Aruba Instant 6.3.1.8-4.0.0.7

aruba NETWORKS

Release Notes

Copyright

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. Includes software from Litech Systems Design. The IF-MAP client library copyright 2011 Infoblox, Inc. All rights reserved. This product includes software developed by Lars Fenneberg et al. 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 an Aruba warranty. For more information, refer to the ArubaCare service and support terms and conditions.

Aruba Instant 6.3.1.8-4.0.0.7 is a software patch release that introduces enhancements and fixes to the issues detected in the previous releases of Aruba Instant.

For more information on features described in the following sections, see the *Aruba Instant 6.3.1.1-4.0 User Guide*.

Contents

Contacting

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	http://www.arubanetworks.com/support-services/support-program/contact-support
Software Licensing Site	licensing.arubanetworks.com/login.php
End of Support Information	http://www.arubanetworks.com/support-services/end-of-life-products/end-of-life-policy/
Security Incident Response Team (SIRT)	http://www.arubanetworks.com/support-services/security-bulletins/
Support Email Addresses	
Americas, EMEA, and APAC	support@arubanetworks.com
SIRT Email Please email details of any security problem found in an Aruba product.	sirt@arubanetworks.com

This chapter provides information on the enhancements and issues fixed in this release of Aruba Instant.

Enhancements

The following enhancement is added in this release.

Support for Mexico country code

Starting from 6.3.1.8-4.0.0.7, IAPs support the usage of the Mexico country code.

Resolved Issues in this Release

The following issues are fixed in this patch release.

Authentication

Table 1: *Authentication Fixed Issue*

Bug ID	Description
101378	**Symptom**: IAP sent an accounting stop packet when the client was re-authenticated. This issue is resolved by preventing the IAP from sending any accounting stop packets during L2 re-authentication. **Scenario**: This issue occurred when the client attempted to re-authenticate on the IAP. This issue was not limited to a specific IAP model or Aruba Instant release version.

AirWave

Table 2: *AirWave Fixed Issue*

Bug ID	Description
99252	**Symptom**: Virtual Controller sometimes failed to connect to AirWave. This issue is resolved after making a minor change to the code. **Scenario**: This issue occurred when the Palo Alto Network connectivity failed and caused the AirWave connection to fail as well. This issue was observed in all IAPs running Aruba Instant 6.3.1.1-4.0.0.0 release and later versions.
100687	**Symptom**: Users observed that the client had an incorrect role called "instant" on the AirWave Management Platform. This issue is resolved after making a minor change to the code. **Scenario**: This issue occurred when the user authenticated trap was sent to the AirWave Management Platform with the incorrect role name. This issue was observed in all IAPs running Aruba Instant 6.3.1.1-4.0.0.0 and later versions.

Captive Portal

Table 3: *Captive Portal Fixed Issue*

Bug ID	Description
99229	**Symptom**: IAP cluster was unstable when the filename for the uploaded Captive Portal logo had a space in it. This issue is resolved after making a minor change to the code. **Scenario**: This issue was not limited to a specific IAP model or Aruba Instant release version.

CLI

Table 4: *CLI Fixed Issue*

Bug ID	Description
99828	**Symptom**: IAPs were randomly rebooting in the network after receiving an information update message from a client that was not listed in the IAP database. This issue is resolved by making a minor code change to avoid the IAP from operating on any non-exit client. **Scenario**: This issue was observed in all IAPs running Aruba Instant 6.3.1.1-4.0.0.0 release and later versions.

Datapath/Firewall

Table 5: *Datapath/Firewall Fixed Issue*

Bug ID	Description
100458	**Symptom**: Kernel crashed during L3 roaming. This issue is resolved by making a minor change to the code. **Scenario**: This issue occurred when L3 mobility was enabled on the IAP and the SSID name had a blank character. This issue was observed in all IAP platforms running Aruba Instant 6.3.1.4-4.0.0.6 release.

General

Table 6: *General Fixed Issue*

Bug ID	Description
92338	**Symptom**: IAP was unable to send out Gratuitous ARP after a Slave Virtual Controller became a Master Virtual Controller. This issue is resolved by enabling the IAP to send out Gratuitous ARP on becoming the new Master Virtual Controller. **Scenario**: This issue was observed in all IAPs running Aruba Instant 6.3.1.1-4.0.0.0 release and later versions.

RAP-NG

Table 7: *RAP-NG Fixed Issue*

Bug ID	Description
99497	**Symptom**: L3 clients were unable to reach the VPN tunnel destination when the IAP failed over to the WiFi uplink. The issue is resolved by setting the correct uplink to route the VPN tunnel destination traffic. **Scenario**: This issue occurred when the IAP failed over to the WiFi uplink and used the wrong route-cache entry for the client traffic. This issue was observed in all IAPs running Aruba Instant 6.3.1.4-4.0.0.5 and lower versions.

VPN

Table 8: *VPN Fixed Issue*

Bug ID	Description
100228	**Symptom**: IAPs were unable to communicate with the Syslog server using the **Inner IP address**. This issue is resolved by adding support for Inner IP address on the IAP. **Scenario**: This issue occurred since the IAPs were not supporting communication with the **Inner IP address**. This issue was not limited to a specific IAP model or Aruba Instant release version.

The following issues were fixed in the previous release of Aruba Instant.

Resolved Issues in 6.3.1.4-4.0.0.6

The following issues are fixed in this patch release.

Authentication

Table 9: *Authentication Fixed Issue*

Bug ID	Description
99341	**Symptom**: When the first RADIUS authentication server was down, clients were prompted to enter the username and password twice. This issue is resolved after a minor enhancement was made to prevent multiple authentication requests from being prompted to the client. **Scenario**: This issue was not limited to a specific IAP model or Aruba Instant release version.

Aruba Central

Table 10: *Aruba Central Fixed Issue*

Bug ID	Description
99672	**Symptom**: IAP-105 was unable to come up on Aruba Central without a valid NTP configuration. This issue is resolved by correcting the date in the IAP which preceded the valid start of the certificate from device.arubanetworks.com. **Scenario**: This issue occurred when the IAP was trying to connect to the NTP server and performed an NTP time sync. This issue was observed in all IAPs running Aruba Instant 6.3.1.1-4.0.0.0 release and later versions..

General

Table 11: *General Fixed Issue*

Bug ID	Description
100316	**Symptom**: Executing the **clear-cert server** command did not delete the uploaded server certificate. This issue is resolved by cleaning up the associated certificate file while executing the **clear-cert-server** command. **Scenario**: This issue occurred when the uploaded server certificate switched to cyassl format. This issue was observed in all IAP platforms running Aruba Instant 6.3.1.4-4.0.0.5 release.

Palo Alto Server

Table 12: *Palo Alto Server Fixed Issue*

Bug ID	Description
98604	**Symptom**: When a client connected to a 802.1x SSID, the mac address of the client was displayed in the Palo Alto server. This issue is resolved by using the correct username to sync with the Palo Alto server. **Scenario**: This issue occurred when the number of AirGroup servers exceeded a certain number. This issue was found in IAPs running Aruba Instant 6.3.1.2-4.0.0.2 and later.

RAP-NG

Table 13: *RAP-NG Fixed Issue*

Bug ID	Description
98604	**Symptom**: VPN tunnel goes down during a fail over from the Ethernet uplink to Wi-Fi uplink. This issue is resolved by fixing the incorrect route update that caused the traffic to stop flowing through the VPN tunnel when the uplink failed over from Ethernet to Wi-Fi. **Scenario**: This issue was observed in all IAPs running Aruba Instant 6.3.1.1-4.0.0.0 and later releases.

STM

Table 14: *STM Fixed Issue*

Bug ID	Description
99520	**Symptom**: DHCP timeout alerts were generated by the IAP even after an IP address was delivered to the client from the DHCP server. The fix ensures that the timeout alerts are not generated if an IP address is delivered from the DHCP server. **Scenario**: This issue was not limited to a specific IAP model or Aruba Instant release version.

User Interface

Table 15: *User Interface Fixed Issue*

Bug ID	Description
99863	**Symptom**: Users were unable to rename an IAP from the Graphical User Interface. The fix ensures that the users are able to rename an IAP from the Graphical User Interface. **Scenario**: This issue occurred when management authentication was configured on the IAP. This issue was observed in all IAP platforms running Aruba Instant 6.3.1.4-4.0.0.5 release.

WiFi Driver

Table 16: *WiFi Driver Fixed Issue*

Bug ID	Description
100559	**Symptom**: Wireless Clients were unable to receive Address Resolution Protocol (ARP) broadcast data from the IAP. This issue is resolved by correcting the internal counter in the wireless driver. **Scenario**: This issue occurred when the broadcast filter was not set during heavy downstream traffic. This issue was observed in IAP-225 running Aruba Instant 6.3.1.1-4.0.0.0 release.

Resolved Issues in 6.3.1.4-4.0.0.5

The following issues are fixed in this patch release.

AirGroup

Table 17: *AirGroup Fixed Issue*

Bug ID	Description
97064	**Symptom**: Of all the connected Apple® TVs, only a few of them could be detected randomly by the client devices. To resolve this issue, the size of mDNS packets sent was reduced to match the Maximum Transmission Unit (MTU) size. **Scenario**: This issue occurred when the number of AirGroup servers exceeded a certain number. This issue was found in IAPs running Aruba Instant 6.3.1.2-4.0.0.2 release.

AirWave

Table 18: *AirWave Fixed Issues*

Bug ID	Description
97059	**Symptom**: An IAP stopped communicating with AirWave and was marked as **Down** in the AirWave UI, although the IAP functioned locally. This issue is resolved by introducing a change in the IAP to detect packet loss between the IAP and AirWave, and recover these packets by re-establishing the SSL session. **Scenario**: This issue occurred when certain SSL packets were lost between the IAP and AirWave Management Platform. This issue was not limited to a specific IAP model or Aruba Instant release version.
97087	**Symptom**: When the **AirwaveIP address**, **shared key**, and **organization** configuration details were applied to an IAP from the AirWave management system, the AirWave IP details were not displayed in the CLI. This issue is resolved by clearing the AirWave related configuration received from the DHCP server, before adding the new AirWave configuration information received from AirWave management system, Aruba Central, or the IAP UI. **Scenario**: This issue occurred when the new AirWave IP address received from AirWave Management Platform was the same as the IP address that was previously received from the DHCP server. This issue was found in IAPs running Aruba Instant 6.3.1.2-4.0.0.4.

AP Platform

Table 19: *AP Platform Fixed Issues*

Bug ID	Description
97418	**Symptom**: The Bandwidth graphs did not display any data due to the AP clock corruption. To resolve this issue, some logs are added to record instances of the AP clock being reset. A change is also introduced to either prevent the operation or reboot the AP when the clock is set backward for more than an hour. **Scenario**: This issue occurred when the AP clock was set to an incorrect value. This issue was found across all platforms running Aruba Instant 6.3.1.2-4.0.0.4 or earlier.
98080	**Symptom**: The IAP-22x devices kept sending multicast traffic even though no wireless client was connected to the IAP. This issue is resolved by introducing a change to verify if the clients are connected to the IAP and thus prevent the IAP from sending multicast traffic in air. **Scenario**: This issue occurred when no client was connected to the IAP, or after the clients roamed away from the IAP. This issue was found in IAP-22x devices running Aruba Instant 6.3.1.1-4.0 in a multicast deployment scenario.

AP Provisioning

Table 20: *AP Provisioning Fixed Issue*

Bug ID	Description
96559	**Symptom**: The system log of an IAP displayed the error message, **APAS provision failed, code: fail-prov-no-rule.** This log is no longer displayed if the IAP has an SSID configuration. **Scenario**: When a locally managed IAP boots up, it contacts the Activate server to check if there is a new provisioning rule. If there is no provisioning rule, the error log is displayed. This issue was found in IAPs running Aruba Instant 6.2.1.0-3.4.0.5 or later.

Authentication

Table 21: *Authentication Fixed Issue*

Bug ID	Description
96888	**Symptom**: Some Apple devices could not authenticate. This issue is resolved by setting the default EAP type to **gtc** when EAP termination is enabled and an LDAP server is chosen as the authentication server. **Scenario**: This issue occurred when EAP termination is enabled on the SSID with an LDAP server as the authentication server. This issue was found in IAPs running Aruba Instant 6.3.1.1-4.0 or later.

Captive Portal

Table 22: *Captive Portal Fixed Issues*

Bug ID	Description
97820	**Symptom**: The HTTP 408 error was displayed when the users tried to connect to the external captive portal through Port 80. This issue is resolved by making a configuration change to allow a space in the name of an external captive profile. **Scenario**: This issue occurred when there was a space in the name of an external Captive Portal profile. This issue was found in IAPs running Aruba Instant 6.3.1.1-4.0 or later.
97565	**Symptom**: In an external captive portal network, a user was assigned an exceeded bandwidth, although a role-based bandwidth contract was configured by the administrators. This issue is resolved by introducing a change to apply the configured bandwidth contract to the users, irrespective of the changes in the user role. **Scenario**: This issue occurred when the user role changed from the pre-authenticated role to a captive portal role, after which the configured bandwidth contract was not applied to the user role. This issue was found in IAPs running Aruba Instant 6.3.1.1-4.0 or later.

Datapath

Table 23: *IAP Datapath Fixed Issue*

Bug ID	Description
98434	**Symptom**: An IAP rebooted randomly when the CLI process opened too many files. To resolve this issue, a change is added in the IAP code and a new debug command, **show opened-file <pid>** is introduced. **Scenario**: This issue occurred because the process files were not closed and the open files resulted in a system reboot. This issue was not limited to any specific IAP model and was found in IAPs running Aruba Instant 6.3.1.1-4.0 or later.

Instant UI

Table 24: *Instant UI Fixed Issue*

Bug ID	Description
96766	**Symptom**: The **Continue login** link in the **Login** page was not correctly displayed when the Instant UI was launched from an unsupported browser. The link is now correctly displayed along with the unsupported browser warning message in the UI. **Scenario**: This issue occurred when the users launched the Instant UI through an unsupported browser, for example, IE11. This issue was found in IAPs running Aruba Instant 6.3.1.1-4.0 or later.

SNMP

Table 25: *SNMP Fixed Issue*

Bug ID	Description
97452	**Symptom**: When an SNMP GET operation was performed for the **aiClientUptime** object (OID-1.3.6.1.4.1.14823.2.3.3.1.2.4.1.16), no output was received. The **aiClientUptime** object now returns an appropriate client uptime value. **Scenario**: The issue occurred because the MIB variable could not fetch the required information. This issue was found in IAPs running Aruba Instant 6.2.1.0-3.3 or later.

VLAN Configuration

Table 26: *VLAN Configuration Fixed Issue*

Bug ID	Description
98548	**Symptom**: The **allowed VLAN** configuration settings on Virtual Controller were not replicated on slave IAPs in a cluster. To resolve this issue, execute the **no allow-vlan all** command in the CLI. **Scenario**: This issue occurred when a slave IAP with the **allow-vlan all** configuration joined master IAP. Due to this, the slave IAP configuration was not synchronized. This issue was found in IAPs running Aruba Instant 6.3.1.1-4.0.

Wi-Fi Driver

Table 27: *Wi-Fi Driver Fixed Issue*

Bug ID	Description
93650	**Symptom**: GE Dash devices were not able to access devices on the network when connected an IAP on a WPA-PSK-TKIP SSID. This issue is resolved by introducing a change in the group-key delay timer. **Scenario**: This issue occurred because the group-key delay timer was set to ZERO, which sometimes resulted in group key exchange failure. This issue was found in IAP-135 and IAP-105 devices running Aruba Instant 6.3.1.2-4.0.0.4 or earlier.

Resolved Issues in 6.3.1.2-4.0.0.4

The following issues are fixed in this patch release.

Access Points

Table 28: *Access Points Fixed Issues*

Bug ID	Description
81794	**Symptom**: An IAP-225 crashed when the configuration in flash memory was erased. This issue is resolved by introducing a change in the IAP to handle multi-process flash operation. **Scenario**: This issue occurred when the AP was manually rebooted or powered off during the course of flash operation and was found in IAPs running Aruba Instant 6.2.0.0-3.2.
95534	**Symptom**: Multiple IAPs crashed due to the MDNS process failure. This issue is resolved by introducing a change in the internal code to ignore the counter limit. **Scenario**: This issue occurred when AirGroup was enabled and multiple clients were connected to an IAP. As the counter that tracks the number of current users reached the maximum limit, the MDNS process crashed. This issue was found in IAPs running Aruba Instant 6.3.1.2-4.0.0.2.

Aruba Central

Table 29: *Aruba Central Fixed Issue*

Bug ID	Description
96357	**Symptom**: An IAP-175 could not connect to Aruba Central. This issue is resolved by introducing a change in the signature format used for authentication with Central. **Scenario**: This issue occurred because the signature format used by CyaSSL was not compatible with Central. This issue was found in the IAP-175 device running Aruba Instant 6.3.1.1-4.0.

Authentication

Table 30: *Authentication Fixed Issue*

Bug ID	Description
93690	**Symptom**: The Instant UI displayed the **Authentication Server is down** error message, although there were no authentication issues. To resolve this issue, a change in the IAP is introduced to generate error information only for one server that is down during the dead time. **Scenario**: This issue occurred when an SSID configuration was modified. Due to this, the server dead timer was changed and some server error messages could not be removed from the fault history. This issue was found in IAPs running Aruba Instant 6.2.1.0-3.4.0.3.

Firewall

Table 31: *Firewall Fixed Issue*

Bug ID	Description
95727	**Symptom**: The **show datapath user** command displayed incorrect user details when clients repeatedly roamed and associated to an IAP. The command displays the correct details in the 6.3.1.2-4.0.0.4 release version. **Scenario**: This issue was found in IAP-22x devices running Aruba Instant 6.3.1.2-4.0.0.3.

L2TPv3

Table 32: *L2TPv3 Fixed Issues*

Bug ID	Description
95091	**Symptom**: Sometimes, the L2TP tunnel was deleted due to the blocking or unblocking of L2TPv3 traffic on a Small Office/Home Office (SOHO) router. To resolve this issue, a check is introduced to verify if the retry timer is running and not to trigger another timer if it is already running. **Scenario**: This issue occurred because some SOHO routers do not block L2TPv3 traffic completely from L2TP Network Server (LNS) to L2TP Access Concentrator (LAC). When such packets were received, the same retry timer was triggered, although it was already running. As a result, the tunnel was deleted. This issue was found in IAPs running Aruba Instant 6.3.1.1-4.0.
95923	**Symptom**: When the L2TP tunnel was down, the DNS packets from wireless client were detected at the default gateway of the IAP. This issue is resolved by introducing a change in the IAP to prevent DNS packet routing when the L2TP tunnel is down. **Scenario**: This issue was found in IAPs running Aruba Instant 6.3.1.1-4.0.
96026	**Symptom**: The L2TP session was removed and was not re-established when the tunnel was in retry state and the IAP received a Call Disconnect-Notify (CDN) from the LNS. To resolve this issue, the session delete reason is set to *ALREADY deleted by CDN* to ensure that the session is not removed when the tunnel goes down. **Scenario**: Sometimes, the L2TP session was not re-established due to the blocking or unblocking of L2TP traffic on the LNS server, which resulted in the tunnel retry state. This issue was found in IAPs running Aruba Instant 6.3.1.1-4.0.

RTLS

Table 33: *RTLS Fixed Issue*

Bug ID	Description
95802	**Symptom**: The periodic associated and unassociated station updates were not received by the RTLS server. To resolve this issue, the IAP SAPD is updated to use the IP address string for RTLS communication. **Scenario**: This issue occurred, because the IAP was not updated to consider both DNS and IP address for RTLS communication. This issue was found in IAPs running Aruba Instant 6.3.1.1-4.0.

Security

Table 34: *Security Fixed Issue*

Bug ID	Description
95861	**Symptom**: A security assessment tool reported a few medium level vulnerabilities with a few supported cipher suites on an IAP. To resolve this issue, the unused cipher suites have been removed. **Scenario**: This issue was detected during a scan by a security assessment tool and was found in IAPs running Aruba Instant 6.2.1.0-3.4.0.x.

STM

Table 35: *STM Fixed Issue*

Bug ID	Description
95840	**Symptom**: Due to an issue with the STM process, some clients were not allowed to associate to IAP-225. This issue is resolved by introducing a change that prevents potential loops in the memory allocation library. **Scenario**: This issue was found when the Background spectrum-monitoring and Client-Match features were enabled on an IAP-225 device running Aruba Instant 6.3.1.1-4.0.

Virtual Controller

Table 36: *Virtual Controller Fixed Issue*

Bug ID	Description
89028	**Symptom**: An IAP-225 device rebooted due to master to local transition. This issue is resolved by introducing a change in the IAP to prevent frequent access to the process handle function. **Scenario**: This issue was found in IAPs running Aruba Instant 6.3.1.0-4.0.

Resolved Issues in 6.3.1.2-4.0.0.3

The following issues are fixed in the 6.3.1.2-4.0.0.3 patch release.

Authentication

Table 37: *Authentication Fixed Issues*

Bug ID	Description
94788	**Symptom**: The Instant UI displays an upload successful message when an invalid certificate is uploaded. This issue is resolved by introducing an error check in IAP to verify the validity of certificates. **Scenario**: This issue occurred when an invalid certificate was uploaded through the Instant UI and was found in IAPs running Aruba Instant 6.3.1.1-4.0.0.1.
94787	**Symptom**: The .pem certificate uploaded to the IAP database was not displayed in the output of the **show cert-all** command. This issue is resolved by introducing a change in the IAP to add a new line at the end of the text in the certificate. **Scenario**: This issue occurred because IAPs did not accept the certificates with no end of line. This issue was found in IAPs running Aruba Instant 6.3.1.1-4.0.0.1.

Firewall Configuration

Table 38: *Firewall Configuration Fixed Issues*

Bug ID	Description
94813	**Symptom**: The DSCP mapping value of client traffic was not copied to the outer header during GRE encapsulation. To resolve this issue, a change was introduced to copy the Type of Service (TOS) bit from inner IP to the outer IP. **Scenario**: This issue occurred when DSCP tagging was enabled for client traffic passing through the GRE tunnel to controller. This issue was found in IAPs running Aruba Instant 6.2.1.0-3.4.0.0.
95050	**Symptom**: When the 0.0.0.0 routing profile was defined, the source IP address was translated for the traffic generated by the IAP, even though the traffic was destined to the local subnet of the IAP. This issue is resolved by updating the firewall rules. **Scenario**: This issue occurred when VPN was configured with the 0.0.0.0 routing profile on the IAP and was found in devices running Aruba Instant 6.2.1.0-3.4.0.0.

IAP Configuration

Table 39: *IAP Configuration Fixed Issue*

Bug ID	Description
95022	**Symptom**: The master IAP did not apply system location configuration to the slave IAPs joining the cluster. This issue is resolved by introducing a change in the IAP to apply system location information to slave IAPs from the master IAPs. **Scenario**: This issue occurred when slave IAPs rebooted with configuration changes applied from the master IAP, but without the system location information. This issue was found in IAPs running Aruba Instant 6.2.0.0-3.2 or later releases.

Wi-Fi Driver

Table 40: *Wi-Fi Driver Fixed Issue*

Bug ID	Description
95152	**Symptom**: Although the RF conditions were favorable, the users experienced network latency. This issue is resolved by introducing a change in the IAP code. **Scenario**: This issue occurred when an encrypted SSID was used. This issue was found in IAP-225 devices running Aruba Instant 6.3.1.2-4.0.0.2.

Resolved Issues in 6.3.1.2-4.0.0.2

AirWave

Table 41: *AirWave Fixed Issue*

Bug ID	Description
93909	**Symptom**: The Instant UI allowed double byte characters for the organization string configured for the AirWave management console login. The UI now allows only the ASCII characters in the organization string. **Scenario**: This issue was found in IAPs running Aruba Instant 6.3.1.1-4.0.0.0 or later versions.

ARM

Table 42: *ARM Fixed Issue*

Bug ID	Description
90503	**Symptom**: The radios on an IAP were continuously getting reset. A potential fix has been in implemented in the ARM algorithm to measure the channel quality and switching to better channel in environments when interfering devices are randomly turned on and off. **Scenario**: The issue occurred when interfering devices such as Drive-Thru Headset Systems HME-37R03939 were present in the same channel as that of AP. The AP was not able to detect and change the channel based on the randomly used RF-interfering devices. This issue was found in IAPs running Aruba Instant 6.2.1.0-3.4 or later versions.

Firewall

Table 43: *Firewall Fixed Issue*

Bug ID	Description
94162	**Symptom**: When **Drop bad ARP** was enabled, clients could not reconnect to the network. This issue is resolved by allowing the ARP packets to pass. **Scenario**: This issue occurred when the **Drop bad ARP** option in the **Security**>**Firewall Setting** window was enabled. This issue was found in IAPs running Aruba Instant 6.3.1.1-4.0.0.0 and 6.3.1.1-4.0.0.1.

IDS

Table 44: *IDS Fixed Issue*

Bug ID	Description
93778	**Symptom**: A syslog message was not generated when a rogue AP was detected in the network. The IAPs now generates syslog message (with 106000 as the message ID) when a rogue AP is detected. **Scenario**: This issue was found in IAPs running Aruba Instant 6.3.1.1-4.0.0.1 or earlier versions.

SNMP

Table 45: *SNMP Fixed Issue*

Bug ID	Description
94307	**Symptom**: The ColdStart or WarmStart traps were not generated after an IAP boot or reload. To resolve this issue, upgrade to Aruba Instant 6.3.1.2-4.0.0.2. **Scenario**: This issue was found in IAPs running Aruba Instant 6.3.1.1-4.0.0.0 and 6.3.1.1-4.0.0.1.

Uplink Management

Table 46: *Uplink Management Fixed Issue*

Bug ID	Description
94467	**Symptom**: Users could not configure uplink VLAN through the Instant CLI. To resolve this issue, the procedure for setting or resetting the environment variable was changed. **Scenario**: This issue occurred when a user configured uplink VLAN using the Instant CLI and executed the **commit apply** command, which in turn cleared the individual IAP settings. This issue occurred in IAPs running Aruba Instant 6.3.1.1-4.0.0.1 or earlier versions.

VPN Configuration

Table 47: *VPN Configuration Fixed Issue*

Bug ID	Description
93353	**Symptom**: DHCP renew packets were dropped in a network of single IAP, resulting in the VPN tunnel going down. A change in the firewall rules has fixed this issue. **Scenario**: This issue occurred when VPN switched over in a network with a single IAP. This issue was found in IAPs running Aruba Instant 6.2.1.0-3.4.0.4.

WLAN Configuration

Table 48: *WLAN Configuration Fixed Issue*

Bug ID	Description
93921	**Symptom**: An IAP-93 broadcast the SSID configured in the incorrect band. This issue is resolved by introducing a change to the IAP's internal software. **Scenario**: As IAP-93 supports a single dual band radio, it can only work on 2.4GHz or 5GHz at a time, which is a global configuration. This issue occurred when the SSID configured in the other band was broadcast by IAP-93 in the 2.4 GHz band. This issue was found in IAP-93 devices running Aruba Instant 6.3.1.1.-4.0.0.1 or earlier versions.

Resolved Issues in 6.3.1.1-4.0.0.1

Instant UI

Table 49: *Instant UI Fixed Issue*

Bug ID	Description
93647	**Symptom**: The wired profile could not be created through the Instant UI. A change in the ACL process has fixed this issue. **Scenario:** This issue occurred when the user tried to create a wired profile using the Wired Network wizard in the Instant UI. This issue was found in IAPs running Aruba Instant 6.3.1.1-4.0.0.0.

This chapter provides information on the features and enhancements introduced in the 6.3.1.1-4.0 and 6.3.1.1-4.0.0.x releases of Aruba Instant.

Features and Enhancements

The following features and enhancements were introduced in the 6.3.1.1-4.0.0.0 and later releases.

Support of HTTP Proxy Configuration

If your IAP is deployed in a wired network, which requires an HTTP proxy server to access the internet, you need to configure HTTP proxy on the IAP. After you set up the HTTP proxy settings, the IAP can connect to the Activate server, AirWave Management platform, Central, or OpenDNS server through a secure HTTP connection. You can also configure a list of hosts which do not need proxy by providing their host names or IP address.

You can configure the HTTP Proxy in the Instant UI and CLI. For more information, see:

- *Configuring HTTP Proxy on an IAP* in *Aruba Instant 6.3.1.1-4.0 User Guide*
- The **proxy** command in the *Aruba Instant 6.3.1.1-4.0 CLI Reference Guide*

IAP Provisioning Enhancements

In the Aruba Instant 6.3.1.1-4.0 release, for option DHCP 43, besides the old format **<organization>,<ams-ip>,<ams-key>**, a new format **<organization>,<ams-domain>** is supported. If you use the format **<organization>**,**<ams-ip>**,**<ams-key>**, the Pre-Shared Key (PSK) based authentication is used for accessing the AirWave Management server. If you use the format **<organization>**,**<ams-domain>**, the IAP resolves the domain name into two IP address as AirWave primary, AirWave backup, and then starts a certificate-based authentication with the AirWave Management server, instead of the PSK based login.

You can configure the domain name in the Instant UI and CLI. For more information, see:

- *Configuring AirWave Information and Standard DHCP option 60 and 43 on Windows Server 2008* in *Aruba Instant 6.3.1.1-4.0 User Guide*
- The **ams-ip** and **ams-backup-ip** commands in *Aruba Instant 6.3.1.1-4.0 CLI Reference Guide*

Support for Centralized,L3 DHCP Scope

This release of Aruba Instant supports Centralized L3 DHCP scope to serve L3 clients. When this feature is enabled, the IAP relays all DHCP request packets to the DHCP server and acts as gateway for the centralized DHCP scope serving L3 clients. The **DHCP server** window in the Instant UI allows the configuration of a centralized DHCP scope.

When a centralized DHCP scope is configured:

- The Virtual Controller does not assign an IP address to the client and the DHCP traffic is directly forwarded to the DHCP Server.
- For L2 clients, the Virtual Controller bridges the DHCP traffic to the controller over the VPN/GRE tunnel. The IP address is obtained from the DHCP server behind the controller serving the VLAN/GRE of the client. This DHCP assignment mode also allows you to add the DHCP option 82 to the DHCP traffic forwarded to the controller.
- For L3 clients, the Virtual Controller acts as a DHCP relay agent that forwards the DHCP traffic to the DHCP server located behind the controller in the corporate network and reachable through the IPSec tunnel. The centralized L3 VLAN IP is used as the source IP. The IP address is obtained from the DHCP server.

For more information, see:

- *Configuring a Centralized DHCP Scope* in *Aruba Instant 6.3.1.1-4.0 User Guide*
- The **ip dhcp** command in the *Aruba Instant 6.3.1.1-4.0 CLI Reference Guide*

Support for Automatic Configuration of the GRE Tunnel

In the 6.3.1.1-4.0 release, Instant allows you to enable automatic configuration of the GRE tunnel from an IAP to Aruba Mobility Controller. By using an IPsec connection, the IAPs can now set up a GRE tunnel with the controller. This feature eliminates the need for the manual configuration of tunnel interface on the controller.

For more information, see:

- *Enabling Automatic Configuration of GRE Tunnel* in *Aruba Instant 6.3.1.1-4.0 User Guide*
- The **vpn gre-outside** command in the *Aruba Instant 6.3.1.1-4.0 CLI Reference Guide*

Bandwidth Contract Enhancements

Instant supports assigning bandwidth contracts to the user roles. The administrator can assign a bandwidth contract configured in Kbps to upstream (client to the IAP) or downstream (IAP to clients) traffic for a user role. All clients with this user role assigned, will be part of that bandwidth contract. The administrators can also set per user bandwidth to provide a specific bandwidth for every user.

To support this feature:

- In the Instant UI, the **Access** tab of WLAN wizard and Wired network windows now allow setting a rule for bandwidth contract and allocate the bandwidth for downstream and upstream traffic per user in Kbps. You can also assign bandwidth limit for each SSID user under the **WLAN Settings** tab of the WLAN wizard. For more information, see *Aruba Instant 6.3.1.1-4.0 User Guide*.
- In the Instant CLI, the **wlan access-rule** command is enhanced to include the **bandwidth-limit** configuration command. For more information, see *Aruba Instant 6.3.1.1-4.0 CLI Reference Guide*.

In the earlier releases, bandwidth contract could be assigned per SSID. In the 6.3.1.1-4.0 release, the bandwidth contract can also be assigned per SSID user. If the bandwidth contract is assigned for an SSID in *Aruba Instant* 6.2.1.0-3.4.0.x image and when the IAP is upgraded to 6.3.1.8-4.0.0.7 release version, the bandwidth configuration per SSID will be treated as per-user downstream bandwidth contract for that SSID.

Support for 802.11r Roaming and Fast BSS Transition

In the 6.3.1.1-4.0 release, Instant supports 802.11r roaming standard. As part of the 802.11r implementation, Instant supports the Fast BSS Transition protocol. The Fast BSS Transition mechanism reduces client roaming delay when a client transitions from one BSS to another within the same cluster. This minimizes the time required to resume data connectivity when a BSS transition happens.

Fast BSS Transition is operational only if the wireless client supports 802.11r standard. If the client does not support 802.11r standard, it falls back to the normal WPA2 authentication method.

You can enable 802.11r roaming on WLAN SSID by using the Instant UI (**WLAN Wizard>Security** tab) or CLI (**dot11r** command in the **wlan ssid-profile** command configuration mode). For more information, see *Aruba Instant 6.3.1.1-4.0 User Guide* and *Aruba Instant 6.3.1.1-4.0 CLI Reference Guide*.

Support for Client Roaming Based on Opportunistic Key Caching

Instant also supports opportunistic key caching (OKC) based roaming. In the OKC based roaming, the AP stores a cached pairwise master key (PMK) for each client, which is derived from last 802.1X authentication completed by the client in the network. By default, the 802.1X authentication profile enables a cached PMK, which is used when a client roams to a new AP. The cached PMK is used when a client roams to a new AP. This allows faster roaming of clients between the IAPs in a cluster, without requiring a complete 802.1X authentication.

OKC roaming (when configured in the 802.1X Authentication profile) is supported on WPA2 clients. If the wireless client (the 802.1X supplicant) does not support this feature, a complete 802.1X authentication is required whenever a client roams to a new AP.

You can enable OKC roaming on a WLAN SSID by using the Instant UI (**WLAN Wizard>Security** tab) or CLI (**no okc-disable** command in the **wlan ssid-profile** command configuration mode). For more information, see *Aruba Instant 6.3.1.1-4.0 User Guide* and *Aruba Instant 6.3.1.1-4.0 CLI Reference Guide*.

Link Aggregation Support on IAP-22x

IAP-22x supports the IEEE 802.11ac standard for high-performance WLAN. To support maximum traffic, port aggregation is required to increase throughput and enhance reliability. IAP-22x supports link aggregation using either standard port-channel (configuration based) or LACP (protocol signaling based). LACP provides a standardized means for exchanging information with partner systems to form a dynamic link aggregation group. The LACP feature is automatically enabled during IAP boots and it dynamically detects the AP with the LACP capability, by checking if there is any LACP Protocol Data Unit (PDU) received on either eth0 or eth1 port.

For LACP support, the port-channel must be enabled on the switch and there is no configuration required on the IAP. However, you can view the LACP status on the IAP-224 and IAP-225 by using the **show lacp status** command. For more information, see *Aruba Instant 6.3.1.1-4.0 User Guide* and *Aruba Instant 6.3.1.1-4.0 CLI Reference Guide*.

The LACP feature is supported only on IAP-22x.

Guest Management Interface

In the 6.3.1.1-4.0 release, Instant supports the following types of users:

- Administrator–An admin user who creates SSIDs, wired profiles, DHCP server configuration parameters and manages local user database. The admin users can access the Virtual Controller Management User Interface.
- Guest administrator–A guest interface admin who manages guest users.
- Administrator with read-only access–The read-only admin user does not have access to the Instant CLI. The Instant UI is displayed in the read-only mode for these users.
- Employee users – Employees who use the enterprise network for official tasks.
- Guest users–Visiting users who temporarily use the enterprise network to access the Internet.

The user access privileges are determined by IAP management settings in the AirWave Management client and Aruba Central, and the type of the user.

To manage guest users, a guest management interface is introduced in the Instant UI in the 6.3.1.1-4.0 release. The guest administrators can log in with their credentials and configure guest users. To add a guest admin or read-only user, use the **mgmt-user** command in the Instant CLI.

IAP Integration with Analytics and Location Engine (ALE)

Instant supports integration with Analytics and Location Engine (ALE). The ALE server acts as a primary interface to all third-party applications, and the IAP sends client information and other status information to the ALE server. To

enable integration integrate with ALE, the ALE server address must be configured on the IAP.

The **RTLS** tab in the **Services** window of the Instant UI allows the configuration of ALE server on an IAP. The **ale-server** and **ale-report-interval** commands are introduced in the 6.3.1.1-4.0 release to enable IAP integration with the ALE server. For more information, see *Configuring an IAP for Analytics and Location Engine Support in Aruba Instant 6.3.1.1-4.0 User Guide* and *Aruba Instant 6.3.1.1-4.0 CLI Reference Guide*.

IAP-92 and IAP-93 do not support ALE integration.

IAP Integration with Palo Alto Networks Firewall

Instant supports integration with the Palo Alto Networks (PAN) firewall. To integrate an IAP with PAN user ID, a global profile is required. This profile can be configured on an IAP with PAN firewall information such as IP address, port, user name, password, firewall enabled or disabled status. When PAN firewall information is configured on an IAP, the IAP sends messages to PAN based on the type of authentication and client status.

IAP maintains the network (such as mapping IP address) and user information for its clients in the network and can provide the required information for the user ID feature on PAN firewall.

IAP and PAN firewall integration is supported with the XML-API that is available with PAN-OS 5.0 or later.

To support IAP integration with PAN Firewall, the **Network Integration** tab in the **Services** window of the Instant UI and **firewall-external-enforcement** command in the CLI are introduced. For more information, see *Aruba Instant* and *Aruba Instant 6.3.1.1-4.0 CLI Reference Guide*.

Support for Domain-based ACL

Instant supports configuration of domain-based Access Control List (ACL) rule. Access to a specific domain is allowed or denied based on the ACL rule definition. To enable support for creating a domain-based ACL, the **Access Rule** window in WLAN wizard and Wired Network is modified to include **to domain name** option in **Destination** drop-down.

For more information, see *Aruba Instant 6.3.1.1-4.0 User Guide*.

Internal Captive Portal Splash Page Enhancements

Instant now supports customization of logo, policy text, and usage terms for the internal Captive portal splash page. The customized logo can be uploaded to the internal Captive portal server through the **Security** tab of WLAN wizard Wired network window in the Instant UI, or by using the following command sequence in the Instant CLI:

```
(Instant Access Point)# copy config tftp <ip-address> <filename> portal logo
```

Support for Multiple Captive Portal Profiles

You can now configure external Captive portal profiles and associate these profiles to a user role or SSID. You can create a set of Captive portal profiles in the **Security>External Captive Portal** window and associate these profiles with an SSID or a wired profile. You can also create a new Captive portal profile under the **Security** tab of the WLAN wizard or a **Wired Network** window. In the 6.3.1.1-4.0 release, you can configure up to eight external Captive portal profiles.

When the Captive portal profile is associated to an SSID, it is used before user authentication. If the profile is associated to a role, it is used only after the user authentication. When a Captive portal profile is applied to an SSID or wired profile, the users connecting to the SSID or wired network are assigned a role with the Captive portal rule. The guest user role allows only DNS and DHCP traffic between the client and network, and directs all HTTP or HTTPS requests to the Captive portal unless explicitly permitted.

For more information on creating an Captive portal profile, see:

- *Configuring External Captive Portal for a Guest Network* in *Aruba Instant 6.3.1.1-4.0 User Guide*
- **wlan external-captive-portal** command in *Aruba Instant 6.3.1.1-4.0 CLI Reference Guide*

Client Match

Instant supports the ARM client match feature to continually monitor a client's RF neighborhood and to provide the ongoing client bandsteering service, load balancing, and enhanced IAP reassignment for roaming mobile clients.

The Client Match feature supersedes the legacy bandsteering and spectrum load balancing features, which unlike client match, do not trigger IAP changes for clients already associated to an IAP. When the client match feature is enabled on an IAP, the IAP measures the RF health of its associated clients. When the client match criteria is met, the clients are moved from one AP to another for better performance and user experience.

In the Aruba Instant 6.3.1.1-4.0 release, the client match feature is supported only within an IAP cluster.

You can enable client match in the **ARM** tab of the **RF** window in the Instant UI or by using the **client-match** commands in the ARM configuration mode in Instant CLI.

For more information, see *Aruba Instant 6.3.1.1-4.0 User Guide* and *Aruba Instant 6.3.1.1-4.0 CLI Reference Guide*.

Support for Spanning Tree Protocol

Instant allows enabling of Spanning Tree Protocol (STP) on a wired profile. STP ensures that there are no loops in any bridged Ethernet network and operates on all downlink ports, regardless of the forwarding mode. By default Spanning tree protocol is disabled on wired profiles.

To enable STP on a wired profile, navigate to the **More>Wired>Wired Network>Wired Settings** window and select **Enabled** from the **Spanning tree** drop-down. You can also enable STP by using the **spanning-tree** command in the wired port profile configuration mode in the Instant CLI.

STP will not operate on the uplink port and is supported only on the IAPs with three or more ports.

Customization of Internal Captive Portal Server Certificates

In the 6.3.1.1-4.0 release, Instant supports uploading customized internal Captive Portal server certificates in the PEM or PKCS#12 format to the IAP database. The Captive portal server certificate verifies internal Captive portal server's identity to the client.

To upload a Captive portal server certificate, navigate to **Maintenance>Certificates>Upload New Certificate** and select **Captive portal server** from **Certificate type** drop-down. You can also upload the Captive portal certificate by using the following command in the Instant CLI:

```
(Instant Access Point)# copy tftp {<ip-address> <filename> cpserver cert <password> format
{p12|pem}}
```

For more information, see *Aruba Instant 6.3.1.1-4.0 User Guide* and *Aruba Instant 6.3.1.1-4.0 CLI Reference Guide*.

Provisioning an IAP as a master IAP

In most cases, the master election process automatically determines the IAP that can perform the role of Virtual Controller, which will apply its image and configuration to all other IAPs in the same AP management VLAN. When the Virtual Controller goes down, a new Virtual Controller is elected. If manual specification of the Virtual Controller is required, Instant allows you to manually assign one IAP as the master IAP based on network-specific parameters such as the physical location of the Virtual Controller.

To provision an IAP as a master IAP:

- In the Instant UI, go to **Access Points tab> edit>Edit Access Point** <*AP-name*> window and select **Enabled** from the **Preferred Master** drop-down. For more information, see *Aruba Instant 6.3.1.1-4.0 User Guide*.
- In the Instant CLI, execute the **iap-master** command. For more information, see *Aruba Instant 6.3.1.1-4.0 CLI Reference Guide*.

AirGroup Enhancements

In the 6.3.1.1-4.0 release, Instant supports the following AirGroup services:

- AirPlay™– Apple® AirPlay allows wireless streaming of music, video, and slideshows from your iOS device to Apple TV® and other devices that support the AirPlay feature.
- AirPrint™– Apple AirPrint allows you to print from an iPad®, iPhone®, or iPod® Touch directly to any AirPrint compatible printers.
- iTunes– iTunes service is used by iTunes Wi-Fi sync and iTunes home-sharing applications across all Apple devices.
- RemoteMgmt– Use this service for remote login, remote management, and FTP utilities on Apple devices.
- Sharing– Applications such as disk sharing and file sharing, use the service ID that are part of this service on one or more Apple devices.
- Chat– The iChat® (Instant Messenger) application on Apple devices uses this service.

The services are pre-configured and are available as part of the factory default configuration. The administrator can also enable or disable any or all services by using the Instant UI or CLI.

For more information, see:

- The *Configuring AirGroup and AirGroup Services on an IAP* topic in *Aruba Instant 6.3.1.1-4.0 User Guide*
- The AirGroup commands such as **airgroupservice**, **show airgroup**, **show airgroupservice-ids** in *Aruba Instant 6.3.1.1-4.0 CLI Reference Guide*

Dynamic RADIUS Proxy IP Address Configuration

When the dynamic RADIUS proxy feature is enabled, a static Virtual Controller IP must be configured to ensure that all RADIUS packets use Virtual Controller IP as source IP and VLAN. However, if the users need to authenticate to the RADIUS servers through different VLANs, you can specify the dynamic RADIUS proxy parameters such as IP address and VLAN when configuring the authentication server information on an IAP.

When configured, the dynamic RADIUS proxy IP address and VLAN details are used as source IP address and VLAN for RADIUS packets.

For more information, see:

- *Configuring Dynamic RADIUS Proxy Parameters* in *Aruba Instant 6.3.1.1-4.0 User Guide*
- **wlan auth-server** command in *Aruba Instant 6.3.1.1-4.0 CLI Reference Guide*

Restricted Access Management

Instant supports enhanced inbound firewall configuration and allows you to configure management subnets and restrict access to the corporate network. To allow flexibility in firewall configuration, Instant supports the following configuration options:

- Management Subnets–You can configure subnets to ensure that the IAP management is carried out only from these subnets. When the management subnets are configured, Telnet, SSH, and UI access is restricted to these subnets only.

- Restricted corporate access—You can configure restricted corporate access to block unauthorized users from accessing the corporate network. When restricted corporate access is enabled, corporate access is blocked from the uplink port of master IAP, including clients connected to a slave IAP.

You can configure management subnets and restricted corporate access by using the Instant UI or CLI. For more information, see *Managing Inbound Traffic* in *Aruba Instant 6.3.1.1-4.0 User Guide* and **restricted-mgmt-access** and **restrict-corp-access** command pages in *Aruba Instant 6.3.1.1-4.0 CLI Reference Guide*.

Support for IAP-224 and IAP-225

This release extends support to IAP-224 and IAP-225, which enable support for the IEEE 802.11ac standard for high performance WLAN. These IAPs use MIMO (Multiple-in, Multiple-out) technology and other high-throughput mode techniques to deliver high-performance, 802.11n 2.4 GHz and 802.11ac 5 GHz functionality while simultaneously supporting existing legacy wireless services. The IAP-224 and IAP-225 support 802.11ac on the 5GHz band using 80 MHz channels.

IAP-22x does not support wireless mesh functionality.

Support for IAP-114 and IAP-115

This release extends support to IAP-114 and IAP-115 dual radio, dual-band wireless access points that support the IEEE 802.11n standard for high-performance WLAN. These APs use MIMO (Multiple-in, Multiple-out) technology and other high-throughput mode techniques to deliver high-performance, 802.11n 2.4 GHz and 5 GHz functionality while simultaneously supporting existing 802.11a/b/g wireless services.

AP Subscription

The Service providers can now maintain a subscription list, which is separate from the end user's allowed AP list. Even if an AP is allowed by the end-user, the service provider can disable the AP if the subscription expires. To support this, the service provider uses Aruba Central (cloud management platform) to track the subscription status of each AP based on its serial number or MAC address.

You can enable the subscription of a using the Instant CLI. For more information, see *Aruba Instant 6.3.1.1-4.0 CLI Reference Guide*.

Uplink VLAN Monitoring and Detection on Upstream Devices

The Instant UI now displays an alert message when a client connects to an SSID or a wired interface with a VLAN that is not allowed on the upstream device. The alert message notifies the users about the mismatch in the VLAN configuration on the IAP or the upstream device of an IAP. To resolve this issue, ensure that there is no mismatch in the VLAN configuration.

For more information on VLAN configuration, see *VLAN Configuration* in *Aruba Instant 6.3.1.1-4.0 User Guide*.

Support for Telnet Access

In the 6.3.1.1-4.0 release, Instant supports Telnet access to the Instant CLI. To enable Telnet access:

- In the Instant UI, go to **System>Show advanced options** and select **Enabled** from the **Telnet server** drop-down.
- In the CLI, execute the **telnet-server** command in the configuration mode.

Applying Configuration Changes during a CLI Session

In the 6.3.1.1-4.0 release, the **commit apply no-save** command is introduced to allow the users to apply the configuration changes to a cluster without saving the configuration during a CLI session. The users can save the configuration changes by using the **commit apply** or **write memory** command. For more information, see *Aruba Instant 6.3.1.1-4.0 CLI Reference Guide*.

Two SKUs for IAP-22x and IAP-11x

In the earlier Aruba Instant releases, the IAPs were shipped as the following variants:

- IAP-US (United States)
- IAP-JP (Japan)
- IAP-IL (Israel)
- IAP-RW (Rest of World)

In the 6.3.1.1-4.0.0.1 release, the IAP-11x and IAP-22x are shipped as the following variants:

- IAP-US (United States)
- IAP-RW (Rest of World). This variant also includes Japan and Israel regulatory domains.

When you log in to the Instant UI for the first time, the **Country Code** pop-up will be displayed for the IAPs shipped as IAP-RW variant. You can specify a country code by selecting an appropriate option from the **Please Specify the Country Code** drop-down list. For IAP-11x and IAP-22x, the JP and IL country codes are included in the drop-down list.

If the existing Virtual Controller is an older IAP with the JP country code, a new model with the RW variant can join the cluster and it will operate in the JP regulatory domain. The same applies for the IAPs serving in the IL regulatory domain.

If the existing Virtual Controller is a new IAP-RW, an older model IAP with the JP country code can join the cluster only if the IAP-RW is configured for the JP country code. The same applies for the IAPs serving in the IL regulatory domain.

An IAP-RW can be converted to controller-based operation with an IL or RW variant of controller.

Automatic Negotiation Support for Authentication between IAP and AirWave Management Platform

To establish a connection with the AirWave management server, the IAP authenticates to the AirWave server by using a certificate-based authentication model or the PSK login model. AirWave management platform supports PSK only, Certificate only, or both PSK and certificate-based authentication models. In the 6.3.1.2-4.0.0.2 release, an automatic negotiation mechanism is introduced for authentication between IAP and AirWave management server, irrespective of the authentication model used.

PPPoE Configuration

Starting with 6.3.1.2-4.0.0.2, you can now configure up to 80 characters for a user name, service name, password, and the secret key for CHAP authentication.

To configure PPPoE details:

- In the Instant UI, navigate to **System**>**Uplink**. Under PPPoE, specify the required values for **User**, **Service name**, **Password**, and **CHAP secret** fields.
- In the Instant CLI, use the **pppoe-username**, **pppoe-chapsecret**, **pppoe-passwd**, and **pppoe-svcname** commands in the PPPoE configuration mode.

Support for VPN Tunnel States and Statistics Reporting from an IAP

In the earlier releases, in an IAP-VPN network, the controller behind the IAP was sending information on the VPN tunnel status to the AirWave management server. In the 6.3.1.2-4.0.0.2 release, an enhancement has been introduced to allow the IAP to send a report on the VPN tunnel states and statistics directly to the AirWave server.

Regulatory Updates

IAP-225 now supports the Mexico (MX) country code. To view the list of supported country codes, use the **show country-codes** command. To view the channels available for the IAP-225 operating with the Mexico country code, use the **show ap allowed-channels** command.

Change in the Timeout Duration for an Inactive User Entries

Instant now allows you to set the timeout duration of up to 24 hours, after which an inactive user entry expires. The **inactivity timeout** field in **WLAN wizard** > **WLAN Settings**> **Show advanced options** window of the UI and the **inactivity-timeout** command allow you to set a value within the range of 60-86400 seconds as a timeout duration for user entries.

IAP-VPN Scalability Enhancements

In the current patch release, to address the issue of ping loss to the inner IP address of the IAP, the IAP has been enhanced to act upon the response messages from the virtual controller. The issue was found in networks with a large-scale deployment of IAP-VPN. Specific counters are also added in this release to facilitate debugging.

Support for 128 ACL Rules

IAP-22x now supports the configuration of up to 128 ACL rules for an SSID or wired profile role through the CLI. However, you can configure only up to 64 ACL rules in the UI. To configure ACL rules for an SSID or wired port profile role, use the **wlan access-rule** command.

Configurable Port for Communication between IAP and AirWave Management Platform

In the 6.3.1.4-4.0.0.5 release, the IAP allows the customization of port number of the AirWave management server through the **server_host:server_port** format, for example, **amp.google.com:4343**.

Command Outputs generated from the Support Window in a Single Page

In the 6.3.1.4-4.0.0.5 release, when you run debug commands from the **Support** window of the Instant UI and click **Save**, the output of all the selected commands is displayed in a single page. For more information on support commands, see *Running Debug Commands from the Instant UI* in *Aruba Instant 6.3.1.1-4.0 User Guide*.

GUI Enhancements for Air Monitor Configuration

In the 6.3.1.4-4.0.0.5 release, you can set the Air Monitor per radio on an IAP from the UI. In the **Radio** tab of the **Edit Access Point** window, you can now separately set the mode to **Monitor** on 2.4 GHz and 5 GHZ bands. You can also configure the radio options to use different modes, so that the clients can use radio0 when radio1 is in the Air Monitor mode.

Support for Fully Qualified Domain Name (FQDN) lookup

In this release, IAP DNS is enhanced to fully support FQDN.

This chapter describes the known issues and limitations identified in the previous 6.3.1.x-4.0.0.x releases of of Aruba Instant.

No Support for PKCS#12 Certificate Format

Starting from 6.3.1.1-4.0.0.0 release, Instant does not support uploading of certificates in the (Private-Key Information Syntax Standard) PKCS#12 (.p12) format. To view a list of server and CA certificate formats that are supported by the IAP, run the **show supported-cert-formats** command.

Known Issues

Authentication

Table 50: *Authentication Known Issue*

Bug ID	Description
93045	**Symptom:** When the same dynamic RADIUS Proxy (DRP) IP, VLAN, and gateway details are configured on both the primary and backup authentication servers and if the DRP details are deleted for either the primary or backup server, the DRP IP feature does not function. **Scenario**: This issue occurs when the same DRP IP is configured on the primary and backup authentication servers. This issue is found in IAPs running Aruba Instant 6.3.1.1-4.0.0.0. **Workaround**: None.

Captive Portal

Table 51: *Captive Portal Known Issues*

Bug ID	Description
93173	**Symptom**: Captive portal does not support PEM certificates with passphrase protected private key. **Scenario**: This issue occurs in IAPs running Aruba Instant 6.3.1.1-4.0.0.0 when the customized Captive portal certificates are uploaded with passphrase protected private key. **Workaround**: None
93224	**Symptom**: IAP does not support server certificate encrypted by PKCS#8. **Scenario:** This issue is found in IAPs running Aruba Instant 6.3.1.1-4.0.0.0. **Workaround**: Use the PKCS#1 format for certificate encryption.

SNMP

Table 52: *SNMP Known Issue*

Bug ID	Description
98949	**Symptom**: When tunnel mode is configured on an IAP, traps are generated from the Virtual Controller IP instead of the tunnel IP address. **Scenario**: This issue occurs when the Virtual Controller IP and tunnel mode are configured with a 3G uplink connection. This issue is found in IAPs running Aruba Instant 6.3.1.4-4.0.0.5. **Workaround**: Do not configure Virtual Controller IP if 3G uplink is enabled.