Aruba Instant 6.2.1.0-3.4.0.4

ARUBA networks

Release Notes

www.arubanetworks.com

1344 Crossman Avenue
Sunnyvale, California 94089

Phone: 408.227.4500
Fax 408.227.4550

Contents

Chapter 1

Release Overview

Aruba Instant 6.2.1.0-3.4.0.4 is a software patch release that introduces fixes to the issues detected in the previous releases.

For more information on features described in the following sections, see the *Aruba Instant 6.2.1.0-3.4 User Guide*.

Contents

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
End of Support information	www.arubanetworks.com/support-services/end-of-life-products/end-of-life-policy/
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

Chapter 2

What's New in this Release

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

Enhancements

The following enhancement was introduced in 6.2.1.0-3.4.0.4 patch release.

RFC 3576 Enhancements

When RFC3576 is enabled, the IAP can process RFC 3576-compliant Change of Authorization (CoA) and disconnect messages (DM) from the RADIUS server.

In the earlier releases, Instant supported the following scenarios:

- When a client is connected to an IAP and the client information is available in **show client** command output, the IAP sends a confirmation message (ACK) to the RADIUS server. In such a case, the IAP can perform the CoA or DM operation on the client.
- When a client is not connected to an IAP, the IAP sends a failure message (NAK) to the RADIUS Server. In such a case, the IAP cannot perform the CoA/DM operation to the client.

With enhancement in this release, if a client is not connected to an IAP, but the client information is available in the **show client** command output, the IAP sends a confirmation message (ACK) to the RADIUS server. The IAP can perform the CoA/DM operation to the client within the configured timeout period.

Resolved Issues

AirGroup

Table 1 *AirGroup Fixed Issue*

Bug ID	Description
90821	**Symptom:** When the uplink VLAN was configured on an IAP, the AirGroup servers in other VLANs could not be discovered. A change to VLAN tagging has resolved this issue. **Scenario:** This issue occurred when uplink VLAN was configured on the IAP and devices were in a different VLAN other than the one configured as uplink VLAN. This issue was found in IAPs running Aruba Instant 6.2.1.0-3.4.0.3 or earlier versions.

Authentication

Table 2 *Authentication Fixed Issue*

Bug ID	Description
92738	**Symptom:** The Layer -2 user entry could not be deleted from the Datapath User Table when a client disconnected from the IAP. A change in the user action code has fixed this issue. **Scenario:** This issue occurred when MAC authentication was enabled on the IAP. This issue was found in IAPs running Aruba Instant 6.2.1.0-3.4.0.3.

Hotspot 2.0

Table 3 *Hotspot 2.0 Fixed Issue*

Bug ID	Description
88583	**Symptom:** The hotspot configuration information was not available in the beacons after rebooting the IAPs operating in Canada (CA) regulatory domain. To resolve this issue, re-apply the hotspot configuration changes whenever the country code of an IAP is changed. **Scenario:** This issue occurred when the country code was changed on the IAP after configuring the hotspot profiles. This issue was found in IAPs running Aruba Instant 6.2.1.0-3.4.0.0.

Chapter 3

Features Added in the Previous Releases

This chapter provides a brief summary of the new features and enhancements introduced in the previous release of Aruba Instant.

For more information on the features listed in this section and the related configuration procedures, see *Aruba Instant 6.2.1.0-3.4 User Guide*.

New Features

Lawful Intercept and CALEA Integration

In the current release, Instant supports CALEA server integration to enable service providers (SPs) to perform electronic surveillance authorized by the Law Enforcement Agencies (LEA).

Depending on the country of operation, the SPs are required to support Lawful Intercept (LI) in their respective networks. In the United States, SPs are required to ensure LI compliance based on Communications Assistance for Law Enforcement Act (CALEA) specifications.

To support CALEA integration and ensure LI compliance, you can configure the IAPs to replicate a specific client traffic and send it to a remote CALEA server. The replicated traffic can be sent either directly to the CALEA server or through the VPN.

- If the IAP is configured to send the client data directly to the CALEA server, an individual GRE tunnel is configured to the CALEA server and the client traffic is replicated within the GRE tunnel. Each IAP performs GRE encapsulation only for the clients associated to it.
- If the CALEA server is deployed with the Aruba Controller and an additional IPSec tunnel is configured for the corporate access, the client traffic is replicated by the slave IAP. The client data is encapsulated by GRE on slave and then routed to the master IAP. The master IAP sends the IPsec client traffic to the Controller. The Controller handles the IPSec client traffic, while GRE data is routed to the CALEA server.

The client traffic is replicated in the following ways:

- Through RADIUS VSA— In this method, the client traffic is replicated by using RADIUS VSA to assign clients to a CALEA related user role. To enable role assignment to clients, you need to create a user role and CALEA access rule, and then assign the CALEA rule to the user role. Whenever a client that is configured to use a CALEA rule connects, a replication role is assigned.
- Through Change of Authorization (CoA)—In this method, a user session can start without replication. When the network administrator triggers a CoA from the RADIUS server, the user session is replicated. The replication is stopped when the user disconnects or by sending a CoA to change the replication role.

For more information on configuring IAPs for CALEA integration, see *Lawful Intercept and CALEA Integration* section in *Aruba Instant 6.2.1.0-3.4 User Guide* and *calea* command in *Aruba Instant 6.2.1.0-3.4 CLI Reference Guide*.

You can configure DHCP options using Instant UI or CLI. For more information, see *Configuring DHCP Scopes* section in *Aruba Instant 6.2.1.0-3.4 User Guide* and *ip dhcp* command in the *Aruba Instant 6.2.1.0-3.4 CLI Reference Guide*.

L2TPv3 Configuration

The Layer 2 Tunneling Protocol version 3 (L2TPv3) feature allows the IAP to act as an L2TP Access Concentrator (LAC) and tunnels all wireless clients L2 traffic from AP to L2TP Network Server (LNS). In a centralized L2 model, the VLAN on the corporate side is extended to remote branch sites. The wireless clients associated to the IAP get the IP address from the DHCP server running on the LNS.

In this release:

- Instant supports tunnel and session configuration, and uses Control Message Authentication (RFC 3931) for tunnel and session establishment. Each L2TPv3 tunnel supports one data connection and this connection is termed as an L2TPv3 session.
- Each IAP supports tunneling over UDP only.
- If primary LNS is down, it fails over to the backup LNS. The primary and backup IP address can be configured under L2TPV3 tunnel profile. If the primary tunnel creation fails or if the primary tunnel gets deleted, the backup becomes available. The IAPs support the following failover modes:
  - Preemptive: In this mode, if the primary server becomes available when the backup is active, the backup tunnel is deleted and the primary tunnel is set as the only active tunnel. If you configure the tunnel to be preemptive and when the primary tunnel goes down, a persistence timer which tries to bring up the primary tunnel starts.
  - Non-Preemptive: In this mode, when the connection to backup tunnel is established after primary tunnel goes down, the primary tunnel will not be set as the active tunnel when it becomes available.

You can configure the tunnel and session for L2TPv3 by using Instant UI or CLI. For more information, see *Configuring an L2TPv3 Tunnel* in *Aruba Instant 6.2.1.0-3.4 User Guide*, and *l2tpv3 session* and l*2tpv3 tunnel* commands in *Aruba Instant 6.2.1.0-3.4 CLI Reference Guide*.

Support of Regular Expressions in VLAN and Role Derivation Rules

For complex policies of role and VLAN derivation using device DHCP fingerprints, you can use a regular expression to match against the combined string of the MAC address and the DHCP options. The combined string is formed by concatenating the hexadecimal presentation of the MAC address and all of the DHCP options sent by a particular device. The regular expression is a pattern description language that can be used for advanced pattern matching of a given string.

The **matches-regular-expression** operator allows you to use regular expression when creating a VLAN or role derivation rule. The rule is applied only if the attribute value matches the given regular expression pattern. The **matches-regular-expression** operator can be used only for defining a role derivation rule based on the **mac-address-and-dhcp-options** attribute.

For more information on regular expressions, and creating VLAN and role derivation rules, see the following topics in *Aruba Instant 6.2.1.0-3.4 User Guide:*

- *Using Regular Expressions in Role and VLAN Derivation Rules*
- *Creating a Role Derivation Rule*
- *Configuring VLAN Derivation Rules*

Dynamic CPU Management

In the current release, Instant dynamically manages resources across different functions performed by an AP. However, under special circumstances if resource management needs to be enforced or disabled altogether, the dynamic CPU management configuration settings can be modified.

For dynamic resource management:

- The **Dynamic CPU management** drop-down with the following options is added in the **System** window of the Instant UI:

- **Automatic**— When selected, the CPU management is automatically enabled or disabled as required during run-time. This is the default and recommended option.
- **Always enabled in all APs**— Enables dynamic management of resources across different functions performed by an IAP.
- **Always disabled in all APs**— Disables the CPU management feature on all APs, typically for small networks.

- The **dynamic-cpu-mgmt** command with the **auto**, **enable,** and **disable** parameters is added in the Instant CLI.

For more information, see *Dynamic CPU Management* in *Aruba Instant 6.2.1.0-3.4 User Guide* and *dynamic-cpu-mgmt* command in *Aruba Instant 6.2.1.0-3.4 CLI Reference Guide*.

Connectivity Summary on Instant Login Page

You can now view a summary of the connectivity status to the Instant network. The Instant **Login** page displays a summary indicating the status of the Internet availability, uplink, signal strength, VPN, and AirWave configuration details before logging in to the Instant UI.

The Internet status is available only if the Internet failover feature (**System>Show advanced option>uplink>Internet failover**) is enabled.

The cellular provider and cellular strength information is available only when a 3G or 4G modem is in use.

Enhancements to PPPoE Configuration

Instant allows you to set a local interface for the PPPoE uplink connections by configuring the Local,L3 DHCP gateway IP address as the local IP address of the PPPoE interface. When configured, the local interface acts as an unnumbered PPPoE interface and allows the entire Local,L3 DHCP subnet to be allocated to clients.

Before configuring a local interface for the PPPoE connections, ensure that the Local,L3 DHCP scope is configured on the IAP.

For more information, see *Configuring PPPoE Uplink Profile* in *Aruba Instant 6.2.1.0-3.4 User Guide* and *pppoe-uplink-profile* command in *Aruba Instant 6.2.1.0-3.4 CLI Reference Guide*.

Reconnecting Users During a VPN Failover

In the current release of Instant, the IAPs can be configured to disable all SSIDs when the system switches during VPN tunnel transition from primary to the backup VPN tunnel Vice-Versa. You can also specify an interval for VPN tunnel transition, after which the users can be reconnected to the VPN tunnel.

To enable this feature through the Instant UI:

1. Navigate to **More>VPN>Show advanced options>IPSec**.
2. Set **Reconnect user on failover** to **Enabled**.
3. To configure an interval during which wired and wireless users are disconnected due to a VPN tunnel switch, specify the number of seconds in **Reconnect time on failover.**

To enable this feature through the Instant CLI, execute the following commands at the command prompt:

```
(Instant Access Point)(config)# vpn reconnect-user-on-failover
(Instant Access Point)(config)# vpn reconnect-time-on-failover <down_time>
```

For more information, see *Configuring PPPoE Uplink Profile* in *Aruba Instant 6.2.1.0-3.4 User Guide* and *pppoe-uplink-profile* command in *Aruba Instant 6.2.1.0-3.4 CLI Reference Guide*.

Enhancements

The following enhancements are introduced in Aruba Instant *6.2.1.0-3.4*, *6.2.1.0-3.4.0.1*, and *6.2.1.0-3.4.0.2* releases.

Dead Time Configuration for Authentication Servers

In the current release, you can configure a dead time for authentication servers to enable an unavailable authentication server to be marked as "out of service". When two or more authentication servers are configured on the IAP and if a server is unavailable, the dead time configuration determines the duration after which an authentication server is marked as unavailable. When the dead time duration is passed, the IAP retries to connect to the server.

For dead time configuration:

- The **Dead time** field is added in the **New Server** window. The **New Server** window can be launched through **Security>Authentication Servers>New**, or **New WLAN or Edit WLAN>Security> Authentication server 1>New**). For more information, see the *Configuring Authentication Servers* in *Aruba Instant 6.2.1.0-3.4 User Guide*.
- The **deadtime** parameter is added to the **wlan auth-server** command. For more information, see *wlan auth-server* command in *Aruba Instant 6.2.1.0-3.4 CLI Reference Guide*.

Deletion of Dynamically Blacklisted Clients

In the current release of Instant, the administrators can delete the clients that were dynamically blacklisted. The dynamic blacklisting is used when the clients exceed the authentication failure threshold, or when a blacklisting rule triggers as part of the authentication process.

To delete the clients that are blacklisted dynamically, execute the following command:

```
(Instant access point)# remove-blacklist-client <MAC_adress> <AP_name>
```

For more information, see the *remove-blacklist-client* command in *Aruba Instant 6.2.1.0-3.4 CLI Reference Guide*.

Cellular Modem Configuration with PAP and CHAP

In the current release of Instant, the USB modems can be configured to use Password Authentication Protocol (PAP) or Challenge Handshake Authentication Protocol (CHAP) authentication types. This allows the 3G Point-to-Point protocol (PPP) to use either PAP or CHAP to validate clients.

To configure the USB modem, execute the following commands:

```
(Instant access point)(config)# cellular-uplink-profile
(Instant Access Point)(cellular-uplink-profile)# usb-auth-type {pap |chap}
```

For more information on cellular uplink configuration, see *cellular-uplink-profile* command in the *Aruba Instant 6.2.1.0-3.4 CLI Reference Guide* and *Configuring Cellular Uplink Profiles* in the *Aruba Instant 6.2.1.0-3.4 User Guide*.

Maximum Distance Configuration for 5GHz and 2.4 GHz Radio Profiles

Instant now allows you to configure the maximum distance between a client and an AP or between a mesh point and a mesh portal in meters. You can configure a value ranging from 600 to 1000 meters.

A value of 0 specifies the default settings for this parameter, where time-outs are only modified for outdoor mesh radios which use a distance of 16km.

For more information, see the *rf dot11a-radio-profile* and *rf dot11g-radioprofile* commands in the *Aruba Instant 6.2.1.0-3.4 CLI Reference Guide*.

Provisioning Support for Huawei HWD12 Modem

Aruba Instant now supports automatic provisioning of the Huawei HWD12 modem.

Enhancements to the Personal Network Encryption Settings

In the *6.2.1.0-3.4.0.1* release, Instant allows wpa-psk-aes and wpa-psk-tkip encryption types for WPA personal security configuration.

You can configure wpa-psk-aes and wpa-psk-tkip encryption types for personal networks through the Instant UI or CLI.

Using the Instant UI

1. Go to **New WLAN or Edit WLAN>Security>Personal**.
2. Select the **WPA Personal** option from the **Key management** drop-down.
3. Click **Next**.

Using the Instant CLI

Execute the following commands at the command prompt:

```
(Instant Access Point)(config)# wlan ssid-profile <Name>
(Instant Access Point)(SSID Profile <name>)# opmode wpa-psk-tkip,wpa-psk-aes
```

Support for Novatel and Sierra Modems

Aruba Instant now supports the Novatel Wireless U679 (for RAP-3WNP only) and Sierra Wireless 320U modems.

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

Resolved Issues in 6.2.1.0-3.4.0.3

Authentication

Table 1 *Authentication Fixed Issues*

Bug ID	Description
90586	**Symptom:** Radius authentication failed for clients connected to a slave IAP. The issue was fixed by a change in the route cache entry aging logic. **Scenario:** The issue was observed when there were no ARP entries for the RADIUS server for the guest users. Due to this, the virtual controller stopped sending packets. This issue was not limited to any specific IAP model or software version.

IAP-VPN

Table 2 *IAP-VPN Fixed Issue*

Bug ID	Description
90893	**Symptom:** When **Reconnect User on VPN Failover** feature was enabled and VPN primary failed along with an IAP reboot, incorrect configuration was applied. To resolve this issue, do not save the configuration changes to IAP flash. **Scenario:** When **Reconnect User on VPN Failover** feature is enabled and VPN primary fails, there is a configurable interval during which all WLAN SSIDs and Wired ports are disabled. If the IAP reboots within this interval, it comes up with incorrect configuration. This issue was found in IAPs running Aruba Instant 6.2.1.0-3.4.
90928	**Symptom:** When the VPN connection was reestablished after a failover, the wired clients, on which 802.1X with MAC authentication was enabled, were assigned a **Deny All** role. A change in the user table flushing process has resolved this issue. **Scenario**: Due to an internal process, the L2 user details were flushed when the VPN connection was being established. As a result, the wired clients with 802.1X authentication enabled were assigned a **Deny All** role. This issue was found in IAPs running Aruba Instant 6.2.1.0-3.4.0.0.

Mesh Network

Table 3 *Mesh Network Fixed Issue*

Bug ID	Description
89449	**Symptom:** The SAPD process crashed frequently on a mesh portal. To resolve this issue, check if the channel structure pointer is invalid. If the pointer is invalid, do not use it. **Scenario:** This issue occurred when AM scanned some special channels. Due to an invalid channel configuration, the SAPD process crashed. This issue was found in Mesh IAPs running Aruba Instant 6.2.1.0-3.3.0.0 or later.

Mobility

Table 4 *Mobility Fixed Issues*

Bug ID	Description
90039	**Symptom:** When the client VLAN for a given SSID was the same across two IAP clusters, clients roaming across clusters were getting marked as foreign (L3-roaming), even though they were in the same VLAN. The issue is fixed by monitoring the foreign clients and re-assigning them as normal (not foreign) if found to be in the same VLAN. **Scenario:** The issue was observed when clients roamed from one IAP cluster to another, and both clusters had the same client VLAN. This issue was not limited to any specific IAP model or a software version.
90041	**Symptom:** Clients roaming across two IAP clusters with same VLAN were determined as foreign clients (L3-roaming) causing the network loops and connectivity issues. To resolve this issue, do not configure L3 mobility for the IAPs when the client VLAN for a given SSID is same across two IAP clusters. When the client VLAN for a given SSID is same across two IAP clusters, L3 mobility configuration is not required. In case the L3 mobility is configured, it determines clients roaming across clusters as foreign clients (L3-roaming). **Scenario:** The issue was observed when clients roamed from one IAP cluster to another and both clusters had the same client VLAN. The data from the roaming client was tunneled to the home IAP caused a network loop. This issue was not limited to any specific IAP model or a software version.

SNMP

Table 5 *SNMP Fixed Issue*

Bug ID	Description
88575	**Symptom:** Although the SNMP operations could be carried out successfully for the IP address of IAP Virtual Controller, the master AP did not respond to SNMP queries on Ethernet IP. Upgrading to Aruba Instant 6.2.1.0-3.4.0.3 resolves this issue. **Scenario:** This issue was found in IAPs running Aruba Instant 6.2.1.0-3.4.0.0.

Virtual Controller Management

Table 6 *Virtual Controller Management Fixed Issue*

Bug ID	Description
91157	**Symptom:** An IAP failed to get a DHCP IP address from Windows 2012 DHCP Server when the DHCP failover feature was enabled. The **Seconds elapsed** field in the DHCP request packets is now updated correctly to resolve this issue. **Scenario:** This issue occurred because the **Seconds elapsed** field in the DHCP discover or request packets was not updated correctly by the IAP. The **Seconds elapsed** field is used by some DHCP servers, such as Windows 2012 server to determine if client DHCP requests need to be accepted. This issue was found in IAPs running Aruba Instant 6.2.1.0-3.4.0.1 or later.

Resolved Issues in 6.2.1.0-3.4.0.2

Authentication

Table 7 *Authentication Fixed Issues*

Bug ID	Description
87831	**Symptom:** An IAP sent incorrect accounting packets when some clients reconnected to the IAP. A change in the accounting process has fixed this issue. **Scenario:** This issue occurred because the client dissociated from the IAP without sending deauthentication or dissociation packets. When the client reconnected to the IAP, the IAP sent incorrect accounting packets. This issue was found in IAPs running Aruba Instant 6.2.1.0-3.4.
87910	**Symptom:** When both PSK and MAC authentication were configured, the clients using a certain WLAN NIC could not reconnect to the IAP. A change in the authentication context of PSK with MAC authentication has fixed this issue. **Scenario:** This issue occurred because the client dissociated from the IAP without sending deauthentication or dissociation packets. This issue was found in IAPs running Aruba Instant 6.2.1.0-3.4 and the clients using a certain WLAN NIC.

Hotspot 2.0

Table 8 *Hotspot 2.0 Fixed Issues*

Bug ID	Description
88581	**Symptom**: The Connection Capability configuration details were not saved on the IAP. To resolve this issue, use the correct command string to save the configuration. **Scenario**: This issue occurred because an incorrect string was used for configuring the Connection Capability profile. This issue was found in IAPs running Aruba Instant 6.2.1.0-3.4.
88583	**Symptom:** The hotspot configuration information was not available in the beacons after rebooting the IAPs operating in Canada (CA) regulatory domain. To resolve this issue, re-apply the hotspot configuration changes whenever the country code of an IAP is changed. **Scenario:** This issue occurred when the country code was changed on the IAP after configuring the hotspot profiles. This issue was found in IAPs running Aruba Instant 6.2.1.0-3.4.
88584	**Symptom:** IAPs crashed when the hotspot clients sent the ANQP request with the Connection Capability information element. A check has been added to verify the Connection Capability profile configuration to resolve this issue. **Scenario:** This issue occurred because there was no Connection Capability profile configured on the IAP. This issue was found in IAPs running Aruba Instant 6.2.1.0-3.4.

L2TPV3

Table 9 *L2TPV3 Fixed Issue*

Bug ID	Description
89466	**Symptom:** The IAPs did not send the **Hello** packets whenever there was data traffic between the IAP and LNS server. To resolve this issue, the Instant CLI has been enhanced to send **Hello** packets irrespective of the data traffic. **Scenario:** This issue was found in IAPs running Aruba Instant 6.2.1.0-3.4.

Mesh Network

Table 10 *Mesh Network Fixed Issue*

Bug ID	Description
87879	**Symptom:** A mesh point rebooted randomly with the **Udhcpc does not exist on mesh point. Reboot by clid** error message. A change in the internal process has resolved this issue. **Scenario**: This issue occurred when a mesh point was configured with a static IP address. Due to an internal process failure, the mesh point randomly rebooted. This issue was found in IAPs running Aruba Instant 6.2.1.0-3.4 in mesh topology.

SNMP

Table 11 *SNMP Fixed Issue*

Bug ID	Description
87211	**Symptom:** An incorrect source IP address was displayed in the SNMP traps when logging in to Instant through the SSH client failed. A change in the log message generation mechanism has resolved this issue. **Scenario**: This issue occurred when a user tried to log in to Instant through the SSH client using incorrect credentials. This issue was found in IAPs running Aruba Instant 6.2.0.0-3.2 and later versions.

Wireless Driver

Table 12 *Wireless Driver Fixed Issue*

Bug ID	Description
85631	**Symptom:** An Apple® client was randomly disconnected from an E-mail application. A change in the packet handling process has fixed this issue. **Scenario:** This issue was observed in IAPs running Aruba Instant 3.2.0.4 when there was a packet loss with Mac OS X clients accessing a specific E-mail application.

Resolved Issues in 6.2.1.0-3.4.0.1

Access Point

Table 13 *Access Point Fixed Issue*

Bug ID	Description
78122 87187	**Symptom:** Some APs rebooted randomly due to memory issues. To resolve this issue, upgrade to Aruba Instant 6.2.1.0-3.4.0.1. **Scenario:** This issue was found in APs running ArubaOS 6.2.1.0 and IAPs running Aruba Instant 6.2.1.0-3.3.

AirGroup

Table 14 *AirGroup Fixed Issue*

Bug ID	Description
87139	**Symptom:** The AirGroup clients were not able to discover the AirPrint servers as the server records were not synchronized in all IAPs in a cluster. An increase in the buffer from 2K to 4K for storing the server records has resolved this issue. **Scenario:** When the server records exceeded 2K buffer, the synchronization of server records across the IAPs failed. This issue was found in IAPs running Aruba Instant 6.2.1.0-3.3 or later.

Authentication

Table 15 *Authentication Fixed Issue*

Bug ID	Description
86932	**Symptom:** The clients could not authenticate when the IP address for the Bridge interface was lost. To resolve this issue, upgrade to Aruba Instant 6.2.1.0-3.4.0.1. **Scenario:** This issue occurred when the IP address for the Bridge interface was not available in the datapath user entry, after the Bridge interface IP was changed. This issue was found in IAPs running Aruba Instant 6.2.1.0-3.2.0.x releases with Dynamic RADIUS proxy enabled.

Datapath

Table 16 *Datapath Fixed Issue*

Bug ID	Description
86865	**Symptom:** Clients could not connect to the IAP when the master IAP sent packets to the default gateway MAC address instead of the Virtual Controller gateway MAC address. The packets from the Virtual Controller IP address are now channelled through a routing module to ensure correct routing. **Scenario:** The issue occurred on a master IAP with dynamic RADIUS proxy feature enabled. When the Virtual Controller VLAN and gateway were configured on an IAP and the Virtual Controller gateway IP and the default gateway had different MAC addresses, the master IAP sent packets to the default gateway. This issue was found in IAPs running Aruba Instant 6.2.1.0-3.3 and later versions.

L2TPV3 Configuration

Table 17 *L2TPV3 Fixed Issue*

Bug ID	Description
86639	**Symptom:** When the local UDP port was set to a user-defined value, the L2TPv3 process failed to start correctly. To resolve this issue, upgrade to Aruba Instant 6.2.1.0-3.4.0.1. **Scenario:** This issue occurred when the IAPs rebooted with a user-defined local UDP port configured for the L2TP tunnel. This issue was found in IAPs running Aruba Instant 6.2.1.0-3.4.

Station Management

Table 18 *Station Management Fixed Issue*

Bug ID	Description
86996	**Symptom:** IAPs rebooted randomly due to a high CPU utilization. Changes in the log clearing process for the offline clients have resolved this issue. **Scenario:** When many wireless clients disassociated from an IAP, the respective L3 user entries for the offline clients were not deleted from the IAP database. Due to this, the IAPs showed a 100% CPU utilization and rebooted randomly. This issue was found in IAPs running Aruba Instant 6.2.1.0-3.3.

Terminal Access

Table 19 *Terminal Access Fixed Issue*

Bug ID	Description
88020	**Symptom:** The SSH access to the IAP Command-Line Interface (CLI) was enabled, although it was set to disabled before the IAP reboot. A change in the IAP code has resolved this issue. **Scenario:** This issue occurred because the terminal access status was reset to enabled after each IAP reboot. This issue was found in IAPs running Aruba Instant 6.2.1.0-3.3.0.3 or later.

Resolved Issues in 6.2.1.0-3.4

Authentication

Table 20 *Authentication Fixed Issue*

Bug ID	Description
83848	**Symptom:** An IAP sent new accounting information for the re-associated clients, instead of sending accounting information in the previous accounting session ID. Changes to the code base have resolved this issue. **Scenario:** This issue was observed when a client re-associated to an IAP and the IAP sent RADIUS START accounting records for that client to the RADIUS server with a new session ID. This issue was found in IAPs running Aruba Instant 6.2.1.0-3.3.

Mesh Network

Table 21 *Mesh Network Fixed Issue*

Bug ID	Description
85692	**Symptom:** The mesh IAP clients could not obtain an IP address from the DHCP server. Disabling **Deny inter-user bridging** feature through the Instant UI or CLI resolves this issue. **Scenario:** This issue occurred because the **Deny inter-user bridging** feature was enabled on the IAP. Due to this, the IAP denied bridging traffic between its clients and wireless ports, thereby blocking the IP address assignment from the DHCP server for the mesh IAP clients. This issue was found in IAPs running Aruba Instant 6.2.1.0-3.1 or later releases in mesh topology.

Security

Table 22 *Security Fixed Issue*

Bug ID	Description
85410	**Symptom:** The users could not view the uploaded server certificates after an IAP reboot. Changes to the CA certificate reading process have resolved this issue. **Scenario:** After a reboot, the IAPs did not display the server certificates uploaded by the user as there was no CA certificate uploaded by the users in the IAP database. This issue was found in IAPs running 6.2.1.0-3.3.0.1.

SNMP

Table 23 *SNMP Fixed Issue*

Bug ID	Description
82752	**Symptom**: The value for the SNMP **aiRadioPhyEvents** counter was displayed as **0**. The IAP now displays correct values for the SNMP aiRadioPhyEvents counter. **Scenario**: This issue was found in IAPs running Aruba Instant 6.2.1.0-3.3.
86108	**Symptom:** The SNMP GET operations could not be performed on a Virtual Controller, although the Virtual Controller IP address was configured for SNMP operations. Upgrading to Aruba Instant 6.2.1.0-3.4 resolves this issue. **Scenario:** This issue was found in IAPs running Aruba Instant 6.2.1.0-3.3.

VLAN Configuration

Table 24 *VLAN Configuration Fixed Issue*

Bug ID	Description
85162	**Symptom:** An IAP rebooted when connected to a virtual controller that was configured to use the same VLAN as that of uplink. To resolve this issue and to avoid duplication of the route cache entries, do not configure the same VLAN for uplink and Virtual Controller. **Scenario:** This issue was observed when the same VLAN was configured for Virtual Controller and uplink on an IAP. When a client connected to this IAP and tried to reach the Virtual Controller IP, the IAP rebooted. This issue was found in IAPs running Aruba Instant 6.2.0.0-3.3.
85902	**Symptom:** The IAP management through AirWave and the client authentication against Virtual Controller IP address failed due to incorrect VLAN tagging. The IAP now tags the uplink VLAN only if a packet is not tagged already. **Scenario:** When the Virtual Controller VLAN and uplink VLAN were configured separately on the IAP, the Virtual Controller VLAN was not enforced, and was instead tagged with the uplink VLAN. This issue was found in IAPs running Aruba Instant 6.2.1.0-3.3.

The known issues and limitations identified in the previous releases of Aruba Instant are described in the following tables.

Known Issues

AirWave Integration

Table 1 *AirWave Integration Known Issue*

Bug ID	Description
85335	**Symptom:** The users can configure IAP names exceeding the character limit through AirWave Management Server, although the character limit is set to 32. **Scenario:** This issue is found in IAPs running Aruba Instant 6.2.1.0-3.4 with AirWave 7.7. **Workaround:** None

Datapath

Table 2 *Datapath Known Issue*

Bug ID	Description
90886	**Symptom:** IAPs cannot identify and show the OS version of the clients connected to it. **Scenario**: The issue is observed when client traffic missed some part of firewall processing which performs OS identification. The issue is found in IAPs running Aruba Instant 6.2.1.0-3.4.0.0 or later versions. **Workaround**: None.

L2TPV3 Configuration

Table 3 *L2TPV3 Known Issue*

Bug ID	Description
86486	**Symptom:** If an L2TP session is created before configuring the L2TP tunnel, the session cannot be associated with the tunnel. **Scenario:** This issue occurs when a session is created before configuring the tunnel or if a session is created under an incorrectly configured tunnel. This issue is found in IAPs running Aruba Instant 6.2.1.0-3.4. **Workaround:** Do not configure a session profile before creating the L2TP tunnel profile. If a tunnel is incorrectly configured, reconfigure the tunnel and then create a corresponding session profile.

VLAN Configuration

Table 4 *VLAN Configuration Known Issues and Limitations*

Bug ID	Description
75496	**Symptom:** A slave IAP cannot connect to the master IAP when reconnecting to the network. **Scenario:** This issue occurs when the Ethernet uplink fails and switches over to another available uplink. This issue was observed in a hierarchical network topology when the native VLAN on a wired port was set to a value other than 1. This issue is found in IAPs running Aruba Instant version 6.2.0.0-3.2 or later. **Workaround:** None
80849	**Symptom:** In a hierarchical topology, although the clients can obtain an IP address, the Virtual Controller Gateway IP address resolution fails. **Scenario:** This issue occurs when the master IAP assigns a guest VLAN IP address to the client. As the DHCP scope configuration on the slave IAP uses a different subnet, the Virtual Controller gateway IP address cannot be resolved. This issue is found in IAPs running Aruba Instant 6.2.1.0-3.3. **Workaround:** Manually configure the DHCP pool to ensure that the appropriate subnet is used for assigning IP addresses to the clients.

Limitations

Automatic DHCP Pool and IP Address Assignment

When the DHCP server is configured and if the Client IP assignment parameter for an SSID profile is set to **Virtual Controller Assigned**, the Virtual Controller assigns the IP addresses to the WLAN or wired clients. By default, the IAP automatically determines a suitable DHCP pool for Virtual Controller Assigned networks.

In the current release, the IAPs typically select the 172.31.98.0/23 subnet. If the IP address of the IAP is within the 172.31.98.0/23 subnet, the IAP selects the 10.254.98.0/23 subnet. However, this mechanism does not guarantee that it would avoid all possible conflicts with the wired network. If your wired network uses either 172.31.98.0/23 or 10.254.98.0/23, and you experience problems with the **Virtual Controller Assigned** networks after upgrading to Aruba Instant 6.2.1.0-3.4, manually configure the DHCP pool. For more information, see *Configuring DHCP Server for Client IP Assignment* in *Aruba Instant 6.2.1.0-3.4 User Guide*.