


Aruba Instant

6.4.0.2-4.1



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

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.

Contents	3
Release Overview	5
Contents	5
Contacting	5
What's New in this Release	6
New Features and Enhancements	6
AppRF	6
AirGroup Enhancements	7
Support for New Access Points	7
Configurable DSCP Mapping Values for WMM Access Categories	7
Console Access to IAP	8
Instant UI Changes	8
Full Tunnel-Mode VPN Configuration	9
Inbound Firewall	9
Fast Roaming Enhancements	9
Support for 4G Modems	10
Client Match Enhancements	10
Sourcing Virtual Controller Traps from the Virtual Controller IP	10
Support for TACACS+ Servers	11
Integration with an XML API Interface	11
Backup RADIUS Server Configuration with Termination Enabled	11
AP Zone Configuration	11
Authentication Survivability with EAP-TLS	12
Support for 128 ACL Rules	12
Configurable Port for Communication between AirWave Management Server and IAP	12
Disabling of Bridging and Routing Traffic between Clients Connected to an SSID	12
NTP Server Configuration Options	13
Change in Extended SSID Factory Default Settings	13
Support for Read-Only Users to Access CLI	13

Enhancement to the Client Match Maximum Threshold Limit	13
Known Issues and Limitations	14
No Support for IAP-92/93 Platforms	14
Known Issues	14
AirWave	14
Datapath / Firewall	14
General	14
3G/4G Uplink Management	15
Application Classification	15

Aruba Instant 6.4.0.2-4.1 is a major software release that introduces new features and enhancements, and lists the known issues and limitations identified in the current release.

Contents

- [What's New in this Release on page 6](#) describes the new features and enhancements introduced in this release of Aruba Instant.
-
- [Known Issues and Limitations on page 14](#) lists the known issues and limitations identified in the current release of Aruba Instant.

Contacting

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

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

New Features and Enhancements

The following features and enhancements are introduced in the 6.4.0.2-4.1 release of Instant.

AppRF

In this release, 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 from 6.4.0.2-4.1, IAPs support 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 airtgroup** commands in the *Aruba Instant 6.4.0.2-4.1 CLI Reference Guide*

Support for New Access Points

In the 6.4.0.2-4.1 release, Instant software is introduced on the IAP-270 series and IAP-103 devices.

- The IAP-274 and IAP-275 are environmentally hardened, outdoor rated, dual-radio IEEE 802.11ac wireless access points. These access points use MIMO (Multiple-in, Multiple-out) 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-in, Multiple-out) 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.

Configurable DSCP Mapping Values for WMM Access Categories

Instant now 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 1: 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

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 to 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

With Instant 6.4.0.2-4.1 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

You can now 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

IAPs now support 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

In the 6.4.0.2-4.1 release, Instant extends support to the following types of 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

In 6.4.0.2-4.1 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

In 6.4.0.2-4.1 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 6.4.0.2-4.1 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

In 6.4.0.2-4.1 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

In the 6.4.0.2-4.1 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 6.4.0.2-4.1 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

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

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

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 from 6.4.0.2-4.1 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 from 6.4.0.2-4.1 release, read-only users can access the IAP CLI through telnet, SSH, or console.

Enhancement to the Client Match Maximum Threshold Limit

Starting from 6.4.0.2-4.1 release, the maximum threshold limit for Client Match is 255. The previous maximum threshold value was set to 20.

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

No Support for IAP-92/93 Platforms

In the 6.4.0.2-4.1.0.0. release, Instant does not support the IAP-92/93 platforms.



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 the 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 supported release for the IAP-92/93 platforms.

Known Issues

AirWave

Table 2: *AirWave Known Issue*

Bug ID	Description
101945	<p>Symptom: Image sync fails when AirWave Management Platform (AMP) uses user-defined ports with Master APs and Slave APs.</p> <p>Scenario: This issue occurs when the Master AP type is different from the Slave AP type and the Master AP image is different from the Slave AP image. This issue is observed in IAPs running Aruba Instant 6.4.0.2-4.1 release.</p> <p>Workaround: No workaround as yet.</p>

Datapath / Firewall

Table 3: *Datapath / Firewall Known Issue*

Bug ID	Description
101274	<p>Symptom: Prioritization of Voice or Video calls does not work for Lync when the classify media option is enabled</p> <p>Scenario: This issue is observed in IAPs running Aruba Instant 6.4.0.2-4.1 release.</p> <p>Workaround: No workaround as yet.</p>

General

Table 4: *General Known Issue*

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

3G/4G Uplink Management

Table 5: 3G/4G Uplink Management Known Issue

Bug ID	Description
98775	<p>Symptom: 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>Scenario: This issue is observed in RAP-108 and RAP-3WN running Aruba Instant 6.2.0.0-3.3 or later.</p> <p>Workaround: Disconnect and reconnect the USB modem.</p>

Application Classification

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

Table 6: Application Classification Known Issue

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