Aruba Instant 6.4.3.1-4.2.0.2

Release Notes

aruba®
NETWORKS
an HP company

Open Source Code

This product includes code licensed under the GNU General Public License, the GNU Lesser General Public License, and/or certain other open source licenses. A complete machine-readable copy of the source code corresponding to such code is available upon request. This offer is valid to anyone in receipt of this information and shall expire three years following the date of the final distribution of this product version by Hewlett-Packard Company. To obtain such source code, send a check or money order in the amount of US $10.00 to:

Hewlett-Packard Company

Attn: General Counsel

3000 Hanover Street

Palo Alto, CA 94304

USA

Please specify the product and version for which you are requesting source code. You may also request a copy of this source code free of charge at dl-gplquery@arubanetworks.com.

Aruba Instant 6.4.3.1-4.2.0.2 is a patch release that includes fixes to the issues found in the previous releases.

For information on upgrading IAPs to the new release version, refer to the *Upgrading an IAP* topic in the *Aruba Instant 6.4.3.1-4.2 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	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 lists the enhancements and the issues fixed in this release of Aruba Instant.

Regulatory Domain Updates

The following table lists the DRT file versions supported by Instant 6.4.3.x-4.2.x.x releases:

Table 1: *DRT Versions*

Instant Release Version	Applicable DRT Version
6.4.3.1-4.2.0.2	1.0_51997
6.4.3.1-4.2.0.1	1.0_51685
6.4.3.1-4.2.0.0	1.0_50970

For a complete list of countries certified with different AP models, see the respective DRT release notes at support.arubanetworks.com.

Resolved Issues in this Release

The following issues are fixed in the Instant 6.4.3.1-4.2.0.2 release.

Datapath/Firewall

Table 2: *Datapath/Firewall Fixed Issue*

Bug ID	Description
126190	**Symptom**: The ACL roles applied on the SSID were not functioning as expected, when the wired and wireless profiles were both assigned the same pre-authentication role and multiple Local DHCP scopes were configured on the IAP. This issue is resolved by making a change in the IAP code to increase the buffer for ACL entries. **Scenario**: This issue was not limited to a specific IAP model and was observed in IAPs running Instant 6.4.3.1-4.2 release.

VPN

Table 3: *VPN Fixed Issue*

Bug ID	Description
124993	**Symptom**: An IAP was unable to connect to the Airwave Management Server after receiving the controller and server configuration from the Provisioning Airwave Server. An issue with the VPN tunnel state machine caused the IAP to use an incorrect inner IP address to connect to the AMP server. The fix ensures that the IAP uses the correct inner IP address to connect to the AMP server. **Scenario**: This issue was not limited to a specific IAP model or software version.

This chapter describes the issues fixed in the 6.4.3.x-4.2.x.x releases of Aruba Instant.

Issues Resolved in 6.4.3.1-4.2.0.1

AppRF

Table 4: *AppRF Fixed Issue*

Bug ID	Description
115294	**Symptom**: An IAP crashed and rebooted when AppRF was enabled. The **dpimgr** core file indicated that the **dpimgr** process had failed. A change in the IAP code has resolved this issue. **Scenario**: This issue was not limited to a specific IAP model or software version.

Authentication

Table 5: *Authentication Fixed Issue*

Bug ID	Description
125242	**Symptom**: After an IAP was upgraded to 6.4.3.1-4.2.0.0, the clients failed to authenticate to the RADIUS server in the first attempt. A change in the EAP packet handling process has resolved this issue. **Scenario**: This issue was not limited to a specific IAP model and was observed in IAPs running Instant 6.4.3.1-4.2.0.0 release.

Datapath/Firewall

Table 6: *Datapath/Firewall Fixed Issue*

Bug ID	Description
125242	**Symptom**: An IAP crashed when the domain acl dns entries in the setup exceeded the limitation set by the IAP. The fix ensures that the IAP code is protected in case the limitation is exceeded. **Scenario**: This issue was observed in all IAPs running Instant 6.4.3.1-4.2.0.0 release version..

This chapter describes the features and enhancements introduced in the previous Aruba Instant 6.4.3.x-4.2.x.x releases.

Features and Enhancements

This section describes the features introduced in Instant 6.4.3.1-4.2.0.0 release.

Support for New IAP Devices

Instant 6.4.3.1-4.2.0.0 release introduces support for the following new IAP devices. These new devices do not interoperate with Instant versions lower than 6.4.3.1-4.2.0.0. If these IAPs are placed into a cluster running older Instant versions such as 6.4.x.x-4.1.x.x, the devices will reboot with the **Image Sync Fail** reason. To resolve this issue, upgrade the existing cluster to minimum Instant 6.4.3.1-4.2.0.0, and then add the new IAP devices.

Table 7: *New IAP Devices*

AP Platform	Description
IAP-205H	The IAP-205H is a high-performance, dual-radio wireless and wired access point for small business, hospitality, and branch deployments. This device combines high-performance wireless mobility with Gigabit wired local access to deliver secure network access to dormitories, hotel rooms, classrooms, medical clinics, and multi-tenant environments. The IAP-205H can be attached to a wall box using the bracket provided, or converted into a desk-mounted remote access point for branch office deployments using the AP-205H-MNTR desk mount kit. The IAP-205H is equipped with a total of four active Ethernet ports (E0-E3) and USB port . MIMO (Multiple-Input, Multiple-Output) technology enables the IAP-205H to provide wireless 2.4 GHz 802.11n and 5 GHz 802.11n/ac functionality, while simultaneously supporting existing 802.11a/b/g wireless services.
IAP-228	The IAP-228 is a fully temperature-hardened, water-resistant, indoor-rated, dual-radio IEEE 802.11ac wireless access point. This access point use MIMO 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.
IAP-277	The IAP-277 is an environmentally-hardened, outdoor-rated, dual-radio IEEE 802.11ac wireless access point. This access point use MIMO 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.

For more information about the AP platforms, visit www.arubanetworks.com.

No Support for IAP-92/93

Starting with 6.4.3.1-4.2.0.0 release, Instant does not support IAP-92/93 devices.

Do not upgrade an IAP cluster containing IAP-92/93 devices to Instant 6.4.3.1-4.2.0.0 or later version. In

case of an accidental upgrade, the IAPs will be automatically downgraded most of the time. You can also manually downgrade IAPs to an Instant 4.0 or 4.1 release, without losing the existing configuration.

Mesh Support on 802.11ac Access Points

Starting with Instant 6.4.3.1-4.2.0.0 release, the 802.11ac IAPs, including IAP-22x, IAP-27x, IAP-21x, and IAP-20x support Mesh configuration. For more information on Mesh IAP configuration, refer to the *Aruba Instant 6.4.3.1-4.2 User Guide*.

Configurable ESSID in a WLAN profile

Starting with 6.4.3.1-4.2.0.0, Instant UI supports changing the ESSID of a WLAN network without deleting or recreating the entire profile. You can also search for clients by the ESSID instead of the profile name. For more information on configuring an ESSID in a WLAN profile, see *Configuring WLAN Settings for an SSID Profile* in the *Aruba Instant 6.4.3.1-4.2 User Guide*.

Captive Portal Server Offload

Instant 6.4.3.1-4.2.0.0 release introduces the server offload feature to reduce the load on an external captive portal server, by ensuring that the non-browser client applications are not unnecessarily redirected to the external captive portal server. For more information on enabling server offload for captive portal, see *Creating a Captive Portal Profile* in the *Aruba Instant 6.4.3.1-4.2 User Guide*.

Configurable Transmission Power Limits for Radio Profiles

In Instant 6.4.3.1-4.2.0.0, the **Customize ARM power range** option is added to the radio profile configuration window to allow administrators to set transmit power limits for a specific radio band. For more information, see *Configuring Radio Settings* in the *Aruba Instant 6.4.3.1-4.2 User Guide*.

Custom Error Page for Web Access Blocked by AppRF Policies

In Instant 6.4.3.1-4.2.0.0, instead of showing the **Access Denied** page, you can define an ACL rule to redirect users to a specific error page when they access a blocked website. You can create a custom list of URLs that you want to use as redirect URLs and add these URLs to the ACL definition. The ACL rules with redirect URLs can be assigned to the user roles of a WLAN network profile.

For more information, see:

- *Creating Custom Error Page for Web Access Blocked by AppRF Policies* in the *Aruba Instant 6.4.3.1-4.2 User Guide*
- **wlan access-rule** in the *Aruba Instant 6.4.3.1-4.2 CLI Reference Guide*

Support for Multiple XML API Server Configuration

Starting with Instant 6.4.3.1-4.2.0.0, users can now configure up to four XML API servers on an IAP. The server entries can be edited or deleted if required. For more information, see *Integrating an IAP with an XML API interface* in the *Aruba Instant 6.4.3.1-4.2 User Guide*. The users can also configure multiple XML AP server profiles in IAP CLI. For more information, see *xml-server-api* in the *Aruba Instant 6.4.3.1-4.2 CLI Reference Guide*.

Instant 6.4.3.1-4.2.0.0 release does not support SSL2.0/3.0. If the XML server sends XML commands to the IAP using SSL2.0 as the default secure protocol, the IAP does not send any response. Aruba recommends that TLSv1 or higher security protocol be used when executing XML commands on an IAP.

Frame Overlay Prevention Support for External Captive Portal Users

Starting with Instant 6.4.3.1-4.2.0.0, when configuring external captive portal profiles, you can enable the frame overlay prevention feature to ensure that a frame displays a web page only if it is in the same domain as the main page. For more information, see:

- *Configuring External Captive Portal for a Guest Network* in the *Aruba Instant 6.4.3.1-4.2 User Guide*.
- **wlan external-captive-portal** in the *Aruba Instant 6.4.3.1-4.2 CLI Reference Guide*

RADIUS and TACACS Server for Controlling Management User Access Level

Starting with Instant 6.4.3.1-4.2.0.0, you can use the attributes returned from a RADIUS or TACACS authentication transaction to determine the access level of the user. For more information on configuring RADIUS and TACACS servers, see:

- *Configuring an External Server for Authentication* in the *Aruba Instant 6.4.3.1-4.2 User Guide*
- The **wlan auth-server** and **wlan tacacs-server** commands in the *Aruba Instant 6.4.3.1-4.2 CLI Reference Guide*

DNS IP Configuration for Virtual Controller

Starting with Instant 6.4.3.1-4.2.0.0, you can explicitly configure the DNS IP address for Virtual Controllers. IAPs can obtain their DNS IP addresses from per AP configuration (**ip-address** command), from the DHCP server, or from the Virtual Controller DNS IP address configuration. The Virtual Controller DNS IP address is only used for APs and does not apply to the clients connected to the APs.

For more information on Virtual Controller DNS IP, see:

- *Configuring Virtual Controller Network Settings* in the *Aruba Instant 6.4.3.1-4.2 User Guide*
- **virtual-controller-dnsip** in the *Aruba Instant 6.4.3.1-4.2 CLI Reference Guide*

Accounting Server Configuration in Wired Profiles

Starting with Instant 6.4.3.1-4.2.0.0, you can configure accounting servers for a wired network profile. You can either use the same server for authentication and accounting, or configure a separate accounting server. If you enable accounting for wired profile users, configure accounting server, and set an accounting interval. For more information on wired profile configuration, see:

- *Configuring a Wired Profile* in the *Aruba Instant 6.4.3.1-4.2 User Guide*
- **wired-port-profile** in the *Aruba Instant 6.4.3.1-4.2 CLI Reference Guide*

Country Code Selection

When the IAP-RW variants are initialized, the country code must be selected when logging in to the IAP. On selecting a country code, the IAPs operate in the selected regulatory domain and adhere to the local EIRP regulations. However, in the earlier Instant releases, if an IAP was set to an unsupported country code, radios on that IAP were disabled to avoid regulatory conflicts. In the Instant 6.4.3.1-4.2.0.0 release, the **Country Code window** displays only the supported country codes, to ensure that an IAP is always set to a supported country code and there are no regulatory conflicts.

If the supported country code is not in the list, contact your Aruba Support team to know if the required country code is supported and obtain the software release version that supports the required country code.

Configurable USB Port Status

Starting with Instant 6.4.3.1-4.2.0.0, you can set the USB port status to enabled or disabled based on your uplink preferences. If you do not want to use cellular uplink or 3G/4G USB modems in your current network setup, you can set the USB status to disabled. By default, the USB port status is enabled.

For more information on configuring USB port status, see:

- *Changing USB Port Status* in the *Aruba Instant 6.4.3.1-4.2 User Guide*
- **usb-port-disable** in the *Aruba Instant 6.4.3.1-4.2 CLI Reference Guide*

Voice Traffic Prioritization

Starting with Instant 6.4.3.1-4.2.0.0, IAPs comply with Spectralink's Voice Interoperability for Enterprise Wireless (VIEW) Certification to ensure interoperability and high performance between Spectralink 84-Series, 87-Series, and 8020/8030 Wireless Telephones and WLAN infrastructure products.

You can configure the following parameters in a WLAN SSID profile for voice traffic and Spectralink Voice Prioritization:

- **Traffic Specification (TSPEC)**—Prioritizes time-sensitive traffic such as voice traffic initiated by the client.
- **TSPEC Bandwidth**—Reserves bandwidth for voice traffic.
- **Spectralink Voice Protocol (SVP)**—Prioritizes voice traffic for SVP handsets.

New Operator for Configuring VLAN Derivation Rule

In Instant 6.4.3.1-4.2.0.0, a new operator **Is the VLAN** is introduced for configuring the VLAN derivation rules. When configured, the users are assigned the VLAN value returned by the attribute in the VLAN derivation rule. For more information, see *Configuring VLAN Derivation Rules* in the *Aruba Instant 6.4.3.1-4.2 User Guide*.

Captive Portal Support for Web Browsers with HTTP Proxy Configuration

Starting with Instant 6.4.3.1-4.2.0.0, if your browser has a proxy configuration, you can configure a captive portal proxy server or a global proxy server in the guest SSIDs for captive portal clients to match the browser configuration.

For information on configuring ports for external captive portal profiles, see:

- *Configuring External Captive Portal for a Guest Network* in the *Aruba Instant 6.4.3.1-4.2 User Guide*
- The **captive-portal-proxy-server** parameter in the **wlan ssid-profile** command in the *Aruba Instant 6.4.3.1-4.2 CLI Reference Guide*

No Virtual IP Address for IAP-VPN Deployments

Starting with Instant 6.4.3.1-4.2.0.0, the Virtual Controller IP address configuration is no longer required for IAP-VPN deployments.

Support for 3G/4G Modem SIM PIN Locking

IAPs support SIM PIN lock function for 3G/4G modems that support the SIM locking feature to prevent fraudulent use. The IAP can now lock and unlock the SIM PIN using the **pin-enable** and **pin-puk** parameters in the **cellular-uplink-profile** command.

For more information on SIM PIN locking, see **cellular-uplink-profile** in the *Aruba Instant 6.4.3.1-4.2 CLI Reference Guide*

RadSec Certificate Support

Starting with Instant 6.4.3.1-4.2.0.0, you can now upload RadSec and RadSec CA certificates to the IAP. These certificates are used for client authentication when RADIUS communication over TLS is enabled. For more information, see *Uploading Certificates* and *Enabling RADIUS Communication over TLS* in the *Aruba Instant 6.4.3.1-4.2 User Guide*.

On-demand Configuration Download

The IAPs support managed mode operations such as periodic retrieval of configuration files from a specific location. Starting with Instant 6.4.3.1-4.2.0.0, if you want to apply the configuration immediately and do not want to wait until next configuration retrieval attempt, you can use **managed-mode-sync-server** to download the configuration file.

Configuring Multiple Exclusion Ranges of IP Subnets

Starting with Instant 6.4.3.1-4.2.0.0, you can configure multiple exclusion ranges of IP subnets in a local, l2 DHCP profile. Based on the size of the subnet and the configured exclusion range, the IP addresses before and after the defined range are excluded. For more information on configuring local,l2 DHCP profile, see:

- *Configuring Local DHCP Scopes* in the *Aruba Instant 6.4.3.1-4.2 User Guide*
- **ip dhcp** in the *Aruba Instant 6.4.3.1-4.2 CLI Reference Guide*

MTU Configuration for Uplink and Bridge Interfaces

Instant 6.4.3.1-4.2.0.0 introduces the **mtu** command to support the configuration of Maximum Transmission Unit (MTU) size for bridge (br0) and cellular uplink interfaces.

DNS-based Discovery of Provisioning AMP Server

Starting with Instant 6.4.3.1-4.2.0.0, if zero-touch provisioning fails, IAPs can automatically discover the provisioning AirWave server and transfer AirWave configuration to the IAP. For more information on configuring automatic discovery of provisioning AMP server, see *Enabling Automatic Discovery of Provisioning AMP server* in the *Aruba Instant 6.4.3.1-4.2 User Guide*.

Disable Radio Per AP without Rebooting

Instant 6.4.3.1-4.2.0.0 release introduces configuration changes through the IAP CLI to disable 2.4 GHz or 5.0 GHz radio profiles without rebooting IAP or deleting the SSID.

For more information on disabling the 2.4 GHz and 5.0 GHz radio profiles, see **dot11a-radio-disable** and **dot11g-radio-disable** in the *Aruba Instant 6.4.3.1-4.2 CLI Reference Guide*

New Telnet Command in CLI

Instant 6.4.3.1-4.2.0.0 introduces the **telnet** command using which you can initiate a telnet session with the external servers.

MAC Authentication on Guest SSID with Guest-Type Users from Internal Server

Starting with 6.4.3.1-4.2.0.0, you can enable MAC authentication for guest user profiles when captive portal authentication is disabled on a guest SSID. When splash pages profiles are not configured for a guest SSID, you can enable MAC authentication to allow guest clients to authenticate against the internal server of the IAP. For more information on configuring MAC authentication for guest users, see *Disabling Captive Portal Authentication* in the *Aruba Instant 6.4.3.1-4.2 User Guide*.

Transmission Beamforming

Starting with 6.4.3.1-4.2.0.0, the IAP-2xx access points support transmission beamforming to allow effective concentration of its signal at a client location and improve signal, SNR, and throughput.

The transmission beamforming is enabled by default. To disable this feature, use the **no vht-txbf-explicit-enable** command. For more information, see the **wlan ssid-profile** command in the Aruba Instant *6.4.3.1-4.2 CLI Reference Guide*.

Configurable SSL Protocols

Starting with 6.4.3.1-4.2.0.0, the IAP CLI includes the **web-server** command to enable or disable SSL protocols such as tlsv1, tlsv1_1, and tlsv1_2. For more information, see the **web-server** command in the *6.4.3.1-4.2 CLI Reference Guide*.

Captive Portal Logout URL

If the client IP assignment mode is set to **Network assigned** in a guest SSID profile, the guest clients can log out of the captive portal network by accessing the https://securelogin.arubanetworks.com/auth/logout.html URL.

L2 ACL Configuration

Starting from 6.4.3.1-4.2.0.1, Instant supports the configuration of non-IP based Layer-2 (L2) ACLs for both wireless and wired clients in the IAP network. The administrators can choose to allow or block non-IP based L2 packets of a specific Ethernet type. By default, all non-IP based L2 packets are allowed for each ACL. To block non-IP based L2 packets to specific types of Ethernet in your network, you must explicitly set deny ACL rules to these Ethernet types either through UI or CLI.

To configure a deny ACE to block packets to a specific Ethernet type in the Instant UI:

1. Navigate to **Security** > **Roles** > **Rules** > **New Rule**.
2. In the **New Rule** window, ensure that Network service is selected. Select **custom** for the type of service.
3. Under **Protocol**, select **Ethernet** and specify **Ethernet type**.
4. Select **Deny** from the **Actions** drop-down list and select a destination.

You can also configure these rules through CLI using the **wlan access-rule <access_rule>** command. The following example shows how configure ACLs to allow or block packets to specific types of Ethernet:

```
(Instant AP)(config)# wlan access-rule l2acl
(Instant AP)(wlan access-rule l2acl)# Rule eth 0x8864 match any any any permit
(Instant AP)(wlan access-rule l2acl)# Rule eth 0x8864 match any any any permit
(Instant AP)(wlan access-rule l2acl)# Rule eth any match any any any deny
(Instant AP)(wlan access-rule l2acl)# Rule any any match any any any deny
```

Ensure that the permit ACEs are added before the deny ACEs. For example, to allow PPPoE packets for an ACL, add the permitted Access Control Entry (ACE), before adding the deny ACE to block a specific Ethernet type.

Support for Alcatel L800 4G modem

Starting from Instant 6.4.3.1-4.2.0.1 release, Instant supports the Alcatel L800 4G modem.

SSH Server Change

Starting with 6.4.3.1-4.2.0.0 release, the SSH server on the RAP-108/109, IAP-103, IAP-114/115, IAP-224/225, and IAP-214/215 has been changed. This change may cause SSH key exchange warnings when using an SSH client that has cached the SSH key from the previous release. This warning can be safely ignored and does not represent a security risk.

Known Issues and Limitations

This section lists the known issues and limitations in Instant 6.4.3.1-4.2.0.0.

AppRF

Table 8: *AppRF Known Issues*

Bug ID	Description
120228	**Symptom:**: The AppRF deny rules for Skype sessions do not block user access. **Scenario**: This issue is found in IAPs running 6.4.3.1-4.2.0.0 or earlier releases. **Workaround**: None

ARM

Table 9: *ARM Known Issues*

Bug ID	Description
121815	**Symptom:**: When client match is enabled on an IAP, some clients that prefer to connect to the 2.4 GHz band are frequently deauthenticated due to band steering. **Scenario**: When client match is enabled on the IAP, the IAP tries to direct the clients that support dual-band to use 5 GHz. If some clients such as Huawei Honor 6 Plus support dual band and yet prefer to connect to 2.4 GHz, the IAP deauthenticates the client and forces the client to reconnect frequently. This issue is found in IAPs running 6.4.3.1-4.2.0.0 or earlier releases. **Workaround**: Reduce the frequency of client match trigger by increasing the client match calculating interval and virtual beacon report (VBR) entry age (**client-match calc-interval <interval>** and **client-match vbr-entry-age <age>** parameters under the **arm** command) to a higher value.

Mesh Configuration

Table 10: *Mesh Configuration*

Bug ID	Description
122099	**Symptom**: When the 5 GHz radio profile of an IAP is configured to run in the legacy-mode (non-802.11n mode), the 802.11ac mesh link still works in the VHT mode. **Scenario**: Although the 11ac mesh link does not work in the legacy mode, the BSSID functions are not affected. This issue is found in IAP-2xx access points running 6.4.3.1-4.2.0.0 release version. **Workaround**: None