


# **Aruba Instant 6.4.0.3-4.1.0.2**



Release Notes

## Copyright

© 2014 Aruba Networks, Inc. Aruba Networks trademarks include  Airwave, Aruba Networks®, Aruba Wireless Networks®, the registered Aruba the Mobile Edge Company logo, Aruba Mobility Management System®, Mobile Edge Architecture®, People Move. Networks Must Follow®, RFPProtect®, Green Island®. All rights reserved. All other trademarks are the property of their respective owners.

## 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](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.

---

<b>Contents</b> .....	<b>3</b>
<b>Release Overview</b> .....	<b>5</b>
Contents .....	5
Contacting Support .....	5
<b>What's New in this Release</b> .....	<b>6</b>
Enhancements .....	6
Resolved Issues in this Release .....	6
AirGroup .....	6
Authentication .....	6
ARM .....	6
DHCP Server .....	7
User Interface .....	7
VC Management .....	7
VPN .....	7
Known Issues .....	8
Authentication .....	8
<b>Issues Resolved in Previous Releases</b> .....	<b>9</b>
Resolved Issues in 6.4.0.2-4.1.0.1 release .....	9
AirWave .....	9
Authentication .....	9
Captive Portal .....	9
Datapath .....	10
RAP-NG .....	10
STM .....	10
VPN .....	10
Wireless .....	11
<b>Features Added in Previous Releases</b> .....	<b>13</b>
Features and Enhancements .....	13
AppRF .....	13

AirGroup Enhancements .....	14
Support for New Access Points .....	14
Configurable DSCP Mapping Values for WMM Access Categories .....	14
Console Access to IAP .....	15
Instant UI Changes .....	15
Full Tunnel-Mode VPN Configuration .....	16
Inbound Firewall .....	16
Fast Roaming Enhancements .....	16
Support for 4G Modems .....	17
Client Match Enhancements .....	17
Sourcing Virtual Controller Traps from the Virtual Controller IP .....	17
Support for TACACS+ Servers .....	18
Integration with an XML API Interface .....	18
Backup RADIUS Server Configuration with Termination Enabled .....	18
AP Zone Configuration .....	19
Authentication Survivability with EAP-TLS .....	19
Support for 128 ACL Rules .....	19
Configurable Port for Communication between AirWave Management Server and IAP .....	19
Disabling of Bridging and Routing Traffic between Clients Connected to an SSID .....	20
NTP Server Configuration Options .....	20
Change in Extended SSID Factory Default Settings .....	20
Support for Read-Only Users to Access CLI .....	20
Enhancement to the Client Match Maximum Threshold Limit .....	20
Regulatory Updates .....	20
Reintroducing IAP-92/93 in Aruba Instant 6.4.0.3-4.1.0.1 and future 6.4.x.x-4.1.x.x releases .....	20
<b>Known Issues and Limitations in Previous Releases .....</b>	<b>23</b>
No Support for IAP-92/93 .....	23
Known Issues .....	23
AirWave .....	23
General .....	23
3G/4G Uplink Management .....	23
Application Classification .....	23

Aruba Instant 6.4.0.x-4.1.0.2 is a software patch release that introduces enhancements and fixes to the issues found in the previous releases.

For more information, see the *Aruba Instant 6.4.0.2-4.1 User Guide*

## Contents

- [What's New in this Release on page 6](#) describes the enhancements and fixed issues introduced in this release.
- [Features and Enhancement in Previous Release.htm](#) describes the features and enhancements introduced in previous releases.
- [Known\\_Issues\\_in\\_Previous\\_Releases.htm](#) lists the known issues and limitations identified in previous releases

## Contacting Support

Main Site	<a href="http://arubanetworks.com">arubanetworks.com</a>
Support Site	<a href="http://support.arubanetworks.com">support.arubanetworks.com</a>
Airheads Social Forums and Knowledge Base	<a href="http://community.arubanetworks.com">community.arubanetworks.com</a>
North American Telephone	1-800-943-4526 (Toll Free) 1-408-754-1200
International Telephones	<a href="http://www.arubanetworks.com/support-services/support-program/contact-support">http://www.arubanetworks.com/support-services/support-program/contact-support</a>
Software Licensing Site	<a href="http://licensing.arubanetworks.com/login.php">licensing.arubanetworks.com/login.php</a>
End of Support Information	<a href="http://www.arubanetworks.com/support-services/end-of-life-products/end-of-life-policy/">http://www.arubanetworks.com/support-services/end-of-life-products/end-of-life-policy/</a>
Security Incident Response Team (SIRT)	<a href="http://www.arubanetworks.com/support-services/security-bulletins/">http://www.arubanetworks.com/support-services/security-bulletins/</a>
<b>Support Email Addresses</b>	
Americas, EMEA, and APAC	<a href="mailto:support@arubanetworks.com">support@arubanetworks.com</a>
SIRT Email Please email details of any security problem found in an Aruba product.	<a href="mailto:sirt@arubanetworks.com">sirt@arubanetworks.com</a>

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

### Enhancements

There are no enhancements introduced in this current release.

### Resolved Issues in this Release

The following issues are fixed in this patch release.

#### AirGroup

**Table 1:** *AirGroup Fixed Issue*

Bug ID	Description
104037	<p><b>Symptom:</b> AirGroup was unable to maintain the record cache of the servers connected to the IAP cluster in the network. This issue is resolved by implementing a fix to maintain the record cache.</p> <p><b>Scenario:</b> This issue occurred when the AirGroup servers were roaming from one IAP to another in the cluster. This issue was not limited to a specific IAP model or Instant release version.</p>

#### Authentication

**Table 2:** *Authentication Fixed Issues*

Bug ID	Description
103899	<p><b>Symptom:</b> Clients were unable to connect to the slave IAPs when the WPA-passphrase used to connect to the slave IAP contained a space. This issue is resolved by making a code level change.</p> <p><b>Scenario:</b> This issue occurred when a space was included in the WPA2-PSK passphrase for the slave IAP. This issue was observed on all platforms running Aruba Instant 6.3.1.4-4.0.0.5 release and later versions.</p>

#### ARM

**Table 3:** *ARM Portal Fixed Issue*

Bug ID	Description
104127	<p><b>Symptom:</b> Users were experiencing voice call issues when a SIP phone was connected to IAP-225. This issue is resolved by making a code level change to increase the voice aware scan rejects counter during voice calls.</p> <p><b>Scenario:</b> This issue occurred when scanning was enabled on IAP-225 running Instant 6.4.0.2-4.1.0.0 release and later versions.</p>
103674	<p><b>Symptom:</b> Performance of 2.4G band legacy traffic was poor from the IAP towards the client. The IAP was configured to a very high max_distance by default, to allow the RF signal transmitted as far as 6400 meters away, at the cost of low performance. This issue is resolved by changing the default value to 600 meters, which is the common case for ordinary client accessing.</p> <p><b>Scenario:</b> This issue occurred when the legacy client was connected to the IAP at 2.4G band. This issue was observed in IAP-9x, IAP-1xx, RAP3, and RAP5 platforms running Instant 6.3.1.1-4.0.0.0 and later versions.</p>

## DHCP Server

**Table 4:** *DHCP Server Fixed Issue*

Bug ID	Description
102989	<p><b>Symptom:</b> Exclude IP address range in DHCP profile configuration was not taking effect. This issue is resolved by making a code level change.</p> <p><b>Scenario:</b> This issue occurred when the Exclude IP address functionality was broken after the set of configurations from the config manager were not applied correctly to the DHCP Server process. This issue was observed on all IAPs running Aruba Instant 6.4.0.2-4.1.0.0 and later versions.</p>

## User Interface

**Table 5:** *User Interface Fixed Issue*

Bug ID	Description
104466	<p><b>Symptom:</b> IAP User Interface session remained connected even after the password was changed in another CLI/UI session. This issue is resolved by making a code level change to disconnect the UI/CLI session logged in using the old password.</p> <p><b>Scenario:</b> This issue occurred when a change was made to the admin, read-only, or guest accounts for management user accounts. This issue was observed on all IAPs running Instant 6.4.0.3-4.1.0.1 release.</p>

## VC Management

**Table 6:** *VC Management Fixed Issue*

Bug ID	Description
103539	<p><b>Symptom:</b> Some users were getting warning messages that read "CLI module is running in a degraded state. Some commands will not function", when they were trying to access the CLI mode.</p> <p><b>Scenario:</b> This issue occurred when the external RADIUS server was unavailable for authentication to the management account users. This issue was observed on all IAPs running Aruba Instant 6.4.0.3-4.1.0.1 release.</p>
102523	<p><b>Symptom:</b> IAP-105 with mac-prefix D8C7C8C was unable to join the IAP cluster after an upgrade to either the 6.2.x or 6.3.x versions. This issue is resolved by making a code level change to enable the IAP to join the cluster after the upgrade.</p> <p><b>Scenario:</b> This issue occurred when IAP-105 with mac-prefix D8C7C8C was upgraded from a 6.1.x version to a 6.2.x or higher version.</p>

## VPN

**Table 7:** *VPN Fixed Issue*

Bug ID	Description
105416	<p><b>Symptom:</b> Motorola scanners were taking longer than the expected time to connect to the network. This issue is resolved by making a code level change to prevent the IAP from sending de-authentication responses in between authentication requests.</p> <p><b>Scenario:</b> This issue occurred when the IAP began sending de-authentication responses in between authentication requests. This issue was observed on IAP-135 running Aruba Instant 6.3.1.2-4.0.0.4 release and later versions.</p>

## Known Issues

This section describes the known issues identified in this patch release.

### Authentication

**Table 8:** *Authentication Known Issue*

Bug ID	Description
106047	<p><b>Symptom:</b> Wired client is not displayed in AirWave Management Platform and shows an MIB_ETHERNET_TABLE error.</p> <p><b>Scenario:</b> This issue occurs when the IAP has multiple ethernet interfaces and the MAC address of the devices is set as FE or FF. This issue is observed on all IAPs running Instant 6.4.0.2-4.1.0.0 release and earlier versions.</p> <p><b>Workaround:</b> None.</p>



## Resolved Issues in 6.4.0.2-4.1.0.1 release

The following issues are fixed in this patch release.

### AirWave

**Table 9:** *AirWave Fixed Issue*

Bug ID	Description
104037	<p><b>Symptom:</b> IAP was broadcasting the previous Instant SSID, even after receiving the latest configuration from AirWave. This issue is resolved by introducing a fix to handle the packet loss issue between the Virtual Controller and the Slave IAP.</p> <p><b>Scenario:</b> This issue occurred when there was packet loss in the L2 wired network to which the IAP is connected. This issue was observed on all IAP models running Instant 6.3.1.1-4.0.0.0 release and earlier versions.</p>

### Authentication

**Table 10:** *Authentication Fixed Issues*

Bug ID	Description
101378	<p><b>Symptom:</b> 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.</p> <p><b>Scenario:</b> This issue occurred when the client attempted to re-authenticate on the IAP. This issue was not limited to a specific IAP model or Instant release version.</p>
103441	<p><b>Symptom:</b> Users were unable to login to the IAP cluster when the RADIUS server IP was set as 0.0.0.0. This issue is resolved by making a code level change to accept 0.0.0.0 as the RADIUS server IP address.</p> <p><b>Scenario:</b> This issue occurred when the IAP was unable to send RADIUS request to the admin server and failed to fall back to the internal server. This issue was observed in all IAP models running Instant 6.3.1.2-4.0.0.4 release.</p>
101614	<p><b>Symptom:</b> During an 802.1x authentication, the calling-station-id was incorrectly displayed as 5A:00:00:00:00:00. This issue is resolved by using the correct calling-station-id during 802.1x authentication.</p> <p><b>Scenario:</b> This issue was not limited to a specific IAP model or Instant release version.</p>
100843	<p><b>Symptom:</b> IAP used MAC address as the username during MAC authentication. This issue is resolved by providing RADIUS attribute username as the client username during MAC authentication.</p> <p><b>Scenario:</b> This issue was not limited to a specific IAP model or Instant release version.</p>

### Captive Portal

**Table 11:** *Captive Portal Fixed Issue*

Bug ID	Description
99229	<p><b>Symptom:</b> 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.</p> <p><b>Scenario:</b> This issue was not limited to a specific IAP model or Instant release version.</p>

## Datapath

**Table 12: Datapath Fixed Issue**

Bug ID	Description
101274	<b>Symptom:</b> Prioritization of voice or video calls did not work for Lync when the classify media option was enabled. This issue is resolved after making a minor change to the code. <b>Scenario:</b> This issue was observed in all IAP models running Instant6.4.0.2-4.1.0.0 release.
103898	<b>Symptom:</b> A crash was observed in IAP-135 when multiple clients were connected. Upgrading to Aruba Instant 6.4.0.3-4.1.0.1 resolves the issue. <b>Scenario:</b> This issue was observed when DMO was enabled on IAP-135 running Instant6.4.0.2-4.1.0.0 release.

## RAP-NG

**Table 13: RAP-NG Fixed Issue**

Bug ID	Description
102327	<b>Symptom:</b> IAP was unable to send Syslog messages, when VPN connectivity comes online and changes the route to Syslog server, This issue is resolved by recreating the session. <b>Scenario:</b> This issue was not limited to a specific IAP model or Instant release version.

## STM

**Table 14: STM Fixed Issue**

Bug ID	Description
101708	<b>Symptom:</b> IAP reported incorrect client OS type for Blackberry® Z10 device. This issue is resolved after making a minor change to the code. <b>Scenario:</b> This issue occurred when the IAP missed the user agent of the Blackberry Z10 device. This issue was not limited to a specific IAP model or Instant release version.

## VPN

**Table 15: VPN Fixed Issue**

Bug ID	Description
103838	<b>Symptom:</b> IAP register message did not reach the controller due to a low buffer size. The issue is resolved by increasing the buffer size. <b>Scenario:</b> This issue was observed on an IAPs running Instant6.4.0.2-4.1.0.0 release when a VPN tunnel was established with the controller.

## Wireless

**Table 16:** *Wireless Fixed Issues*

Bug ID	Description
99833	<p><b>Symptom:</b> When more than 120 customers were connected in the bridge mode, broadcast packets were dropped and customers lost connectivity. This fix ensures that the broadcast packet handling is modified to resolve the issue.</p> <p><b>Scenario:</b> This issue was observed when the frequency of customers trying to connect to the IAPs was high. This issue was observed in IAP-225 running Instant 6.3.1.2-4.0.0.x releases.</p>
94482	<p><b>Symptom:</b> AnIAP crashed due to an internal Watchdog timeout. This issue is resolved by reducing the wait time, and rebooting the IAP to recover from that state.</p> <p><b>Scenario:</b> This issue occurred within one of the reset functions in the Ethernet driver where there was a long wait, which exceeded the watchdog timeout, causing IAP failure. This issue was observed in IAP-225 running Instant 6.4.0.0-4.0.0.x releases.</p>



This chapter provides information on the features and enhancements introduced in the previous 6.4.0.2-4.1.0.0 and 6.4.0.2-4.1.0.x releases of Aruba Instant.

## Features and Enhancements

The following features and enhancements were introduced in the Instant 6.4.0.2-4.1.0.0 and later releases.

### AppRF

Starting with 6.4.0.2-4.1.0.0, Instant supports AppRF comprising of two feature sets: On-board Deep Packet Inspection (DPI) and cloud-based Web Policy Enforcement (WPE).

1. **Deep packet inspection:** IAPs with DPI capability can analyze data packets to identify the applications in use and allow you to create ACL rules to determine client access. The on-board firewall of the IAP performs the DPI function.
  - **Access control based on application and application category:** You can create firewall policies based on types of applications and application categories. You can also define traffic shaping policies such as bandwidth control and QoS per application. For example, you can block bandwidth monopolizing applications on a guest role within an enterprise.
2. **Web Policy Enforcement:** In case of WPE, the IAP performs lookups against cloud-hosted services. This feature requires an annual per IAP subscription. Please contact the Aruba Instant sales team.
  - **Access control based on web-category and web-reputation:** You can create a firewall policy to allow or deny access based on a predefined list of website categories and reputation score. For example, if you block the **web-based-email** category, clients who are assigned this policy will not be able to visit email-based websites such as mail.yahoo.com.

**Application visibility:** When **AppRF visibility** is enabled in the **System** window in the UI or through the **dpi** command in the CLI, the **AppRF** link appears in the UI when selecting an IAP from the main window. When clicked, the **AppRF** link displays the application traffic summary for IAPs and client devices. The AppRF dashboard presents four different graphs with a traffic mix based on **application**, **application category**, **web-category**, and **web-reputation**. Clicking on each category displays client traffic data in real-time or the usage trend in the last 15 minutes.

Based on the AppRF classification of an application, the IAP can enforce multiple actions including blocking, QoS enforcement, throttling and so on.



---

The AppRF features are not supported on the IAP-92/93 platform.

---

---

The access rule configuration and charts for application and application category are not supported on IAP-104/105, IAP-134/135, and RAP-3WN/3WNP platforms. Only the web category charts are displayed for these IAP models.

---

For more information on DPI and AppRF, see:

- *Deep Packet Inspection and Application Visibility* in the *Aruba Instant 6.4.0.2-4.1 User Guide*
- The **dpi**, **show dpi**, **show dpi-stats**, and **wlan access-rule** commands in the *Aruba Instant 6.4.0.2-4.1 CLI Reference Guide*

## AirGroup Enhancements

Starting with 6.4.0.2-4.1.0.0, Instant supports Universal Plug and Play (UPnP) and DLNA (Digital Living Network Alliance) enabled devices. DLNA is a network standard derived from UPnP, which enables devices to discover the services available in a network. DLNA also provides the ability to share data between the Windows or Android based multimedia devices. All the features and policies applicable to mDNS are extended to DLNA to ensure full interoperability between compliant devices.

With DLNA support, the following services are available for the IAP clients:

- DLNA Media—Applications such as Windows Media Player use this service to browse and play media content on a remote device.
- DLNA Print—This service is used by printers that support DLNA.

For more information on DLNA and how to enable DLNA services, see:

- *Configuring AirGroup and AirGroup Services on an IAP* in the *Aruba Instant 6.4.0.2-4.1 User Guide*
- The **airgroup**, **airgroupservice**, and **show aigroup** commands in the *Aruba Instant 6.4.0.2-4.1 CLI Reference Guide*

## Support for New Access Points

This release adds Instant support for IAP-270 series and IAP-103 devices.

- The IAP-270 series (IAP-274 and IAP-275) are environmentally hardened, outdoor rated, dual-radio IEEE 802.11ac wireless access points. These access points use MIMO (Multiple-Input, Multiple-Output) technology and other high-throughput mode techniques to deliver high-performance, 802.11ac 2.4 GHz and 5 GHz functionality while simultaneously supporting existing 802.11a/b/g/n wireless services.
- The IAP-103 wireless access point supports the IEEE 802.11n standard for high-performance WLAN. This access point uses MIMO (Multiple-Input, Multiple-Output) technology and other high-throughput mode techniques to deliver high performance, 802.11n 2.4 GHz or 5 GHz functionality while simultaneously supporting existing 802.11a/b/g wireless services.

For more information about these products, visit [www.arubanetworks.com](http://www.arubanetworks.com).

## Configurable DSCP Mapping Values for WMM Access Categories

Starting with 6.4.0.2-4.1.0.0, Instant supports customization of Wi-Fi Multimedia to DSCP mapping configuration for upstream (client to IAP) and downstream (IAP to client) traffic.

DSCP classifies packets based on network policies and rules. You can customize the mapping values between WMM ACs and DSCP tags to prioritize various traffic types and apply these changes to a WMM-enabled SSID profile. When WMM AC mappings values are configured, all packets received are matched against the entries in the mapping table and prioritized accordingly.

The following table shows the default WMM AC to DSCP decimal mappings and the recommended WMM AC to DSCP mappings.

**Table 17: Default WMM-DSCP Mapping**

DSCP Decimal Value	WMM Access Category
8	Background
16	
0	Best effort
24	
32	Video
40	
48	Voice
56	

For more information on configuring DSCP mapping values, see:

- *Wi-Fi Multimedia Traffic Management* in the *Aruba Instant 6.4.0.2-4.1 User Guide*
- The **wlan ssid-profile** command in the *Aruba Instant 6.4.0.2-4.1 CLI Reference Guide*

## Console Access to IAP

You can allow or restrict access to an IAP console through the serial port by using the UI or CLI. By default, the console access to an IAP is enabled.

To disable console access to an IAP:

- In the UI, navigate to **System >General >Show advanced options** and select **Disabled** from the **Console access** drop-down..
- In the CLI, run the following commands:

```
(Instant AP) (config)# console
(Instant AP) (console)#
```

## Instant UI Changes

Starting with Instant 6.4.0.2-4.1.0.0 release, the **DHCP** tab for configuring a default DHCP scope for Virtual Controller managed networks is no longer available in the **System** window of the Instant UI. The default DHCP scope configuration options are now available in the **DHCP Server** window. To open the **DHCP Server** window, go to **More >DHCP Server**.

The **VLAN** tab of the WLAN SSID configuration wizard now allows you create a customized DHCP scope to configure a Virtual Controller managed IP and VLAN assignment mode. On selecting the **Virtual Controller managed** option for **Client IP assignment**, the following client VLAN assignment options are displayed:

- **Default:** When selected, the default VLAN as determined by the Virtual Controller is assigned for clients.
- **Custom:** On selecting this, you can either select an existing DHCP scope or create a new DHCP scope by clicking **New**.

For more information, see the following in the *Aruba Instant 6.4.0.2-4.1 User Guide*:

- *Configuring VLAN Settings for a WLAN SSID Profile*
- *DHCP Configuration*

## Full Tunnel-Mode VPN Configuration

Starting with Instant 6.4.0.2-4.1.0.0 release, you can disable split-tunnel configuration for the centralized, L2 subnets. When split-tunnel is enabled, a VPN user can access a public network and a local LAN or WAN network at the same time through the same physical network connection. By default, the split-tunnel function is enabled for all centralized, L2 DHCP profiles.

When split-tunnel is disabled, all the traffic including the corporate and Internet traffic is tunneled irrespective of the routing profile specifications. If the GRE tunnel is down and when the corporate network is not reachable, the client traffic is dropped.

For more information on disabling split-tunnel, see:

- *Configuring Centralized DHCP Scope* in the *Aruba Instant 6.4.0.2-4.1 User Guide*
- The **ip dhcp** command in the *Aruba Instant 6.4.0.2-4.1 CLI Reference Guide*

## Inbound Firewall

Starting with Instant 6.4.0.2-4.1.0.0 release, you can configure firewall rules for the inbound traffic coming through the uplink ports of an IAP. The rules defined for the inbound traffic are applied if the destination is not a user connected to the IAP. If the destination already has a user role assigned, the user role overrides the actions or options specified in inbound firewall configuration. However, if a deny rule is defined for the inbound traffic, it is applied irrespective of the destination and user role. Unlike the ACL rules in a WLAN SSID or wired profile, the inbound firewall rules can be configured based on the source subnet.

---

For all subnets, a deny rule is created by default as the last rule. If at least one rule is configured, the deny all rule is applied to the upstream traffic by default.

---



---

Management access to the AP is allowed irrespective of the inbound firewall rule. For more information on configuring restricted management access, see *Configuring Management Subnets* in *Aruba Instant 6.4.0.2-4.1 User Guide*.

---

---

The inbound firewall is not applied to traffic coming through GRE tunnel.

---

For more information, see:

- *Configuring Inbound Firewall Rules* in the *Aruba Instant 6.4.0.2-4.1 User Guide*
- The **inbound-firewall** and **show inbound-firewall-rules** commands in the *Aruba Instant 6.4.0.2-4.1 CLI Reference Guide*

## Fast Roaming Enhancements

Starting with 6.4.0.2-4.1.0.0, Instant supports 802.11k (Radio Resource Management) and 802.11v (BSS Transition Management) standards to improve Quality of Service (QoS) and seamless connectivity.

The 802.11k protocol provides mechanisms for APs and clients to dynamically measure the available radio resources and enables stations to query and manage their radio resources. In an 802.11k enabled network, APs and clients can share radio and link measurement information, neighbor reports, and beacon reports with each other. This allows the WLAN network infrastructural elements and clients to assess resources and make optimal mobility decisions to ensure Quality of Service (QoS) and seamless continuity.



---

Ensure that the client match feature is enabled to allow AP and clients to exchange neighbor reports.

---



The 802.11v standard provides Wireless Network Management enhancements to the IEEE 802.11 MAC and PHY. It extends radio measurements to define mechanisms for wireless network management of stations including BSS transition management. IAPs support the generation of the BSS transition management request frames to the 802.11k clients when a suitable AP is identified for a client through client match.

For information on configuring a WLAN SSID for 802.11k and 802.11v support, see:

- *Configuring Fast Roaming for Wireless Clients* in the *Aruba Instant 6.4.0.2-4.1 User Guide*
- The **wlan ssid-profile** command in the *Aruba Instant 6.4.0.2-4.1 CLI Reference Guide*

## Support for 4G Modems

Instant 6.4.0.2-4.1.0.0 adds support for the following 4G modems:

- Netgear Aircard 341u
- Pantech UML295
- Franklin Wireless u770
- Huawei 3276s-150

For information on configuring modems to enable 3G or 4G uplink, see:

- *Cellular Uplink* in the *Aruba Instant 6.4.0.2-4.1 User Guide*
- The **cellular-uplink-profile** command in the *Aruba Instant 6.4.0.2-4.1 CLI Reference Guide*

## Client Match Enhancements

Starting with Instant 6.4.0.2-4.1.0.0 release, apart from dynamic load balancing, sticky clients, and band steering, the following conditions trigger client match to allow the clients to be moved from one AP to another for better performance.

- **Channel Utilization:** Based on the percentage of channel utilization, clients are steered from a busy channel to an idle channel..
- **Client Capability Match:** Based on the client capability match, clients are steered to appropriate channel, for example HT20, HT40, or VHT80.

If client match is enabled, you can also view a graphical representation of the radio map of an AP and the client distribution on an AP radio.

- On clicking an access point in the **Access Points** tab and the **Client Match** link, a stations map view is displayed and a graph is drawn with real-time data points for the AP radio. If the AP supports dual band, you can toggle between 2.4GHz and 5 GHz links in the client match graph area to view the data. When you hover the mouse on the graph, details such as RSSI, client match status, and the client distribution on channels are displayed.
- On clicking a client in the **Clients** tab and the **Client Match** link, a graph is drawn with real-time data points for an AP radio map. When you hover the mouse on the graph, details such as RSSI, channel utilization details, and client count on each channel are displayed.

For more information on client match configuration and visualization, see the *Aruba Instant 6.4.0.2-4.1 User Guide*.

## Sourcing Virtual Controller Traps from the Virtual Controller IP

Starting with Instant 6.4.0.2-4.1.0.0 release, if the Virtual Controller IP is configured, the traps are generated from the Virtual Controller IP. However, the source IP address for the interface up and interface down traps is the AP IP address.

The **sysObject** OID object is enhanced to return information on Virtual Controller. Generally, the **sysObjectID** returns OIDs for a specific model number of the device within the IAP product family. When an SNMP query is performed for this object on an AP IP address (either master IAP or slave IAP IP address), information on AP type is retrieved. However, if the query is performed on a Virtual Controller IP address, information on the IAP acting as the Virtual Controller is displayed.

For example, if an IAP-135 is the master IAP, a query on this IAP returns the iso.org.dod.internet.private.enterprise.aruba.products.apProducts.ap135 (1.3.6.1.4.1.14823.1.2.48) result. Similarly, a query on the Virtual Controller IP returns the OID details with **iapvc**.

For more information on SNMP traps and MIB objects, see *Aruba Instant 6.4.0.2-4.1 MIB Reference Guide*.

## Support for TACACS+ Servers

In Instant 6.4.0.2-4.1.0.0 release, a new external server is added to support authentication and accounting privileges for management users. The users can create several TACACS+ server profiles, out of which one or two of the servers can be specified to authenticate management users.

If two TACACS+ servers are configured as authentication servers, the users can use them as primary and backup servers or in the load balancing mode.

TACACS+ servers can also be used along with RADIUS servers. For example, you can use a TACACS server as the primary server and a RADIUS server as the backup server. IAPs also support the TACACS+ accounting feature that reports management commands to TACACS+ servers through console port, Telnet, SSH, web, and Cloud,



---

The TACACS+ accounting option is available only if one of the specified servers is a TACACS+ server.

---

For more information on TACACS+ Server and TACACS+ accounting, see:

- *Supported Authentication Servers, Configuring an External Server for Authentication* in the *Aruba Instant 6.4.0.2-4.1 User Guide*.
- The **wlan tacacs-server**, **show tacacs server**, and **mgmt-accounting** commands in the *Aruba Instant 6.4.0.2-4.1 CLI Reference Guide*.

## Integration with an XML API Interface

Starting with Instant 6.4.0.2-4.1.0.0 release, IAPs can be integrated with an XML API Interface by sending specific XML commands to the IAP from an external server. These commands can be used to add, delete, authenticate, query, or blacklist a user or a client.

For more information on XML API, see:

- *Integrating an IAP with an XML API interface* in the *Aruba Instant 6.4.0.2-4.1 User Guide*.
- The **xml-api-server**, **show xml-api-server** commands in the *Aruba Instant 6.4.0.2-4.1 CLI Reference Guide*.

## Backup RADIUS Server Configuration with Termination Enabled

By default, for 802.1X authorization, the client conducts an EAP exchange with the RADIUS server, and the AP acts as a relay for this exchange. When **Termination** is enabled, the IAP by itself acts as an authentication server and terminates the outer layers of the EAP protocol, only relaying the innermost layer to the external RADIUS server. You can now configure two RADIUS servers for a WLAN SSID when EAP termination is enabled and use these servers in the primary and backup mode.

For more information, see *Configuring 802.1X Authentication for a Wireless Network Profile* in the *Aruba Instant 6.4.0.2-4.1 User Guide*.

## AP Zone Configuration

Starting with 6.4.0.2-4.1.0.0 release, you can configure zone settings for an IAP. The same zone information can be configured on a WLAN SSID, so that the SSID can be broadcast on the IAP.

The following constraints apply to the AP zone configuration:

- An IAP can belong to only one zone and only one zone can be configured on an SSID.
- If an SSID belongs to a zone, all IAPs in this zone can broadcast this SSID. If no IAP belongs to the zone configured on the SSID, the SSID is not broadcast.
- If an SSID does not belong to any zone, all IAPs can broadcast this SSID.

For information on configuring an AP zone, see:

- *Configuring Zone Settings on an IAP and Configuring WLAN Settings for an SSID Profile* in the *Aruba Instant 6.4.0.2-4.1 User Guide*
- The **zonename** and **wlan ssid-profile** commands in the *Aruba Instant 6.4.0.2-4.1 CLI Reference Guide*

## Authentication Survivability with EAP-TLS

In Instant 6.4.0.2-4.1.0.0 release, the authentication survivability feature is enhanced to support EAP-TLS authentication protocol. The authentication survivability feature supports a survivable authentication framework against the remote link failure when working with the external authentication servers. When enabled, this feature allows the IAPs to authenticate the previously connected clients against the cached credentials if the connection to the authentication server is temporarily lost.



---

For EAP-PEAP authentication, ensure that the CPPM 6.0.2 or later version is used for authentication. For EAP-TLS authentication, any external or third-party server can be used.

---

For EAP-TLS authentication, ensure that the server and CA certificates from the authentication servers are uploaded on IAP. For more information, see *Uploading Certificates* in *Aruba Instant 6.4.0.2-4.1 User Guide*.

---

The **show auth-survivability** command is also enhanced to display debug logs for troubleshooting issues. For more information, see:

- *Support for Authentication Survivability* in the *Aruba Instant 6.4.0.2-4.1 User Guide*.
- The **show auth-survivability** command in the *Aruba Instant 6.4.0.2-4.1 CLI Reference Guide*

## Support for 128 ACL Rules

Starting with Instant 6.4.0.2-4.1.0.0 release, you can now configure up to 128 ACL rules for a wired or wireless profile through the WLAN wizard or wired user role through the UI and CLI.

- To configure ACL rules for an SSID or wired port profile role in the CLI, use the **wlan access-rule** command.
- To configure ACL rules in the UI, navigate to **Security > Roles**. Select the role and click **New** under **Access Rules**.

## Configurable Port for Communication between AirWave Management Server and IAP

Starting with Instant 6.4.0.2-4.1.0.0 release, you can now customize the port number of the AirWave management server through the `server_host:server_port` format.

For more information on managing an IAP through AirWave, see *Managing IAP from AirWave* in *Aruba Instant 6.4.0.2-4.1 User Guide*.

## Disabling of Bridging and Routing Traffic between Clients Connected to an SSID

Starting with Instant 6.4.0.2-4.1.0.0, you can now disable bridging and routing traffic between two clients connected to an SSID. When inter-user bridging and local routing is denied, the clients can connect to the Internet but cannot communicate with each other, and the bridging and routing traffic between the clients is sent to the upstream device to make the forwarding decision.

To deny inter-user bridging and local routing for the WLAN SSID clients, run the following commands at the CLI:

```
(Instant AP) (config)# wlan ssid-profile <ssid-profile>
(Instant AP) (SSID Profile <ssid-profile>)# deny-inter-user-bridging
(Instant AP) (SSID Profile <ssid-profile>)# deny-local-routing
(Instant AP) (SSID Profile <ssid-profile>)# end
(Instant AP)# commit apply
```

## NTP Server Configuration Options

The Network Time Protocol (NTP) helps obtain the precise time from a server and regulate the local time in each network element. Connectivity to a valid NTP server is required to synchronize the IAP clock to set the correct time. If NTP server is not configured in the IAP network, an IAP reboot may lead to variation in time data.

By default, the IAP tries to connect to **pool.ntp.org** to synchronize time. A different NTP server can be configured either from the UI or from management platforms such as Central. It can also be provisioned through the DHCP option 42. If the NTP server is configured, it takes precedence over the DHCP option 42 provisioned value. The NTP server provisioned through the DHCP option 42 is used if no server is configured. The default server pool.ntp.org is used if no NTP server is configured or provisioned through DHCP option 42.

## Change in Extended SSID Factory Default Settings

Starting with Instant 6.4.0.2-4.1.0.0 release, extended SSID is enabled by default in the factory default settings of Instant APs. This disables mesh in the factory default settings.

## Support for Read-Only Users to Access CLI

Starting with Instant 6.4.0.2-4.1.0.0 release, read-only users can access the IAP CLI through telnet, SSH, or console.

## Enhancement to the Client Match Maximum Threshold Limit

Starting with Instant 6.4.0.2-4.1.0.0 release, the maximum threshold limit for Client Match is set to 255. The previous maximum threshold value was 20.

## Regulatory Updates

**Table 18:** *Regulatory Domain Updates*

Regulatory Domain	Description
Mexico	Support for all shipping IAPs.
Australia, New Zealand, and Canada	Support for IAP-275 platform.
Australia and New Zealand	Support for IAP-103 platform.

## Reintroducing IAP-92/93 in Aruba Instant6.4.0.3-4.1.0.1 and future 6.4.x.x-4.1.x.x releases

Support for IAP-92/93 is reintroduced in this Instant release and will continue in future 6.4.x.x-4.1.x.x releases. However, the following features are no longer available for IAP-92/93 starting from this release:

- AirGroup
- Internal RADIUS server for 802.1x authentication
- EAP Termination
- Authentication Survivability
- LLDP integration

The features listed above may be configured through Instant CLI/Web UI and AirWave Management Platform, but will have no effect on IAP-92/93. In a cluster running Instant 6.4.x.x-4.1.x.x, only IAP-92/93 will have the above limitations.

In order to conserve memory, IAP-92/93 is now restricted to a single active CLI session, either through a console, SSH, or telnet. An error message "**All CLI sessions are in use**" is displayed if the user attempts to open multiple sessions.



This chapter describes the known issues identified in the previous 6.4.0.2-4.1.0.0 release of Aruba Instant.

### No Support for IAP-92/93

In Instant 6.4.0.2-4.1.0.0, IAP-92/93 devices are not supported.



Do not to upgrade an Instant network running IAP-92/93 platforms to Instant 6.4.0.2-4.1.0.0. In case of an accidental upgrade, downgrade to 6.3.1.1-4.0 release is possible without losing the existing configuration. IAP-92/93 will again be supported in future patch releases (6.4.0.2-4.1.0.x) but with reduced functionality. Instant 6.4.0.2-4.1 is the last code branch to support the IAP-92/93 platforms.

### Known Issues

#### AirWave

**Table 19:** *AirWave Known Issue*

Bug ID	Description
101945	<p><b>Symptom:</b> Image sync fails when AirWave Management Platform (AMP) uses user-defined ports with Master IAPs and Slave IAPs.</p> <p><b>Scenario:</b> This issue occurs when the Master AP type is different from the Slave AP type and the Master IAP image is different from the Slave IAP image. This issue is observed in IAPs running Instant 6.4.0.2-4.1.0.0 release.</p> <p><b>Workaround:</b> None</p>

#### General

**Table 20:** *General Known Issue*

Bug ID	Description
98455	<p><b>Symptom:</b> The Speed or Duplex configuration change of Ethernet Port does not take effect on Instant APs.</p> <p><b>Scenario:</b> This issue is observed in IAPs running Instant 6.2.0.0-3.3 or later releases.</p> <p><b>Workaround:</b> Reboot the IAP.</p>

#### 3G/4G Uplink Management

**Table 21:** *3G/4G Uplink Management Known Issue*

Bug ID	Description
98775	<p><b>Symptom:</b> Sometimes, the USB modem connected to RAP-108 and RAP-3WN is not functional as the 3G and 4G interfaces fail to come up.</p> <p><b>Scenario:</b> This issue is observed in RAP-108 and RAP-3WN running Instant 6.2.0.0-3.3 or later.</p> <p><b>Workaround:</b> Disconnect and reconnect the USB modem.</p>

#### Application Classification

The following is a list of popular applications with expected classification behavior:

**Table 22: Application Classification Known Issue**

Bug ID	Description
<b>Lync</b>	Due to the adaptive nature of Lync, a few sessions might occasionally be wrongly classified.
<b>Skype</b>	<ul style="list-style-type: none"><li>• If user has already logged into Skype or has the previous login session cached, classification might fail, enabling the user to login to Skype even when there is an application rule to deny Skype.</li><li>• Due to the adaptive nature of Skype, voice and video calls might not be wrongly classified at times, affecting bandwidth throttling and enforcement.</li></ul>
<b>Speedtest.net</b>	In certain geographical locations, speedtest.net uses an alternate port (TCP 8080) for the actual data test which can lead to classification failures.
<b>Tor Browser</b>	Proxying through Tor using proxy configuration or using the packaged Tor Browser does not get classified.
<b>Carbonite</b>	Carbonite application classification does not function as expected.
<b>Google Drive</b>	Google drive application is part of the Google Docs application suite. This needs to be enabled to classify google drive.