is flagged with VoIP. This feature takes effect only if **ARM scanning** is enabled from the **ARM** tab of the **RF** page.
- Classify media: Used to prioritize video and voice traffic. When enabled, deep packet inspection is performed on all non-NATed traffic, and the traffic is marked as follows:
  - Video: Priority 5 (Critical)
  - Voice: Priority 6 (Internetwork Control)
- DSCP tag: Value of the DSCP bits marked in the IP header of a packet matching the rule when it leaves the IAP. This tag is used to prioritize traffic. The supported range is 0-63. The higher the value, the higher the priority.
- 802.1p priority: Value of 802.1p priority bits marked in the frame of a packet matching the rule when it leaves the IAP. The supported range is 0-7. The higher the value, the higher the priority.

Hierarchical Mode of Deployment

An IAP can now be connected to the downlink wired port of another IAP (ethX). The upstream IAP has to be an IAP-130 series device or a RAP-3 (which has more than one wired port). For any single Ethernet port

platform like, IAP-90 or IAP-100 series devices, you can also provision it to use enet0_bridging, so that eth0 is converted to a downlink wired port. For single Ethernet port platform deployments, the root AP must use the 3G uplink.

Number of SSIDs Supported

The number of SSIDs that you can configure in the IAP has increased. IAP-175 and IAP-100 series devices support up to 8 SSIDs. RAP-3, IAP-90 series, and IAP-130 series devices support up to 16 SSIDs.

To configure, go to **Settings > Advanced > General**, and enable **Extended SSID** in the Instant WebUI. Once this option is enabled, the number of SSIDs that are active on each IAP depends on the IAP platform.

This configuration requires an IAP reboot to take effect.

Enabling the Extended SSID option disables the mesh.

PPPoE Support

Instant now supports PPPoE in both normal IAP and VPN-IAP deployments. In this release, PPPoE supports only single IAP deployments.

To configure the PPPoE settings, go to **Settings > Advanced > Uplink** in the Instant WebUI.

This configuration requires an IAP reboot to take effect.

When you use the PPPoE feature do not configure the IP address of the Virtual Controller. Uplink redundancy with the PPPoE link is not supported in this release.

Dynamic Radius Proxy is not supported in a single IAP deployment.

DNS Support for RAP/CAP Conversion

You now have the option to specify a fully qualified domain name of the mobility controller instead of its IP address when converting an IAP to a Campus or Remote AP.

Bugs Fixed in this Release

The following issues have been fixed in the Aruba Instant 6.1.3.4-3.1.0.0. For a list of issues fixed in previous versions of Aruba Instant, see Chapter 3 on page 17.

Captive Portal

Table 2 *Captive Portal Issues Fixed*

Bug ID	Description
64257	The Instant AP (IAP) now does not allow clients using captive portal SSID to access the IAP WebUI before passing authentication.
69528	An issue has been fixed where the IAP unexpectedly rebooted when an external captive portal page opened.
71933, 71908	An issue has been fixed where the users were redirected to an incorrect webpage when clients connected to a Guest network via the external captive portal.

Station Management (STM)

Table 3 *Station Management Issues Fixed*

Bug ID	Description
70474	An issue has been fixed where a captive portal authenticated user who was manually disconnected in the Instant WebUI still appeared in the **Client** tab as an authenticated user.
69190	When 802.1X authentication is configured, the RADIUS authentication request packets now contain the following additional VSA attributes: • Aruba-AP-Group: contains the name of the Virtual Controller • Aruba-Location-Id: contains the name of the Instant AP

SNMP

Table 4 *SNMP Issues Fixed*

Bug ID	Description
69177	The Instant MIB file `aruba-instant.my` is now available as part of the standard Aruba MIB distribution package.

Standalone Mode

Table 5 *Standalone Mode Issues Fixed*

Bug ID	Description
72103	An issue has been fixed where the configuration of an IAP in standalone mode could be affected by another IAP that is not in standalone mode. The IAP then blocked the upstream switch port causing connectivity issues.

Security

Table 6 *Security Issues Fixed*

Bug ID	Description
69446, 72671	An issue has been fixed where clients got access despite failing MAC authentication. This issue was observed on IAPs, running Aruba Instant 6.1.3.1-3.0.0.0, when MAC authentication was configured to authenticate clients and the RADIUS server timed out.
69823, 70915, 70757	An IAP now properly accepts up to 32 Access Control Lists (ACLs) per user role.

Kernel

Table 7 *Kernel Issues Fixed*

Bug ID	Description
70172, 71856, 72217	An issue has been fixed where the IAP continuously crashed and rebooted because an error case was not handled while cleaning up a user session.

Access Point

Table 8 *Access Point Issues Fixed*

Bug ID	Description
70383	An issue has been fixed where iPhones, iPads, and Android tablets could not connect to the Instant network when the **Legacy only** option was enabled in the **RF > Show advanced options > Radio** window. This issue was found in IAP-105 (6.1.2.3-3.0.0.2 version) when the SSID was configured with encryption.
71932, 71822	An issue has been fixed where the IAP-93/105 rebooted due to an "out of memory" condition. This occurred when multiple clients connect to a Guest network.

WebUI

Table 9 *WebUI Issues Fixed*

Bug ID	Description
70776	A security issue in IAP-105 when the Instant WebUI was using SSLv2 authentication on port 443 (TCP) has been fixed. This fix disables SSLv2 authentication on the port and forces the SSLv3 and TLS 1.0 authentications, which are cryptographically stronger.

New Known Issues and Limitations

The following issues and limitations have been identified since the last release.

Access Point

Table 10 *Access Point Known Issues and Limitations*

Bug ID	Description
64338	If two WEP-encrypted SSIDs have more than one BSS sharing the same **Tx key** index value, DHCP offer packets are sometimes dropped, preventing clients from getting an IP address. IAP radios support only four key-cache slots for WEP multicast encryption. When there is an overflow, the last BSS overrides the others and this results in all the other BSS losing the multicast **Tx key**. This issue was observed in IAP-105 (6.1.2.3-2.0.0.3 version).
71953	The country code **ID** is not supported in 802.11a platforms. This issue was seen in IAP-134 and IAP-105 Instant versions 6.1.3.1-3.0.0.0 and 6.1.2.3-2.0.0.0.

Mobility

Table 11 *Mobility Limitation*

Bug ID	Description
70212	The Mobility Trail in the home network of the Instant WebUI does not show foreign IAP information for clients roaming across L3 boundaries.

Security

Table 12 *Security Limitation*

Bug ID	Description
71508	DHCP configured in the Mobile Device Access Control (MDAC) environment does not support the configuration of a captive portal.

Chapter 3

Issues Fixed in Previous 6.1.3.1-3.0.0.2 Release

The following issues have been fixed in this release of 6.1.3.1-3.0.0.2.

Fixed in 6.1.3.1-3.0.0.2

Table 1 *Bugs Fixed in 6.1.3.1-3.0.0.2*

Bug ID	Description
68059	The Instant AP now does not append the domain name suffix to all the DNS queries from the IAP.
68874	The Authentication Server field is no longer required while configuring the Authentication text for the External Captive Portal setting in the Instant WebUI.
69048	An issue has been resolved where IAP clients are not being blacklisted when Instant uses an internal server for authentication.
68299	An issue has been resolved where clients connected to the Guest SSID were able to access the network even though they were denied by the Access Rules.