# Aruba Instant
# 6.3.1.1-4.0

**ARUBA®**
n e t w o r k s

Release Notes

## Copyright

## Open Source Code

Certain Aruba products include Open Source software code developed by third parties, including software code subject to the GNU General Public License (GPL), GNU Lesser General Public License (LGPL), or other Open Source Licenses. Includes software from Litech Systems Design. The IF-MAP client library copyright 2011 Infoblox, Inc. All rights reserved. This product includes software developed by Lars Fenneberg et al. The Open Source code used can be found at this site:

http://www.arubanetworks.com/open_source

## Legal Notice

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

## Warranty

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

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

Aruba Instant 6.3.1.1-4.0 is a major software release that introduces new features and enhancements and known issues and limitations identified in the current release.

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

## Contents

- What's New in this Release on page 6 lists the new features and enhancements introduced in this release of Aruba Instant.
- Known Issues and Limitations on page 13 describes the known issues and limitations that are applicable to this release of Aruba Instant.

## Contacting Support

**Table 1:** *Contact Information*

| | |
|---|---|
| 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) <br> 1-408-754-1200 |
| International Telephones | arubanetworks.com/support-services/aruba-support-program/contact-support/ |
| Software Licensing Site | licensing.arubanetworks.com/login.php |
| Wireless Security Incident Response Team (WSIRT) | arubanetworks.com/support/wsirt.php |
| Support Email Addresses | |
| Americas and APAC | support@arubanetworks.com |
| EMEA | emea_support@arubanetworks.com |
| WSIRT Email <br> Please email details of any security problem found in an Aruba product. | wsirt@arubanetworks.com |

This chapter provides information on the new features and enhancements introduced in this release of Aruba Instant.

# New Features and Enhancements

## Support of HTTP Proxy Configuration

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

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

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

## IAP Provisioning Enhancements

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

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

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

## Support for Centralized,L3 DHCP Scope

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

When a centralized DHCP scope is configured:

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

For more information, see:

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

## Support for Automatic Configuration of the GRE Tunnel

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

For more information, see:

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

## Bandwidth Contract Enhancements

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

To support this feature:

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

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

## Support for 802.11r Roaming and Fast BSS Transition

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

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

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

## Support for Client Roaming Based on Opportunistic Key Caching

Instant also supports opportunistic key caching (OKC) based roaming. In the OKC based roaming, the AP stores a cached pairwise master key (PMK) for each client, which is derived from last 802.1X authentication completed by the client in the network. By default, the 802.1X authentication profile enables a cached PMK, which is used when a

client roams to a new AP. The cached PMK is used when a client roams to a new AP. This allows faster roaming of clients between the IAPs in a cluster, without requiring a complete 802.1X authentication.

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

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

## Link Aggregation Support on IAP-22x

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

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

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

## Guest Management Interface

In the current release, Instant supports the following types of users:

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

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

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

## IAP Integration with Analytics and Location Engine (ALE)

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

The **RTLS** tab in the **Services** window of the Instant UI allows the configuration of ALE server on an IAP. The **ale-server** and **ale-report-interval** commands are introduced in the current release to enable IAP integration with the

ALE server. For more information, see *Configuring an IAP for Analytics and Location Engine Support in Aruba Instant  6.3.1.1-4.0 User Guide* and *Aruba Instant 6.3.1.1-4.0 CLI Reference Guide*.

| | |
|---|---|
| **NOTE** | IAP-92 and IAP-93 do not support ALE integration. |

## IAP Integration with Palo Alto Networks Firewall

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

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

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

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

## Support for Domain-based ACL

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

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

## Internal Captive Portal Splash Page Enhancements

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

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

## Support for Multiple Captive Portal Profiles

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

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

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

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

## Client Match

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

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

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

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

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

## Support for Spanning Tree Protocol

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

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

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

## Customization of Internal Captive Portal Server Certificates

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

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

```
(Instant Access Point)# copy tftp {<ip-address> <filename> cpserver cert <password> format {p1
2|pem}}
```

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

## Provisioning an IAP as a master IAP

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

To provision an IAP as a master IAP:

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

- In the Instant CLI, execute the **iap-master** command. For more information, see *Aruba Instant 6.3.1.1-4.0 CLI Reference Guide*.

## AirGroup Enhancements

In the current release, Instant supports the following AirGroup services:

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

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

For more information, see:

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

## Dynamic RADIUS Proxy IP Address Configuration

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

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

For more information, see:

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

## Restricted Access Management

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

- Management Subnets—You can configure subnets to ensure that the IAP management is carried out only from these subnets. When the management subnets are configured, Telnet, SSH, and UI access is restricted to these subnets only.
- Restricted corporate access—You can configure restricted corporate access to block unauthorized users from accessing the corporate network. When restricted corporate access is enabled, corporate access is blocked from the uplink port of master IAP, including clients connected to a slave IAP.

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

## Support for IAP-224 and IAP-225

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

| | IAP-22x series does not support wireless mesh functionality. |
|---|---|

## Support for IAP-114 and IAP-115

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

## AP Subscription

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

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

## Uplink VLAN Monitoring and Detection on Upstream Devices

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

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

## Support for Telnet Access

In the current release, Instant supports Telnet access to the Instant CLI. To enable Telnet access:

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

## Applying Configuration Changes during a CLI Session

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

This chapter describes the known issues and limitations identified in the current release of Aruba Instant.

## No Support for PKCS#12 Certificate Format

Starting from 6.3.1.1-4.0 release, Instant does not support uploading of certificates in the (Private-Key Information Syntax Standard) PKCS#12 (.p12) format. To view a list of server and CA certificate formats that are supported by the IAP, run the **show supported-cert-formats** command.

## Known Issues

### Authentication

**Table 2:** *Authentication Known Issue*

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

### Captive Portal

**Table 3:** *Captive Portal Known Issues*

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