

ArubaOS 6.2.1.8



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®, RFProtect®, 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 for 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 vendor's 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 details, see the Aruba Networks standard warranty terms and conditions

Contents	3
Release Overview	11
Chapter Overview	11
Release Mapping	11
Supported Browsers	11
Contacting Support	12
Features in ArubaOS 6.2.1.x Releases	13
Features Introduced in ArubaOS 6.2.1.8	13
MIB and Trap Enhancements	13
Features Introduced in ArubaOS 6.2.1.7	13
Features Introduced in ArubaOS 6.2.1.6	13
Change in User Idle Timeout Behavior	13
Features Introduced in ArubaOS 6.2.1.5	13
Features Introduced in ArubaOS 6.2.1.4	13
Features Introduced in ArubaOS 6.2.1.3	13
Default Value Changes	13
Features Introduced in ArubaOS 6.2.1.2	14
Features Introduced in ArubaOS 6.2.1.1	14
Features Introduced in ArubaOS 6.2.1.0	14
Support for New Modem Types	14
Enhanced MultiMode Modem Provisioning	14
In the WebUI	14
In the CLI	15
Regulatory Updates	17
Regulatory Updates in ArubaOS 6.2.1.8	17
Regulatory Updates in ArubaOS 6.2.1.7	17
Regulatory Updates in ArubaOS 6.2.1.6	18
Regulatory Updates in ArubaOS 6.2.1.5	18

Regulatory Updates in ArubaOS 6.2.1.4	18
Regulatory Updates in ArubaOS 6.2.1.3	19
Regulatory Updates in ArubaOS 6.2.1.2	20
Regulatory Updates in ArubaOS 6.2.1.1	21
Regulatory Updates in ArubaOS 6.2.1.0	21
Resolved Issues	23
Resolved Issues in ArubaOS 6.2.1.8	23
Air Management- IDS	23
Base OS Security	23
Captive Portal	23
Controller-Platform	24
LDAP	24
VLAN	25
Voice	25
WebUI	26
Resolved Issues in ArubaOS 6.2.1.7	26
AP-Platform	26
Base OS Security	26
Mobility	26
WebUI	27
Resolved Issues in ArubaOS 6.2.1.6	27
AP-Platform	27
AP-Wireless	27
Base OS Security	28
Captive Portal	28
Configuration	28
Controller-Datapath	29
Controller-Platform	30
Controller-Software	30
IPv6	30
RADIUS	31

SNMP	31
Spectrum UI	31
WebUI	31
Resolved Issues in ArubaOS 6.2.1.5	32
802.1X Authentication	32
Air Management - IDS	32
AP-Datapath	32
AP-Platform	32
AP-Regulatory	33
AP-Wireless	33
Base OS Security	34
Captive Portal	34
Controller-Datapath	35
Controller-Platform	35
DHCP	36
Hardware Management	36
IPv6	37
Master-Redundancy	37
Mesh	37
Mobility	37
Remote AP	38
Voice	38
WebUI	39
Resolved Issues in ArubaOS 6.2.1.4	39
802.1X Authentication	39
AP-Datapath	40
AP-Regulatory	40
AP-Wireless	40
ARM	40
Base OS Security	41
Captive Portal	41
Controller-Datapath	41

Controller-Platform	42
Intrusion Detection System	42
Mobility	43
PPPoE	43
WebUI	43
Resolved Issues in ArubaOS 6.2.1.3	44
Air Management - IDS	44
AP-Platform	44
AP-Datapath	44
AP-Regulatory	44
AP-Wireless	45
Base OS Security	45
Controller-Datapath	46
Controller-Platform	46
DHCP	46
Local Database	47
OSPF	47
Remote AP	47
RADIUS	48
Role/VLAN Derivation	48
SNMP	49
Station Management	49
Voice	49
WebUI	50
Resolved Issues in ArubaOS 6.2.1.2	50
802.1X Authentication	50
AP-Platform	51
AP-Wireless	51
Base OS Security	51
Command Line Interface	52
Control Plane Security (CPsec)	52
Controller-Datapath	52

Controller-Platform	53
Controller-Software	53
Enhanced Voice-Data Optimized	53
IPv6	54
Mobility	54
RADIUS	54
SNMP	54
Voice SIP	55
WebUI	55
Resolved Issues in ArubaOS 6.2.1.1	55
802.1X Authentication	56
Air Management - IDS	56
AMON	56
Resolved Issues in ArubaOS 6.2.1.0	56
3G/4G	57
802.1X Authentication	57
Air Management-IDS	57
AP-Platform	58
AP-Wireless	58
Controller-Datapath	59
Controller-Platform	60
Base OS Security	60
IPSec	61
Management Authentication	61
Mesh	61
RADIUS	61
Remote AP	62
Spectrum-Infrastructure	62
Station Management	62
WebUI	63

Known Issues	65
Known Issues and Limitations in ArubaOS 6.2.1.8	65
AP-Datapath	65
AP-Platform	65
Base OS Security	65
Captive Portal	66
Configuration	66
Controller-Datapath	66
Controller-Platform	67
LLDP	67
Remote AP	67
WebUI	68
Known Issues and Limitations in ArubaOS 6.2.1.7	68
Controller-Platform	68
Known Issues and Limitations Prior to ArubaOS 6.2.1.7	68
802.1X Authentication	68
AMON	69
AP-Wireless	69
AP-Platform	70
Air Management -IDS	70
Authentication	71
Base OS Security	71
Captive Portal	72
Controller-Datapath	72
Controller-Platform	73
DHCP	74
IDS	74
IPsec	74
IPv6	74
Management Authentication	75
Master-Redundancy	75

Mobility	75
Remote AP	76
Station Management	76
Startup Wizard	77
WebUI	77
WMM	79
Issues Under Investigation	79
WebUI	79
Maximum DHCP Leases Per Platform	79
Upgrade Procedures	81
Upgrade Caveats	81
Important Points to Remember and Best Practices	82
Memory Requirements	83
Backing up Critical Data	83
Back Up and Restore Compact Flash in the WebUI	84
Back Up and Restore Compact Flash in the CLI	84
Upgrading in a Multi-Controller Network	84
Upgrading to 6.2.x.x	85
Install Using the WebUI	85
Upgrading From an Older Version of ArubaOS	85
Upgrading From a Recent version of ArubaOS	85
Upgrading With RAP-5 and RAP-5WN APs	86
Install Using the CLI	86
Upgrading From an Older version of ArubaOS	87
Upgrading From a Recent version of ArubaOS	87
Downgrading	88
Before you Begin	88
Downgrading Using the WebUI	89
Downgrading using the CLI	89
Before You Call Technical Support	90

7200 Series Migration	91
Migrating to the 7200 Series Controller	91
Important Points to Remember	91
Backing Up Your Data Before Upgrading to 6.2	91
Back Up the Flash File System in the WebUI	92
Back Up the Flash File System in the CLI	92
Upgrading Your Network	92
Backing Up Your Data After Upgrading to 6.2	92
Transferring Licenses	93
Installing Your New Controller	93
Installing Backed Up Controller Data	93
Restore the Flash File System in the WebUI	93
Restore the Flash File System in the CLI	93
Applying Licenses	94
Applying the Software License Key in the WebUI	94
Applying the Software License Key in the License Wizard	94
Backing Up Licenses in the WebUI	94
Backing Up Licenses in the CLI	94
Reload Your Controller	94
Establishing Network Connectivity	95
Connecting to the Controller	95
Verifying Controller Operation	95
Verifying Migration in the WebUI	95
Verifying Migration in the CLI	95

ArubaOS 6.2.1.8 is a software patch release that introduces fixes to the issues identified in the previous releases. For details on all of the features described in the following sections, see the *ArubaOS 6.2 User Guide*, *ArubaOS 6.2 CLI Reference Guide*, and *ArubaOS 6.2 MIB Reference Guide*.

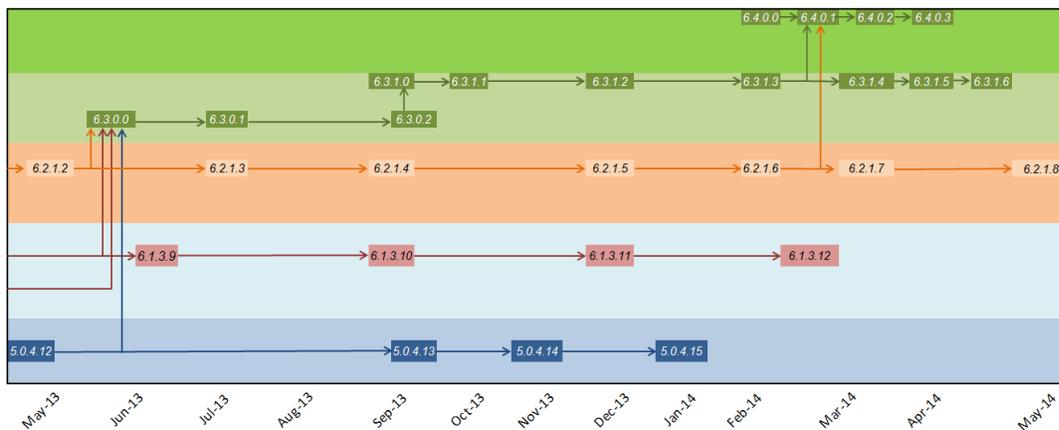
Chapter Overview

- [Features in ArubaOS 6.2.1.x Releases on page 13](#) provides a description of features and enhancements added in ArubaOS 6.2.1.x
- [Resolved Issues on page 23](#) provides a description of issues resolved in ArubaOS 6.2.1.x.
- [Known Issues on page 65](#) provides a description and workaround for the issues identified in ArubaOS 6.2.1.x.
- [Upgrade Procedures on page 81](#) describes the procedures for upgrading a controller to ArubaOS 6.2.1.x.

Release Mapping

The following illustration shows the patch and maintenance releases that are included in their entirety in ArubaOS 6.2.1.8.

Figure 1 *ArubaOS Releases and Code Stream Integration*



Supported Browsers

The following browsers are officially supported to use with ArubaOS 6.2.1.8 WebUI:

- Microsoft Internet Explorer 10.x and 11.0, on Windows 7, and Windows 8
- Mozilla Firefox 23 or higher on Windows Vista, Windows 7, and Mac OS
- Apple Safari 5.1.7 or higher on Mac OS

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) 1-408-754-1200
International Telephone	http://arubanetworks.com/support-services/aruba-support-program/contact-support/
Software Licensing Site	http://licensing.arubanetworks.com
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
Wireless Security Incident Response Team (WSIRT)	wsirt@arubanetworks.com

This chapter describes features introduced in ArubaOS 6.2.1.x. For more information about features introduced in ArubaOS 6.2.0.x, refer to the *ArubaOS 6.2.x User Guide*.

Features Introduced in ArubaOS 6.2.1.8

This section lists the new features introduced in ArubaOS 6.2.1.8.

MIB and Trap Enhancements

The **wlsxAccessPointIsUP** and **wlsxAccessPointIsDown** traps are deprecated and replaced by **wlsxNAccessPointIsUp** and **wlsxNAccessPointIsDown** traps for AP up and down events respectively. For more information on these traps, download the **aruba-mibs_6.2.1.8_43656.tar** from the support site and view the **aruba-trap.my** file.

Features Introduced in ArubaOS 6.2.1.7

There are no new features added in ArubaOS 6.2.1.7.

Features Introduced in ArubaOS 6.2.1.6

Change in User Idle Timeout Behavior

Starting from ArubaOS 6.2, the split-tunnel and bridge users are timed out based on the **aaa user idle-timeout** value and not based on the value set in the L2 ageout. This change causes Captive portal with split-tunnel users to fall to pre-cp role for a short idle time. To avoid the occurrence of this issue, you can set the value of the **aaa user idletimeout** parameter in each captive portal profile.

Features Introduced in ArubaOS 6.2.1.5

There are no new features added in ArubaOS 6.2.1.5.

Features Introduced in ArubaOS 6.2.1.4

There are no new features added in ArubaOS 6.2.1.4.

Features Introduced in ArubaOS 6.2.1.3

Default Value Changes

The **CSD Override** (Cyclic Shift Diversity) parameter is now set to be disabled by default in the **HT Radio** profile. The default behavior has changed because some clients incorrectly reported a low signal strength.



The change in default settings will not impact the upgrade if you have already disabled the **CSD Override** parameter.

The following example describes how to enable and disable the **CSD Override** parameter:

```

(host) (config) #rf ht-radio-profile default-a
(host) (High-throughput radio profile "default-a") csd-override
(host) (High-throughput radio profile "default-a") no csd-override
(host) (High-throughput radio profile "default-a") #end
(host) #show rf ht-radio-profile default-a
High-throughput radio profile "default-a" (Predefined (editable))
-----
Parameter                Value
-----
40 MHz intolerance       Disabled
Honor 40 MHz intolerance Enabled
CSD override             Disabled

```

Features Introduced in ArubaOS 6.2.1.2

There are no new features added in ArubaOS 6.2.1.2.

Features Introduced in ArubaOS 6.2.1.1

There are no new features added in ArubaOS 6.2.1.1

Features Introduced in ArubaOS 6.2.1.0

Support for New Modem Types

ArubaOS 6.2.1.0 introduces support for the Novatel Ovation MC551 4G LTE USB Modem and the Pantech UML290 4G USB modem.

Enhanced MultiMode Modem Provisioning

ArubaOS 6.2.1.0 introduces a new method of provisioning a multimode USB modem (such as a Verizon UML290) for a remote AP. These changes simplify modem provisioning for both 3G and 4G networks.

The previous modem configuration procedure required that you define a driver for a 3G modem in the **USB modem** field in the AP provisioning profile, or define a driver for a 4G modem in the **4G USB type** field. Starting with ArubaOS 6.2.1.0, you can configure drivers for both a 3G or a 4G modem using the **USB field**, and the **4G USB Type** field is deprecated.

In the WebUI

The AP provisioning profile in ArubaOS 6.2.1.0 includes a new **Cellular Network Preference** setting that allows you to select how the modem should operate. This setting includes parameters described in [Table 2](#).

Table 2: Cellular Network Preference Parameters

Parameter	Description
auto (default)	In this mode, modem firmware will control the cellular network service selection; so the cellular network service failover and fallback is not interrupted by the remote AP (RAP).
3g_only	Locks the modem to operate only in 3G
4g_only	Locks the modem to operate only in 4G

Table 2: Cellular Network Preference Parameters

Parameter	Description
advanced	<p>The remote AP (RAP) controls the cellular network service selection based on an Received Signal Strength Indication (RSSI) threshold-based approach.</p> <ul style="list-style-type: none">• Initially the modem is set to the default auto mode. This allows the modem firmware to select the available network.• The RAP determines the RSSI value for the available network type (for example 4G), checks whether the RSSI is within required range, and if so, connects to that network.• If the RSSI for the modem's selected network is not within the required range, the RAP will then check the RSSI limit of an alternate network (for example, 3G), and reconnect to that alternate network.• The RAP will repeat the above steps each time it tries to connect using a 4G multimode modem in this mode.

In the CLI

```
(host) (config) #provision-ap
(Host) (AP provisioning) #cellular_nw_preference ?
3g-only          Set the modem to operate only in 3G
4g-only          Set the modem to operate only in 4G
advanced         Use advanced algorithm to select the available network
auto             Let modem to select the network preference (default)
```


The following regulatory updates were introduced in ArubaOS 6.2.1.x releases.

Periodic regulatory changes may require modifications to the list of channels supported by AP. For a complete list of channels supported by AP using a specific country domain, access the controller command-line interface and issue the command **show ap allowed-channels country-code <country-code> ap-type <ap-model>**.

Regulatory Updates in ArubaOS 6.2.1.8

The following table describes regulatory enhancements introduced in ArubaOS 6.2.1.8:



Contact your local Aruba sales representative on device availability and support for the countries listed in the following table.

Table 3: Regulatory Domain Updates

Regulatory Domain	Update
India and Indonesia	Added support for AP-114 and AP-115.
Colombia, Dominican Republic, Puerto Rico, Montenegro, Albania, and Bosnia, and Herzegovina	Added support for RAP-155.
Mexico	Added support for AP-224 and AP-225.
Algeria	Added support for AP-104.

Regulatory Updates in ArubaOS 6.2.1.7

The following table describes regulatory enhancements introduced in ArubaOS 6.2.1.7:



Contact your local Aruba sales representative on device availability and support for the countries listed in the following table.

Table 4: Regulatory Domain Updates

Regulatory Domain	Update
Costa Rica	Added support for AP-92, AP-93, AP-134, and AP-135 access points.
Senegal	Added support for AP-134 and AP-135 access points.

Regulatory Updates in ArubaOS 6.2.1.6

The following table describes regulatory enhancements introduced in ArubaOS 6.2.1.6:



Contact your local Aruba sales representative on device availability and support for the countries listed in the following table.

Table 5: *Regulatory Domain Updates*

Regulatory Domain	Update
Algeria	Added support for AP-175P, AP-175AC, and AP-175DC access points.
Argentina	Added support for AP-93, AP-92, RAP-108, and RAP-109 access points.
Thailand	Added support for the RAP-109 access point.
Israel	Added support for the RAP-3WN, RAP-3WNP, RAP-108, RAP-109, AP-224, AP-225, AP-114, and AP-115 access points.
Uruguay	Added support for AP-93, AP-92, and AP-104 access points.
Vietnam	Added support for AP-93 and AP-92 access points.
Costa Rica	Added support for AP-134 and AP-135 access points.

Regulatory Updates in ArubaOS 6.2.1.5

There are no regulatory updates introduced in ArubaOS 6.2.1.5.

Regulatory Updates in ArubaOS 6.2.1.4

The following table describes regulatory enhancements introduced in ArubaOS 6.2.1.4:



Contact your local Aruba sales representative on device availability and support for the countries listed in the following table.

Table 6: *Regulatory Domain Updates*

Regulatory Domain	Update
Columbia, Dominican Republic, India, Macau, Pakistan, Puerto Rico, Qatar, Saudi Arabia, South Korea, and UAE	Added support for RAP-108 and RAP-109 access points.
Brazil	Added support for the RAP-2WG access point.

Regulatory Updates in ArubaOS 6.2.1.3

The following table describes regulatory enhancements introduced in ArubaOS 6.2.1.3.



Contact your local Aruba sales representative on device availability and support for the countries listed in the following table.

Table 7: Regulatory Domain Updates

Regulatory Domain	Update
Russia, Brazil, South Africa, Colombia, Macedonia	Added support for RAP-3WN and RAP-3WNP access points.
Algeria, Bosnia and Herzegovina, Columbia, Dominican Republic, South Korea, Macedonia, Puerto Rico	Added support for AP-104 access points.
Republic of Trinidad and Tobago	Added support for AP-135 and AP-175 access points.
Algeria	Added support for AP-92, AP-93, and AP-105 access points.
Bermuda, Bosnia and Herzegovina, Colombia, Dominican Republic and Macedonia	Added support for the AP-175DC access point.
Bolivia, Ecuador, El Salvador, Guatemala, Nicaragua, Panama, Puerto Rico, Venezuela, and Zambia	Added support for the AP-105 access point.
Colombia	Added support for the AP-92 access point.
Colombia, Dominican Republic, Mexico, Puerto Rico, Singapore	Added support for the AP-93 access point.
Azerbaijan, Belarus, Bosnia and Herzegovina, Colombia, Croatia, Kazakhstan, Peru, Russia	Added support for the AP-135 access point.
Argentina	Added support for the RAP-5WN access point.
Venezuela	Added support for AP-175 and AP-175AC access points.
Macau	Added support for AP-134 and AP-135 access points.
Macau, Ukraine	Added support for the AP-175P access point.
Canada	Enabled DFS channels for AP-175P, AP-175AC, and AP-175DC access points.
Uganda, Malaysia	Added support for the AP-175AC access point.
Australia, New Zealand, Brazil, South Africa, Hong Kong, Singapore, Egypt, Ukraine	Added support for RAP-108 and RAP-109 access points.

Regulatory Updates in ArubaOS 6.2.1.2

The following changes impact new AP and remote AP installations running ArubaOS 6.2.1.2:



Contact your local Aruba sales representative on device availability and support for the countries listed in the following table.

Table 8: Regulatory Domain Updates

Regulatory Domain	Update
Changes for RAP-108/RAP-109 Access Points	
Malaysia	ArubaOS now supports this country domain.
Changes for AP-124/AP-125 Access Points	
Kazakhstan and Dominican Republic	ArubaOS now supports these country domains.
Australia and New Zealand	These country domains support all channels allowed by the FCC (including indoor, outdoor and DFS channels). In previous releases, Australia and New Zealand used ETSI channels.
UAE	Removed support for channels 149-165.
Mexico	This domain requires Dynamic Frequency Selection (DFS) in all 802.11a channels. In previous releases, all 802.11a channels were open without DFS support.
Serbia	Added DFS support for channels 52-64 and 100-140. These channels were not open in previous releases.
New Zealand, Puerto Rico, Columbia	Removed support for channels 120-128, because these channels were removed from the FCC list of allowed channels.
Changes for AP-134/AP-135 Access Points	
Kazakhstan, Chile, Serbia, Dominican Republic and Nigeria	ArubaOS now supports these country domains.
Bermuda, Costa Rica, Ecuador, El Salvador, Guatemala, Honduras, Kenya, Pakistan, Mauritius, Panama, Qatar, Trinidad and Tobago and Uruguay	Removed support for AP-134 and AP-135 in these country domains.
South Korea and Taiwan	Added support for DFS Channels 52-64, and 100-128. Previous releases did not include any support for these channels.
Singapore	Added support for DFS Channels 100-140. Previous releases did not include any support for these channels.
Israel	Channels 36-48 require DFS. In previous releases, these channels were open without DFS support.
Saudi Arabia	Removed support for channel 165.
Ireland and UAE	Removed support for channel 149-165.

Table 8: Regulatory Domain Updates

Regulatory Domain	Update
Australia, New Zealand	These country domains support all channels allowed by the FCC (including indoor, outdoor and DFS channels).
Mexico	Requires DFS in all 802.11a channels. In previous releases, all 802.11a channels were open without DFS support.
New Zealand and Puerto Rico	Added DFS channel support for channels 52-64, 100-128. Previous releases did not include any support for these channels.
Colombia and Thailand	Removed support for channels 116-128
Russia	Removed support for channel 132.
Egypt	Removed support for channels 149-165. This country domain no longer supports 40MHz on any channel.
Ukraine	Added 40 MHz support for channels 149-161.
Peru	Removed support for channels 12-13, 52-64, 100-140, and 165. (The only supported channels for this country domain are 1-11, 36-48, and 149-161.)
Venezuela	Added 40MHz support for channels 36-48, 52-64, and 149-161.
Jordan	Added 40MHz support for channels 36-48 and 149-161.

Regulatory Updates in ArubaOS 6.2.1.1

There are no regulatory updates introduced in ArubaOS 6.2.1.1.

Regulatory Updates in ArubaOS 6.2.1.0

There are no regulatory updates introduced in ArubaOS 6.2.1.0.

The following issues are resolved in ArubaOS 6.2.1.x releases.

Resolved Issues in ArubaOS 6.2.1.8

The following issues are resolved in ArubaOS 6.2.1.8.

Air Management- IDS

Table 9: *Air Management- IDS Fixed Issues*

Bug ID	Description
81740 97522	<p>Symptom: Traps were sent when an SSID went up or down instead of being sent when an AP went up or down. Also, an incorrect IP address of the AP was sent. This issue is resolved by replacing the incorrect traps with the correct traps, and by verifying the IP address of the AP sent is correct.</p> <p>Scenario: This issue was not limited to a specific controller model or release version.</p>

Base OS Security

Table 10: *Base OS Security Fixed Issues*

Bug ID	Description
93237	<p>Symptom: An internal module (Authentication) crashed on the controller. Ignoring the usage of the equivalentToMe attribute, which was not used by the master controller resolved this issue.</p> <p>Scenario: This issue was observed when the Novell® Directory System (NDS) pushed the bulk of user data as the value for the attribute to the master controller. This issue was not limited to a specific controller model or release version.</p>
99038	<p>Symptom: An increase in the memory usage was observed in the authentication module. This issue is resolved by fixing the memory leak in the authentication module.</p> <p>Scenario: This issue was observed when client devices performed EAP-TLS with EAP-termination enabled using certificates containing the optional field Subject Alternative Name.</p>

Captive Portal

Table 11: *Captive Portal Fixed Issues*

Bug ID	Description
93927	<p>Symptom: On 7200 Series controllers the output of show datapath user displayed a user entry but the user entry was not present in the control plane. This issue was resolved by internal code changes.</p> <p>Scenario: This issue occurred when WLAN was configured in the tunnel mode and was observed in ArubaOS 6.2 or later versions.</p>
94167	<p>Symptom: When client traffic was moving through an L3 GRE tunnel between a data switch and a controller, the controller did not provide the captive portal page to the client. The fix ensures that the controller provides the captive portal page to the client.</p> <p>Scenario: This issue was observed after an M3 controller was upgraded to ArubaOS 6.1.3.10. This issue was caused because the controller was unable to find the correct role for the client traffic and, therefore, did not provide the captive portal page.</p>

Controller-Platform

Table 12: *Controller-Platform Fixed Issues*

Bug ID	Description
91097	<p>Symptom: A local controller rebooted unexpectedly. The log files for the event listed the reason for the reboot as Mobility Processor update. The fix ensures that the controller does not reboot unexpectedly by making code level changes to the primary and secondary nor flash boot partition.</p> <p>Scenario: This issue was observed in controllers running ArubaOS 6.1.3.9.</p>
96347 94427 97078 97287 97456 97468 97988 98425 98656	<p>Symptom: An M3 controller rebooted unexpectedly. The log files for the event listed the reason for the reboot as User pushed reset error. The issue is resolved by removing the lock contention.</p> <p>Scenario: This issue was observed due to panic dump or SOS crash, which was a result of jumbo packet or packet corruption. This issue was observed in M3, 3200, 3400, and 3600 controllers, but was not limited to any specific ArubaOS release version.</p>
96712	<p>Symptom: A local controller rebooted unexpectedly during a terminal/ssh related operation. The log files for the event listed the reason for the reboot as Kernel panic.</p> <p>Scenario: This issue was observed in 7240 controllers running ArubaOS 6.2.1.4.</p>
97658 97388 98373	<p>Symptom: Some access points lost connectivity when the controller to which they were connected rebooted. This issue is resolved by ensuring that the boot partition information is updated in the secondary bank of the controller.</p> <p>Scenario: This issue occurred when the controller rebooted due to a watchdog reset. This issue was not limited to any specific controller model or release version.</p>
98873	<p>Symptom: A 650 controller was crashing during reboot. The log files for the event listed the reason as an address error on CPU4.</p> <p>Scenario: This issue was observed on the 650 controllers running on ArubaOS 6.2.1.7.</p>
99106	<p>Symptom: A large number of Only Bottom slots can arbitrate debug messages were generated and as a result the controller console was flooded with these redundant messages. The issue is fixed by disabling these redundant messages in the arbitration algorithm.</p> <p>Scenario: This issue was observed in M3 controllers and is not limited to any ArubaOS version.</p>

LDAP

Table 13: *LDAP Fixed Issues*

Bug ID	Description
90859	<p>Symptom: A controller intermittently disconnected from the LDAP server because the LDAP server reset its TCP connection. Establishing a TCP connection for each user and binding it using admin-dn and password fixed this issue. Once the user is authenticated, the connection binds the actual user.</p> <p>Scenario: This issue was triggered by null binds created when the controller established TCP/SSK connections in advance, so that they can be used whenever a user joined the network. This issue occurred in a 3000 Series controller running ArubaOS 6.1.3.10.</p>

VLAN

Table 14: *VLAN Fixed Issues*

Bug ID	Description
97117	<p>Symptom: When the RADIUS server returned multiple Vendor Specific Attributes (VSAs), ArubaOS did not check these attributes or set user roles. This issue is fixed by verifying the list of attributes before matching them with the rules.</p> <p>Scenario: This issue was observed when a user tried to set a role using the VSA attributes that were returned from the RADIUS server. This issue was observed in 3400 Series controllers running ArubaOS 6.2.1.4.</p>

Voice

Table 15: *Voice Fixed Issues*

Bug ID	Description
91910 94031 100262	<p>Symptom: The output of the show voice call-cdrs command displayed multiple CDR with INITIATED state for calls between ASCOM® phones. The fix ensures correct handling of the state transitions for New Office Environment (NOE) application layer gateway.</p> <p>Scenario: This issue occurred during a consulted call scenario. This issue is observed in an NOE deployed voice environment with controllers running ArubaOS 6.1 or later.</p>
94038 94600	<p>Symptom: The show voice call-cdrs and show voice client-status commands displayed incorrect state transitions for consulted, transfer, and speaker announced call scenarios. The fix ensures the correct state transitions for New Office Environment (NOE) application layer gateway.</p> <p>Scenario: This issue was observed in an NOE deployed voice environment with controllers running ArubaOS 6.1 or later versions.</p>
94342	<p>Symptom: The Station Management (STM) process crashed in a New Office Environment (NOE) deployment. This issue is resolved by making code level changes to avoid a STM crash.</p> <p>Scenario: This issue was observed when an NOE user tried to call an extension, but disconnected the call before it was complete, as a result the CDR changed to CONNECTING state. This issue was observed in controllers running ArubaOS 6.1.3.10.</p>
95566	<p>Symptom: When two parties made a VoIP call using Microsoft® Lync 2013, media classification running on the controller prioritized the media session with wrong DSCP values. The fix ensures that the wmm value is read from the Tunnel Entry rather than the Bridge Entry, so that the value is correct.</p> <p>Scenario: The DSCP values configured under the ssid-profile did not take effect. This issue occurred when the initial VLAN and the assigned VLAN were different. This issue was observed on M3 controllers running ArubaOS 6.1.3.10.</p>
97823	<p>Symptom: SVP, Lync, or Facetime calls prioritized using VoIP ALGs, continued to have call detail records in the connected state although the calls were disconnected. This caused a memory leak in the station management process. This issue is resolved by freeing the memory that was leaking in the station management module.</p> <p>Scenario: This issue was seen in deployments that used SVP phones, Lync, or Facetime with media classification enabled. This issue was observed on controllers running ArubaOS 6.2.1.5 or later.</p>

WebUI

Table 16: WebUI Fixed Issues

Bug ID	Description
96284 100319	Symptom: When you click on the Plan tab of the controller's WebUI using Microsoft® Internet Explorer 11, the Plan page fails to load. This issue is resolved by making changes to the internal code such that the Plan page loads successfully. Also, removed the scope for function declaration and object creation. Scenario: This issue was observed on controllers running ArubaOS 6.2.1.x and ArubaOS 6.1.3.x.

Resolved Issues in ArubaOS 6.2.1.7

The following issues are resolved in ArubaOS 6.2.1.7.

AP-Platform

Table 17: AP-Platform Fixed Issues

Bug ID	Description
96913	Symptom: When a controller was upgraded from ArubaOS 5.x or ArubaOS 6.0.x to ArubaOS 6.3.1.3, APs failed to upgrade to ArubaOS 6.3.1.3. A defensive check is made in the affected API so that PAPI messages which are smaller than the PAPI header size are handled properly in 6.0.x compared to 5.x. Scenario: This issue was observed in APs running ArubaOS 5.x or ArubaOS 6.0.x. APs running ArubaOS 6.1 and later versions were not impacted.
97237	Symptom: A controller rebooted because of a memory leak in the module that handles address, route, and interface related configurations and notifications on the system. This issue is resolved by fixing the memory leak in the flow. Scenario: The memory leak occurred when an interface or STP states changed frequently with a PAPI error. This issue was observed on 650 controllers running ArubaOS 6.2.1.6 or later.

Base OS Security

Table 18: Base OS Security Fixed Issues

Bug ID	Description
96458	Symptom: A controller rebooted with the reboot cause Nanny rebooted machine - low on free memory . This issue is resolved by freeing the memory that was leaking in the authentication module. Scenario: This issue was observed for VPN users when the cert-cn-lookup parameter was disabled under aaa authentication vpn profile. This issue was not limited to a specific controller model or release version.

Mobility

Table 19: Mobility Fixed Issues

Bug ID	Description
96569	Symptom: The client did not receive an IP address through DHCP, and could not pass traffic when L3 mobility was enabled on the controller. This issue is resolved by clearing the state machine of the affected client. Scenario: This issue was observed when the client roamed from a Virtual AP (VAP) in which the mobile-ip parameter was enabled to a VAP in which the mobile-ip parameter was disabled. This issue was observed in ArubaOS 6.2 and later versions, but was not limited to a specific controller model.

WebUI

Table 20: WebUI Fixed Issues

Bug ID	Description
68464	Symptom: The user was forced out of a WebUI session with the Session is invalid message. This issue is resolved by fixing the timing issue for the exact session ID from cookies in the https request. Scenario: This issue was observed when a web page of the parent domain name was accessed previously from the same browser. This issue was not limited to a specific controller model or release version.

Resolved Issues in ArubaOS 6.2.1.6

The following issues were resolved in ArubaOS 6.2.1.6:

AP-Platform

Table 21: AP-Platform Fixed Issues

Bug ID	Description
87857	Symptom: Fragmented configuration packets sent from the controller to the AP can cause the AP to come up with the "D:" (dirty) flag. Improvements to how ArubaOS handles out-of-order packets resolve this issue. Scenario: This issue is triggered by network congestion or breaks in the connection between the controller and AP.

AP-Wireless

Table 22: AP Wireless Fixed Issues

Bug ID	Description
67847 69062 69346 71530 74352 74687 74792 75212 75792 75944 76142 76217 76715 77273 77275 78118 80735 82147 83242 83243 83244 83624 83833 84170 84339 84511 85015 85054 85086 85367 85959 88515 89136 89253 89256 89816 90603 91084 92871 92877 92878 92879 93923	Symptom: APs unexpectedly rebooted. The log files listed the reason for the reboot as Data BUS error . A change in the exception handling module has fixed this issue. Scenario: This issue was observed in AP-120 Series and AP-68P devices connected to controllers running ArubaOS 6.3.1.2.

Base OS Security

Table 23: *Base OS Security Fixed Issues*

Bug ID	Description
76239	<p>Symptom: VPN user entries did not properly age out of the user table. These user entries became stale and prevented new users with the same IP address from associating to the network. This issue occurred when one Inner-IP address was assigned to two different L2TP outer-IP addresses. ArubaOS 6.2.1.6 resolves this issue by introducing a fix that prevents a previously assigned IP address from returning to the free IP address pool during Next-pin mode using SecureID authentication.</p> <p>Scenario: The issue was identified in 2400 controllers running ArubaOS 5.0.4.5 during Next-pin mode using SecureID as authentication.</p>
77227	<p>Symptom: An internal process that handles user authentication unexpectedly crashed in the controller due to incorrect memory allocation. The issue was fixed by making changes to the IP address pool.</p> <p>Scenario: When remote VPN users were deleted from the system, unexpected sequence of events pointed at stale memory entries. This resulted in an internal process failure. This issue is not limited to a specific controller model or release version.</p>
93130	<p>Symptom: A controller reboots unexpectedly. The log files for the event listed the reason for the reboot as datapath exception. This issue is resolved by adding SSL implementation to validate a packet before processing it.</p> <p>Scenario: This issue was observed when VIA was used to establish a tunnel with the controller, using SSL fallback. This issue was not limited to any specific controller model or release version.</p>

Captive Portal

Table 24: *Captive Portal Fixed Issues*

Bug ID	Description
93674	<p>Symptom: Clients are unable to access an external captive portal page after the controller resets. Changes in how ArubaOS manages captive portal authentication profiles resolved this issue.</p> <p>Scenario: This issue occurred in ArubaOS 6.1.3.x when the controller failed to use the correct ACL entry for a pre-authentication captive portal role.</p>
92927	<p>Symptom: When iOS 7 clients tried to connect through the Captive Portal profile, the users were not redirected to the next page even after a successful authentication. A change in the redirect URL has fixed this issue.</p> <p>Scenario: This issue was observed only in clients using Apple iOS 7 devices.</p>

Configuration

Table 25: *Configuration Fixed Issues*

Bug ID	Description
88120	<p>Symptom: The Configuration > Wireless > AP Installation > AP provisioning > Status tab of the controller WebUI and the output of the commands show ap database long status up start 0 sort-by status sort-direction ascending and show ap database long status up start 0 sort-by status sort-direction descending do not correctly sort the AP entries in ascending or descending order by up time. Improvements to how the controller sorts APs by status and up time resolve this issue.</p> <p>Scenario: This issue was identified in controllers running ArubaOS 6.2.1.2</p>
94559	<p>Symptom: An ACL configured by the user could not be edited or deleted. This issue is resolved by ensuring that the non-editable flag is reset if ACLs are reused after the whitelist is removed..</p> <p>Scenario: This issue was observed in ArubaOS 6.2.x or later, when a user configuration had a white-list defined in a Captive Portal profile, and was triggered because the ACLs that enable white-listing for destinations in a captive-portal profile were reused for user-configured ACLs.</p>

Controller-Datapath

Table 26: *Controller-Datapath Fixed Issues*

Bug ID	Description
93423	<p>Symptom: A controller unexpectedly rebooted, and the log file listed the reason for the reboot as Datapath timeout. This issue is fixed by increasing the stack memory size in the data plane.</p> <p>Scenario: This issue was observed when clients using SSL VPN connected to RAP and the controller tried to decompress these packets. This issue is not limited to any specific controller model or ArubaOS release version.</p>
87417 87846 90469 90896 89641 88039 94157 89433 90746 94636 88445 95332 90024 91853 92827 92828 92829 92830 92832 87949 92464 92466 95655 88226 90458 92294 93555 95333 93825 94007 95703 92988 89539 94476	<p>Symptom: A master controller reboots unexpectedly. The log files for the event listed the reason for the reboot as datapath exception.</p> <p>Scenario: This issue is observed in a 7240 controller running ArubaOS 6.3.1.1 in a master-local topology.</p>
82770	<p>Symptom: Using Aruba Discovery Protocol (ADP), access points did not discover the master controller after enabling Broadcast/Multicast (BC/MC) rate optimization. With this fix, enabling BC/MC rate optimization does not block ADP packets.</p> <p>Scenario: When BC/MC rate optimization was enabled on the VLAN, the controller dropped ADP packets from access points. This issue was not limited to a specific controller model or release version.</p>
95756	<p>Symptom: The firewall stall-detection feature was not enabled by default in ArubaOS 6.2.1.x. This issue is resolved, and firewall stall-detection is now enabled by default. The output of the show firewall CLI command now shows stall detection is enabled.</p> <p>Scenario: This issue occurred in ArubaOS 6.2.1.x, and is not limited to a specific controller model.</p>

Controller-Platform

Table 27: *Controller Platform Fixed Issues*

Bug ID	Description
90619 91950 92250 92273	Symptom: The controller WebUI stopped responding indefinitely. The fix ensures that the AirWave query fails if there is no firewall visibility. Scenario: This issue occurred when AirWave queried for firewall visibility details from a controller on which the firewall visibility feature was disabled. This issue was observed in controllers running ArubaOS 6.2 or later.
91541 94045 95079	Symptom: A controller rebooted due to low memory. Changes to how the controller uses buffers during the image copy process fixes this issue. Scenario: This issue occurred when there was continuous high traffic terminating on the control plane. This resulted in an internal component of the ArubaOS software to take up high memory. This issue was observed in 600 Series, 3000 Series, and M3 controllers running ArubaOS 6.1 and later versions.
95044	Symptom: Some access points went down when the controller to which they are connected rebooted. This issue is resolved by ensuring that the boot partition information is updated in the secondary bank of the controller. Scenario: This issue occurred when the controller rebooted due to a watchdog reset. This issue was not limited to any specific controller model or release version.

Controller-Software

Table 28: *Controller Software Fixed Issues*

Bug ID	Description
89460	Symptom: When an AP used adjacent DFS channels, that AP incorrectly detected RADAR and exhausted all DFS channels. If no non-DFS channels were enabled, the AP stopped responding to clients. Improvements that prevent incorrect RADAR detection resolve this issue. Scenario: This issue occurred on AP-135 access points using adjacent DFS channels, and was triggered when the AP misidentified a small data packet as a FCC type-5 RADAR packet, causing false RADAR detection.

IPv6

Table 29: *IPv6 Fixed Issues*

Bug ID	Description
74367	Symptom: Clients using temporary IPv6 addresses are not be able to communicate as traffic is getting dropped. The issue is been fixed by rotating the ipv6 addresses allocated to the client, and replacing the old IP address by new IP addresses Scenario: A client can support up to four IPv6 addresses. The usage of temporary IPv6 addresses on the clients replaced old IPv6 addresses allocated in user-table and sent traffic using these addresses. The issue occurred on the controllers that support IPv6 clients

RADIUS

Table 30: RADIUS Fixed Issues

Bug ID	Description
93689	<p>Symptom: When Windows phone clients run a script for 802.1X authentication, the controller sends a EAP Failure message. This issue is resolved by removing the EAP-Failure messages when the client times out during 802.1X authentication.</p> <p>Scenario: This issue was identified in ArubaOS 6.1.3.8, and was not limited to any specific controller mode.</p>

SNMP

Table 31: SNMP Fixed Issues

Bug ID	Description
94205	<p>Symptom: The MIB <code>sysExtFanStatus</code> cannot be queried. This issue is resolved by changes that ensure that the internal <code>fanCount</code> value is initialized for 7200 Series controllers.</p> <p>Scenario: This issue occurs on 7200 Series controllers running ArubaOS 6.2.x and 6.3.x. 6.3.1.1. This issue was triggered because the internal hardware monitoring process did not return the proper values for <code>fanStatus</code> SNMP queries.</p>

Spectrum UI

Table 32: Spectrum UI Fixed Issues

Bug ID	Description
76439	<p>Symptom: The Spectrum Analysis section of the ArubaOS WebUI fails to respond when a connected spectrum monitor is in a DOWN state. Changes to how the WebUI displays popup messages resolve this issue.</p> <p>Scenario: This issue occurred in ArubaOS 6.2.0.0, when anAP-105 access point in hybrid AP mode failed to appear as a connected spectrum monitor in the controller WebUI.</p>

WebUI

Table 33: WebUI Fixed Issues

Bug ID	Description
92340 92649	<p>Symptom: The WebUI of a controller failed to load in Internet Explorer 11 with the error message can't create XMLHttpRequest object: Object doesn't support property or method 'createXMLHttpRequest'. The ArubaOS WebUI is updated to be compatible with the new standards in Internet Explorer 11.</p> <p>Scenario: This issue was caused by differences between Internet Explorer 11 and Internet Explorer 10. This issue was observed in Internet Explorer 11 and not limited to any specific controller model or release version.</p>
93606	<p>Symptom: Clients were not displayed in the Monitoring > Controller > Clients page of the WebUI when filtered with AP Name. This issue is fixed by changing the <code>show user-table location <ap-name></code> command to <code>show user-table ap-name <ap-name></code>.</p> <p>Scenario: This issue was triggered by changes to CLI commands. This issue was observed in controllers running ArubaOS 6.2 and 6.3.</p>

Resolved Issues in ArubaOS 6.2.1.5

The following issues were resolved in ArubaOS 6.2.1.5:

802.1X Authentication

Table 34: 802.1X Authentication Fixed Issues

Bug ID	Description
89106	<p>Symptom: The class attribute was missing from RADIUS accounting messages sent to clients when previously idle clients reconnected to the network.</p> <p>Scenario: This issue occurred in a deployment using RADIUS accounting, where the RADIUS server sends class attributes in the access-accept messages for 802.1X authentication. In previous releases, when an idle user timed out from the network, ArubaOS deleted the class attribute for the user along with rest of the user data.</p> <p>This issue is resolved with the introduction of the delete-keycache parameter in the 802.1X authentication profile, which, when enabled, deletes the user keycache when the client's user entries get deleted. This forces the client to complete a full 802.1X authentication process when the client reconnects after an idle timeout, so the CLASS attributes will again be sent by the RADIUS servers.</p>

Air Management - IDS

Table 35: Air Management IDS Fixed Issues

Bug ID	Description
90330	<p>Symptom: An adhoc AP marked to be manually contained would not be contained unless the protect from adhoc feature was enabled. This issue is resolved by allowing traditional adhoc containment whenever enhanced adhoc protection is enabled, even if the protect from adhoc feature is not enabled.</p> <p>Scenario: This issue was observed on controllers running ArubaOS 6.2.x.</p>

AP-Datapath

Table 36: AP-Datapath Fixed Issues

Bug ID	Description
90645	<p>Symptom: The ap-name option in the command show datapath session ap-name did not take affect.</p> <p>Scenario: This issue was observed on ArubaOS 6.2.1.3 and any controller model can be impacted.</p>

AP-Platform

Table 37: AP-Platform Fixed Issues

Bug ID	Description
88389 89882 90175 90332	<p>Symptom: 802.11n-capable access points unexpectedly rebooted. The log files for the event listed the reason for the reboot as kernel page fault. Improvements in the wireless driver of the AP resolved this issue.</p> <p>Scenario: This issue was observed when a 802.11n-capable campus AP was in bridge forwarding mode and there was a connectivity issue between the AP and the controller. This issue was observed in 802.11n-capable access points running ArubaOS.</p>
89016	<p>Symptom: The SNMP OID wlanStaAccessPointESSID had no value when a client roamed from a down AP to an active AP. Improvements to internal processes that manage Layer-2 roaming resolve this issue.</p> <p>Scenario: This issue was observed when clients roamed between APs running ArubaOS 6.2.x</p>

AP-Regulatory

Table 38: AP-Regulatory Fixed Issues

Bug ID	Description
86764	<p>Symptom: The output of the show ap allowed channels command incorrectly indicated that AP-68 and AP-68P access points supported 5 GHz channels. This issue is resolved by changes that modify how ArubaOS displays the allowed channel list for AP-68 and AP-68P APs.</p> <p>Scenario: This issue was observed on AP-68 and AP-68P access points running ArubaOS 6.1.x and 6.2.x.</p>

AP-Wireless

Table 39: AP-Wireless Fixed Issues

Bug ID	Description
89046 89053 89058 84081 88044 88569 88631 88843 89044 89325 89326 89811 89901 92336 93335	<p>Symptom: An access point continuously stopped responding and rebooted. This issue was resolved by improvements to the wireless drivers in ArubaOS 6.1.3.11.</p> <p>Scenario: This issue was observed in AP-125 and AP-220 Series access points running ArubaOS 6.1.3.x when the clients disconnected from the network.</p>
88328 89623	<p>Symptom: Wireless clients experienced packet loss when connected to remote APs in bridge mode. This issue is fixed by changes that ensure some buffer is reserved for transmitting unicast traffic.</p> <p>Scenario: This issue was observed in AP-105 APs running ArubaOS 6.1.3.8 with high levels of multicast or broadcast traffic in the network. This issue was not limited to a specific controller model.</p>
90960	<p>Symptom: Microsoft® Surface Pro and Surface RT clients were unable to acquire an IP address or correctly populate the ARP table with a MAC address when connecting to an AP using 20 MHz channels on 2.4 GHz or 5 GHz radios. This issue is resolved by channel scanning improvements to APs in 20 MHz mode.</p> <p>Scenario: This issue was triggered when Microsoft Surface clients running Windows 8 or Windows 8.1 connected to 20 MHz APs running ArubaOS 6.1.3.8.</p>
91856	<p>Symptom: Certain 802.11b clients did not communicate with Aruba 802.11n-capable access points. Improvements in the wireless driver of 802.11n-capable access points resolve this issue.</p> <p>Scenario: This issue was observed when Denso® 802.11b handy terminals communicated with Aruba 802.11n-capable access points on channel 7. This issue was not limited to any specific controller model or release version.</p>

Base OS Security

Table 40: *Base OS Security Fixed Issues*

Bug ID	Description
84164 92279	<p>Symptom: Issuing the command <code>clear aaa device-id-cache mac <mac></code>, where <mac> was the MAC address of a wireless user that did not have an entry in the station table, caused the controller to stop responding. Improvements to the internal controller module that manages user authentication resolves this issue.</p> <p>Scenario: This issue occurred in 3000 Series controllers running ArubaOS 6.2.1.x.</p>
89453	<p>Symptom: The <code>show rights</code> command did not display all the user roles configured in the controller. This issue is resolved by a change that ensures that the output of this command displays all the user roles configured in the controller.</p> <p>Scenario: This issue was observed when more than 50 user roles were configured in a controller running ArubaOS 6.2.1.3.</p>
90233	<p>Symptom: Clients with a <code>logon</code> user role did not age out from the user-table after the <code>logon-lifetime</code> AAA timer expired. This issue is resolved by a change that ages out users with the <code>logon</code> user role if User Derivation Rule (UDR) is configured in the AAA profile.</p> <p>Scenario: This issue was observed when UDR was configured in the AAA profile with <code>logon</code> defined as the default user role. This issue was observed on controllers running ArubaOS 6.2.1.x.</p>
80396	<p>Symptom: An internal (<code>profmgr</code>) process crashed on a controller and users were not able to change, add, or delete the corrupted configuration. This issue is fixed adding additional checks that ensure internal data is copied to a valid location with correct references.</p> <p>Scenario: This issue occurred when a configuration profile referring to an external RADIUS server, for example, the <code>aaa-server-group</code> profile, was changed and pointed to another server. This caused the data structure and refcounts to the new RADIUS server to become invalid. This issue was not specific to any profile or the RADIUS server associated with a controller. This issue was observed on controllers running ArubaOS 6.1.3.x and 6.2.x.</p>
92674 93609	<p>Symptom: Class attribute was missing in Accounting STOP packet. This issue is resolved by not resetting the counters when an IPv6 user entry is deleted.</p> <p>Scenario: This issue occurred when the counters were reset during an IPv6 user entry aged out. This issue was not limited to any specific controller or ArubaOS version.</p>

Captive Portal

Table 41: *Captive Portal Fixed Issues*

Bug ID	Description
91442	<p>Symptom: When configuring the captive portal login page using the master controller's command line interface, the question mark symbol was not getting added to the configuration or pushed to the local controller. This issue is resolved by making sure that the master controller's command line interface accepts the question mark symbol as part of the login page configuration.</p> <p>Scenario: This issue was observed when synchronizing the captive portal configuration from the master controller to the local controller.</p>

Controller-Datapath

Table 42: *Controller-Datapath Fixed Issues*

Bug ID	Description
88469	<p>Symptom: A controller denied any FTP download which used Extended Passive mode over IPv4. This issue is resolved by modifying the FTP ALG to handle the Extended Passive mode correctly.</p> <p>Scenario: This issue was observed when an IPv4 FTP client used the Extended Passive mode. In such a case, the FTP ALG on the controller detected it as a Bounce Attack and denied the session. This issue was not limited to a specific controller model or release version.</p>
87846 87949 88039 88226 88445 89433 89539 89641 90024 90458 90469 90746 90896 91853 92464 92466 92827 92828 92829 92830 92832	<p>Symptom: A controller stopped responding to network traffic and rebooted. The log file for the event listed the reason for the reboot as Datapath timeout. This fix ensures that the CPU livelock does not recur.</p> <p>Scenario: This issue occurred on 7200 Series controllers running ArubaOS 6.3.0.1 and 6.2.x.</p>
90454	<p>Symptom: A remote AP unexpectedly rebooted because it failed to receive heartbeat responses from the controller. Changes to the order in which new IPsec SAs are added and older IPsec SAs are removed resolve this issue.</p> <p>Scenario: This issue occurred after a random IPsec rekey, and was triggered when the outbound IPsec SA was deleted before the inbound IPsec SA was added. This removed the route cache for the inner IP, causing the session entry to incorrectly point to the default gateway, and preventing heartbeat responses from reaching the AP.</p>

Controller-Platform

Table 43: *Controller-Platform Fixed Issues*

Bug ID	Description
82736 82875 84022 85628 86005 86572 86589 87410 87505 87587 88332 88351 88434 88921 89818 90909 91269 91308 91370 91517 93294	<p>Symptom: A controller rebooted unexpectedly. Changes in the watchdog implementation on the controller resolve the issue.</p> <p>Scenario: Log files for the event indicated the reason for the reboot as soft watchdog reset. This issue was not limited to any specific controller model or release version.</p>
86216 85566 87090 87635 88321 88387 88699 89436 89727 89839 89911 90162 90338 90481 91193 91387 91941 92139 92187 92516 92808 93630 93693 93931 94308	<p>Symptom: During a kernel panic or crash, the panic dump generated by the controller was empty. New infrastructure has been added to improve the collection of crash dumps.</p> <p>Scenario: This issue impacts 3000 Series, 600 Series, and M3 controllers and was observed in ArubaOS 6.1.3.7.</p>
83502 83762 85355 85370 86029 86031 88005 89636 92823	<p>Symptom: A controller rebooted unexpectedly. Changes in the watchdog implementation on the controller resolve the issue.</p> <p>Scenario: Log files for the event indicated the reason for the reboot as user pushed reset. This issue was identified in ArubaOS 6.1.3.x, and is not limited to any specific controller model.</p>

Table 43: Controller-Platform Fixed Issues

Bug ID	Description
89155	<p>Symptom: 600 Series controllers experienced high levels of CPU usage during bootup, triggering the warning messages Resource 'Controlpath CPU' has exceeded 30% threshold. This issue is resolved by changes to internal CPU thresholds that better reflect expected CPU usage levels.</p> <p>Scenario: This issue was observed in controllers running ArubaOS 6.1.2.3.</p>
90751 90633 90863 91154 91138 91474 91656	<p>Symptom: Controllers continuously stopped responding and rebooted. Enhancements to memory allocation resolved this issue.</p> <p>Scenario: The issue occurred when an internal module (FPCLI) stopped responding due to memory corruption. This issue was observed in M3 controllers and is not limited to a specific version of ArubaOS.</p>
91383	<p>Symptom: Issuing a show command causes the controller command-line interface to display the error Module Configuration Manager is busy. Please try later. Improvements to how the controller manages HTTP session keys resolve this issue.</p> <p>Scenario: This issue occurred when issuing show commands from the command-line interface of a 3000 Series standby controller, and is triggered when the database synchronization process attempts to simultaneously replace and add an HTTP session key in the user database.</p>

DHCP

Table 44: DHCP Fixed Issues

Bug ID	Description
90611 91512	<p>Symptom: The Dynamic Host Configuration Protocol (DHCP) module crashed on a controller and users were not able to perform a new DHCP configuration. Improvements to internal DHCP processes fix this issue in ArubaOS 6.2.1.5.</p> <p>Scenario: This issue was triggered by a race condition that caused the DHCP wrapper process to continually crash and restart. This issue was not specific to any controller model or release version.</p>

Hardware Management

Table 45: Hardware Management Fixed Issues

Bug ID	Description
87481	<p>Symptom: The 7200 Series controllers returned an invalid value when an SNMP query was performed on the internal temperature details (OID .1.3.6.1.4.1.14823.2.2.1.2.1.10). The fix ensures that the SNMP attribute is set correctly for the temperature details.</p> <p>Scenario: This issue was limited to 7200 Series controllers running ArubaOS 6.3 or later versions.</p>

IPv6

Table 46: *IPv6 Fixed Issues*

Bug ID	Description
88814	<p>Symptom: Users connected to the controller with derived VLANs received IPv6 router advertisements from VLANs other than those to which the clients were associated. This issue is resolved by updating the controller datapath with a router advertisement conversion flag so the datapath converts multicast router advertisements to unicast.</p> <p>Scenario: This issue was observed in IPv6 networks with derived VLANs and was not limited to a specific controller model or release version.</p>

Master-Redundancy

Table 47: *Master-Redundancy Fixed Issues*

Bug ID	Description
80041	<p>Symptom: The database that synchronizes settings between a master and a backup controller failed to synchronize. Log files for the event listed the reason for the error as Last failure cause: Standby switch did not respond to the start request or is not ready. This issue is resolved by changes that allow ArubaOS to ignore any aborted database synchronization sequence number on the master controller. This allows subsequent database synchronization attempts to proceed without waiting for the standby controller to respond to the previously aborted synchronization attempt.</p> <p>Scenario: This issue was triggered when the standby controller database was out-of-sync with the master controller. Any switchover during this out-of-sync state caused the controller to be in an inconsistent state. This issue was observed on controllers in a master-standby configuration and was not specific to a release version.</p>

Mesh

Table 48: *Mesh Issues*

Bug ID	Description
92614	<p>Symptom: A Mesh Point rebooted frequently as it could not connect to a Mesh Portal.</p> <p>Scenario: This issue occurred when the transmission power on the Mesh Point was very low compared to the configured power. This issue was observed in AP-105 and AP-175 access points with controllers running ArubaOS 6.1.x and later versions.</p>

Mobility

Table 49: *Mobility Fixed Issues*

Bug ID	Description
88281	<p>Symptom: IP mobility entries were not cleared even when the client leaves the controller and user entries aged out. Additionally, the command clear ip mobile host <mac-address> did not clear the stale entry.</p> <p>Scenario: This issue was caused by a message loss between the controller's Mobile IP and Authentication internal processes. This message loss caused the affected clients to become stuck. All controller models running ArubaOS 6.3.x, 6.2.x, and 6.1.x were impacted by this issue.</p>

Remote AP

Table 50: Remote AP Fixed Issues

Bug ID	Description
85473	<p>Symptom: A RAP-3WN AP using a USB modem was unable to come up as an active AP until it rebooted. Changes to how the controller determines modem product IDs resolves this issue. As a result of this issue, the default dial string for a TATA photon plus Huawei E156 USB modem is changed from AATDDTT##777777 to AATDDTT**9999##.</p> <p>Scenario: This issue occurred on a RAP-3WN ArubaOS AP running 6.2.1.2 when it was connected to a Huawei E156 modem.</p>
86096	<p>Scenario: DHCP clients connected to an AP received only the first entry of the DNS server list, even though the controller was configured with multiple DNS server IP addresses. With the new fix, DHCP clients get the complete list of DNS server IP addresses.</p> <p>Scenario: This issue was observed on controllers running ArubaOS 6.2.x when a user configured multiple DNS servers in local Remote AP (RAP) DHCP pool. This issue was observed when a user configured multiple DNS server in local Remote AP (RAP) DHCP pool, DHCP clients received only the first entry of the DNS server list. This issue was observed in controllers running ArubaOS 6.2 and later versions.</p>
86650	<p>Symptom: A controller sent continuous RADIUS requests for the clients connected behind the wired port of a remote AP (RAP). This issue is resolved by ArubaOS enhancements that prevent memory corruption.</p> <p>Scenario: This issue was observed when a RAP used a PPPoE uplink and operated as a wired AP in split-tunnel or bridge mode. This issue occurred on ArubaOS running 6.1.3.6, and was not limited to any specific controller model.</p>
90355	<p>Symptom: AP-70 and RAP-108 access points connecting to the network using a cellular uplink were not able to achieve a 3G connection. This issue is resolved by improvements to the AP boot process, and changes that allow cellular modems to support multiple ports on the AP.</p> <p>Scenario: This issue was observed in 6.3.x. and 6.2.x when AP-70 and RAP-108 access points connected to a Huawei® E220 Modem.</p>

Voice

Table 51: Voice Fixed Issues

Bug ID	Description
74401 88173 88174	<p>Symptom: Avaya® IP desk phones did not register in the controller and the show voice call-cdrs and show voice-client status commands displayed incorrect call status for these phones. Changes to the H.323 parser in the controller fixed the issue.</p> <p>Scenario: This issue was observed when an Avaya IP desk phone was connected to the wired port of an access point. This issue was observed on controllers running ArubaOS 6.2.x.</p>
77716 88996 90000	<p>Symptom: Incompatibility issues observed between 3600 controllers and a Cisco CUCM using SCCP version 20. Users were able to make and receive calls using a Cisco phone but there was no audio. This issue is resolved by changes to that allow the controller to handle Open Receive Channel Acknowledge (ORCA) messages for SCCP Version 20.</p> <p>Scenario: The Cisco CUCM was compatible with the Skinny Client Control Protocol (SCCP) version 20, while the 3600 controller supported only up to version 17 of the SCCP. This incompatibility issue resulted in media traffic not passing through the 3600 controller as it was not able to parse the SCCP signaling packets. This issue was observed in a 3600 controller running ArubaOS 6.0 or later.</p>
86683	<p>Symptom: The show voice call-cdrs and show voice client-status command outputs did not display the call details for Lync wired clients with media classification configured on session ACL. This issue is resolved by ensuring to handle the message appropriately for wired clients.</p> <p>Scenario: This issue was observed when Lync clients were identified as voice clients via media classification. This issue occurred on ArubaOS running 6.2.x and not limited to any specific controller version.</p>

Table 51: Voice Fixed Issues

Bug ID	Description
93517	<p>Symptom: Access points rebooted unexpectedly resulting in wireless clients to lose network connectivity. Releasing CDR events for AP statistics and AP event in the CDR buffer resolved the issue.</p> <p>Scenario: This issue was observed in a VoIP deployment when the Station Management (STM) process that handles AP management and user association crashed on the controller. This issue was observed in controllers running ArubaOS 6.1 and later versions.</p>

WebUI

Table 52: WebUI Fixed Issues

Bug ID	Description
88398	<p>Symptom: The Dashboard > Security page of a controller did not allow network administrators to manually contain or reclassify a group of detected rogue APs. This issue is fixed by adding support to select multiple rogue APs.</p> <p>Scenario: This issue occurred when multiple rogue APs were selected in the Dashboard > Security page. This issue was observed in controllers running ArubaOS 6.2.1.3.</p>
90110	<p>Symptom: The ArubaOS Campus WLAN Wizard was not accessible.</p> <p>Scenario: The Campus WLAN wizard was not accessible due to the presence of an ampersand (&) in the LDAP server filter. LDAP server filters can now include an ampersand. This issue was observed on a 650 controller running ArubaOS 6.2.1.3 but could impact any controller model.</p>

Resolved Issues in ArubaOS 6.2.1.4

The following issues were resolved in ArubaOS 6.2.1.4:

802.1X Authentication

Table 53: 802.1X Authentication Fixed Issues

Bug ID	Description
71930	<p>Symptom: Client 802.1X authentication failed after the controller uploaded a new security certificate. This issue was the result of a rare condition where values in a RSA private key were less than 128 bytes in length, and is resolved by changes to the process by which the controller manages RSA keys.</p> <p>Scenario: This issue occurred on controllers running ArubaOS 6.1.3.2 in a master-local topology when the controllers were updated with new certificates.</p>
85896	<p>Symptom: A controller rebooted after an internal controller module stopped responding. Internal memory improvements resolve this issue.</p> <p>Scenario: This issue was caused by memory corruption while the controller processed 802.1X packets in an error flow. It was observed in controllers running ArubaOS 6.1 or later, and is not specific to any controller model.</p>
86162	<p>Symptom: Clients using WPA2-PEAP authentication failed to authenticate due to an EAP-failure error after the controller switched to a new 2k server certificate. This issue is fixed by changes to how RSA constants for XLR-SAE are handled as they are downloaded from the assigned server certificate.</p> <p>Scenario: This issue was triggered by some 2k server certificates. This issue was observed on 600 Series controller platforms with XLR/XLS processors, 3000 Series, and 600 Series controllers running ArubaOS 6.2.x.</p>

AP-Datapath

Table 54: *AP-Datapath Fixed Issues*

Bug ID	Description
86469 89714	Symptom: An AP unexpectedly rebooted due to errors triggered by internal timers. Changes that prevent address bit flipping resolve this issue. Scenario: This issue was observed in AP-120 Series access points associated to a controller that upgraded from ArubaOS 6.1.3.7 to ArubaOS 6.1.3.x.

AP-Regulatory

Table 55: *AP-Regulatory Fixed Issues*

Bug ID	Description
83338	Symptom: AP-93 access points configured to use the regulatory maximum transmission power displayed mismatching EIRP and the maximum EIRP values in the output of the show ap active and show ap radio-summary commands. An improvement to the algorithm used to determine the regulatory limit resolves this issue. Scenario: This was observed on AP-93 access points, and was not limited to any specific release of ArubaOS.

AP-Wireless

Table 56: *AP-Wireless Fixed Issues*

Bug ID	Description
81508	Symptom: Clients associated to AP-93 access points configured as remote APs aged out and were deauthorized. This issue is resolved by additional checks in station ageout behavior that ensure clients are not aged out unnecessarily. Scenario: This was observed on AP-93 access points running ArubaOS 6.2.0.0.

ARM

Table 57: *ARM Fixed Issues*

Bug ID	Description
87026 86951	Symptom: The mode-aware Adaptive Radio Management (ARM) feature changed an unexpectedly high number of APs using the 5 GHz band into Air Monitors (AMs). This issue is resolved by improvements to interference idx calculations. Scenario: This issue occurred in a high density deployment when an AP radio was associated to multiple Virtual APs. It was triggered when the Signal-to-Noise Ratio (SNR) of the radio was counted many times when the neighbor's view of the coverage index was calculated. This issue was observed in ArubaOS 6.2.1.2 and was not specific to any AP or controller model.

Base OS Security

Table 58: *Base OS Security Fixed Issues*

Bug ID	Description
81390	<p>Symptom: When clients connected using EAP-TLS authentication, the following error message appeared in the controller error log files: <ERRS> [authmgr] user.c, derive_role2:5759: {04:f7:e4:26:c3:fb-??} Missing server in attribute list, auth=802.1x, utype=L2. Improvements in the process that manages server names resolves this issue.</p> <p>Scenario: This issue was observed when Common Name (CN) lookup was disabled in the client certificate. The issue was not specific to any ArubaOS version or controller model.</p>
92817	<p>Symptom: Wireless clients were blacklisted even when the rate of the IP Session did not exceed the threshold value set. This issue is resolved by increasing the storage of the threshold to 16 bits.</p> <p>Scenario: This issue was observed if the threshold of the IP Session rate was set to a value greater than 255. This issue was observed in controllers running ArubaOS 6.x.</p>

Captive Portal

Table 59: *Captive Portal Fixed Issues*

Bug ID	Description
87294	<p>Symptom: When user role was assigned by a captive portal profile, the ACL configuration synchronized from a master controller to a standby controller did not include the captive portal whitelist. This issue is resolved by the addition of internal checks that verify that a configured whitelist is correctly attached to the user role.</p> <p>Scenario: This issue was identified in a network topology with a master controller, standby controller and four local controllers running ArubaOS 6.2.1.2.</p>

Controller-Datapath

Table 60: *Controller-Datapath Fixed Issues*

Bug ID	Description
84071	<p>Symptom: A controller stopped responding and unexpectedly rebooted. The log files for the event listed the reason for the reboot as Datapath exception. Improvements to how frame headers are managed resolve this issue.</p> <p>Scenario: This issue occurred when an SSL-encapsulated invalid ESP frame was received and processed by the controller. It occurred on 3000 Series and 7200 Series controllers running ArubaOS 6.2.1.0.</p>
83029	<p>Symptom: A 7200 Series or 3000 Series controller with the firewall-visibility feature enabled may fail to respond if the controller has a high number of IPv6 sessions. This issue is resolved by improvements to IPv6 session management.</p> <p>Scenario: This issue occurred on a controller running ArubaOS 6.2.1.0. The datapath CPUs utilization reaches 100% and fails to return to nominal levels.</p>

Controller-Platform

Table 61: *Controller-Platform Fixed Issues*

Bug ID	Description
85398	<p>Symptom: A controller configured as a DNS server responded to DNS queries, even if the IP domain lookup and captive portal redirect features were disabled. This issue is resolved by a change that prevents the controller from providing DNS services when DNS hostname translation is disabled using the no ip domain lookup command.</p> <p>Scenario: This issue occurred on a 3400 controller configured to operate as a DNS server while running ArubaOS 6.1.3.6.</p>
85685	<p>Symptom: An M3 controller module running ArubaOS 6.1.3.8 stopped responding and rebooted. The log files for the event listed the reason for the crash as fpapps: Segmentation fault. The internal fpapps process handles the VLAN interfaces on the controller. Changes to the internal fpapps process fix the issue.</p> <p>Scenario: This issue was observed when the VLAN interface on the controller constantly changed between an UP and DOWN state, resulting in a VRRP status change. This issue is not limited to any specific controller model or software version.</p>
86266	<p>Symptom: In rare cases, issuing commands through a telnet shell caused an internal controller process to stop responding, triggering an unexpected controller reboot. This issue is resolved by changes that prevent ArubaOS from referencing null pointers within the software.</p> <p>Scenario: This issue was triggered by varying sequences of commands issued via the telnet shell, and is not specific to any controller model or software version.</p>
87721 88368 89434 89441 89742 89924 90029 90059 90492 90634 91777 92675 94053	<p>Symptom: When the controller performs an SNMP walk on a voice client, an internal controller process that manages client stations stopped responding. Changes to how SNMP entries are deleted resolve this issue.</p> <p>Scenario: This issue occurred on a controller running ArubaOS 6.3.x and ArubaOS 6.2.x, with voice clients connected to the controller using a wired connection.</p>
87794 88311 88360 88683 88740 88505 88833	<p>Symptom: A 7200 Series controller unexpectedly rebooted. Controller log files listed the reason for the event as a datapath timeout. Improvements to how tunnels are created in the internal controller datapath resolve this issue.</p> <p>Scenario: This issue occurred in 7200 Series controllers running ArubaOS 6.2.1.x.</p>

Intrusion Detection System

Table 62: *Intrusion Detection System Fixed Issues*

Bug ID	Description
86681	<p>Symptom: The IDS (Intrusion Detection System) feature frequently triggered false alarms. ArubaOS resolves this issue by changing the default setting for the IDS Large Duration Attack Detection feature from enabled to disabled.</p> <p>Scenario: This issue occurred because legitimate frames sent with a large duration were also treated as an IDS Large Duration attack, triggering false alarms.</p>

Mobility

Table 63: *Mobility Fixed Issues*

Bug ID	Description
88063	<p>Symptom: If a controller uses the IP mobility feature and RADIUS server vendor specific attributes (VSAs) to derive a user role for RADIUS-authenticated clients, the user role assigned to the client at its home agent (HA) can incorrectly change to the default AAA profile role after that client roams to a foreign agent (FA). This issue is resolved by improvements to mobile IP role management.</p> <p>Scenario: This issue occurs when a client with a VSA-derived user role roams between controllers in an IP mobility domain. It is triggered when a user gets a dynamically assigned role from a foreign agent, and that role is not present on the client's home agent. As a result, the client gets assigned the default AAA profile role when it roams back to its home agent.</p>

PPPoE

Table 64: *PPPoE Fixed Issues*

Bug ID	Description
85398	<p>Symptom: A controller was not able to connect to the internet using a Point-to-Point Protocol over Ethernet (PPPoE) connection. This issue is fixed by modifying how PPPoE handles usernames that contain special characters.</p> <p>Scenario: This issue occurred if the PPPoE connection was not established with the internet service provider server because the PPPoE username contained special characters (for example: #0001@t-online.de). This issue was observed in ArubaOS 6.1.3.7, and is not specific to any controller model.</p>

WebUI

Table 65: *WebUI Fixed Issues*

Bug ID	Description
73459	<p>Symptom: The output of the show acl hits CLI command and the firewall hits information that appears on the UI Monitoring page of the controller WebUI displayed conflicting information.</p> <p>Scenario: This issue was triggered by formatting errors in the XML response from the controller to the WebUI that appeared when the output was larger than a specified limit. This issue was not limited to any specific controller model or software version.</p>
80233 82724 83235 83949 84159 85375 85445 85686 85805 86423 86424 86632 86839 86933 87335 87933 88826 89523 91212	<p>Symptom: The Monitoring > Access Points and Monitoring > Network > All Access Points pages of the controller WebUI showed APs as down, even if they are shown as up in the command-line interface. Improvements to an internal process that handles AP IP addresses resolves this issue.</p> <p>Scenario: This issue occurred on a master/local topology with one 6000 master controller and two local controllers running ArubaOS 6.2.1.0.</p>

Resolved Issues in ArubaOS 6.2.1.3

The following issues are resolved in ArubaOS 6.2.1.3:

Air Management - IDS

Table 66: Air Management - IDS Fixed Issues

Bug ID	Description
84889	Symptom: False alarms for AP spoof detection were observed in ArubaOS 6.2.1.2. This issue is resolved by removing the Detect AP Spoofing check that looks for frames sent to the AP on the wrong channel. Scenario: This issue occurred when the Detect AP Spoof option was enabled in the Configuration > Wizards > Configure WIP page of the WebUI. This issue was not specific to any software version.

AP-Platform

Table 67: AP-Platform Fixed Issues

Bug ID	Description
64778 63852 84004	Symptom: Users were unable to make calls to IP phones. This issue is fixed by increasing the maximum acceptable frame size to 1518 bytes in RAP-3WN AP's Ethernet driver. Scenario: This issue occurred when the IP phone was connected to the Ethernet interface of a RAP-3WN AP, and was observed in ArubaOS 6.2.1.1.
85397 78289	Symptom: An internal controller module stopped responding when a client disconnected. This issue is resolved by changes to references to objects in memory after the controller frees and allocates memory to another object. Scenario: This issue was triggered by aggressive client station roaming and power save settings, and was not specific to any software version.

AP-Datapath

Table 68: AP-Datapath Fixed Issues

Bug ID	Description
85279	Symptom: In a master-local topology, all users connected to an AP in bridge or split-tunnel forwarding mode experienced low throughput even though bandwidth contracts were not configured. This issue is resolved by correcting the role-to-bandwidth-contract mapping table. Scenario: This issue occurred on controllers running ArubaOS 6.2 or later, due to incorrect mapping of a user role to the bandwidth contract when the ACL IDs in the master and local controllers were different for the same role. It was also observed during an authentication process restart.

AP-Regulatory

Table 69: AP-Regulatory Fixed Issues

Bug ID	Description
76222	Symptom: The country code for Algeria was not supported on AP-105, AP-92, and AP-93 access points. The country code for Algeria is added in the country list for these APs to fix this issue. Scenario: This issue was observed in ArubaOS 6.2.1.0 and was not limited to a controller model.

AP-Wireless

Table 70: AP-Wireless Fixed Issues

Bug ID	Description
85806	<p>Symptom: Excessive jitter was observed in Blackberry devices making voice calls when the controller enabled the Wireless Multimedia UAPSD (Unscheduled Automatic Power Save Delivery) option from the Configuration > Wireless > AP Configuration > Select AP > SSID profile > Advanced tab in the WebUI. This issue is fixed in ArubaOS 6.2.1.3 by enhancing the packet queuing mechanism for UAPSD hardware transmit queues, reducing packet loss.</p> <p>Scenario: This issue was triggered by high packet loss in a UAPSD-enabled configuration. This issue was observed in AP-124, AP-125, and AP-105 access points running ArubaOS 6.1.3.6.</p>

Base OS Security

Table 71: Base OS Security Fixed Issues

Bug ID	Description
72093	<p>Symptom: A controller did not display a portion of the output of the show run result command when it is sent using SSH/telnet connections to a teraterm client. An increase in the socket buffer size resolves this issue.</p> <p>Scenario: This issue was not limited to a specific controller model or software version.</p>
80006 85167	<p>Symptom: The internal controller module that manages authentication stopped responding. Enhancements to the internal code that provide valid values to the authentication process fixes this issue in ArubaOS 6.2.1.3.</p> <p>Scenario: This issue occurred when XML API was used to add or modify a user with a session timeout configured on for that user. The issue was not specific to a controller model or a software version.</p>
80805 81775 85642	<p>Symptom: Some wireless users were displayed as wired users with an incorrect tunnel ID in the user table. Disabling the wired-ap parameter in the ap-group profile fixes this issue in ArubaOS 6.2.1.3.</p> <p>Scenario: This issue occurred when some APs rebootstrapped and the wired-ap parameter was enabled in the ap-group profile. This issue was not specific to any controller model or a software version.</p>
81458	<p>Symptom: Wired user-entries were displayed in the user-table even though wired users were not connected to any of the APs. This issue is resolved by clearing the entries for the table which tracks the ap-wired ports in the authentication module when an internal module (STM) was restarted.</p> <p>Scenario: This issue occurred when the user entries for ap-wired ports were not cleared in the table if the internal controller module that handles client stations restarted. The issue was not specific to a controller model or a software version.</p>
83776	<p>Symptom: Atheros clients did not support multiple relay counters using WPA-TKIP encryption and were unable to connect to the network after upgrading to ArubaOS 6.1.3.8. This issue is fixed by disabling the use of a multiple Traffic Identifier (TID) for WPA-TKIP.</p> <p>Scenario: This issue was observed when Wireless Multimedia Extensions (WMM) was enabled and the atheros clients did not support multiple relay controllers.</p>
84628 86814	<p>Symptom: A 6000 controller unexpectedly rebooted. Log files for the event listed the reason for the reboot as Datapath timeout. This issue is resolved by validating the bridge entries for VoIP clients.</p> <p>Scenario: This issue occurred when an invalid bridge value was computed and stored in an internal controller module. This issue is occurred in Aruba 6000 controllers running ArubaOS 6.2.0.0.</p>
85519	<p>Symptom: One or more SSH (Secure Shell) sessions to a controller failed when multiple simultaneous SSH sessions occurred. This issue is resolved by updates that ensure every SSH Daemon process corresponding to a SSH login session uses a different IPC (Inter-Process Communication) port number.</p> <p>Scenario: This issue was triggered by sshd processes using the same IPC port number, causing collisions when multiple SSH sessions tried to authenticate. This issue was observed in ArubaOS 6.1.x and 6.2.x.</p>

Controller-Datapath

Table 72: *Controller-Datapath Fixed Issues*

Bug ID	Description
81214 82914 85597 87043 87338	Symptom: High central processing unit (CPU) utilization on a network processors resulted in loss of IP connectivity for some users. The issue is resolved by fixing the automatic update of the clients route cache entries. Scenario: This issue was caused by a loop while routing L2 Virtual Local Area Network (VLAN) traffic. It was observed on controllers running ArubaOS 6.2 and routing L2 VLAN traffic.

Controller-Platform

Table 73: *Controller-Platform Fixed Issues*

Bug ID	Description
80956 81014 81555 83239	Symptom: A controller crashed and rebooted after upgrading from ArubaOS 6.1.3.6 to 6.1.3.7. The log files for the event listed the reason for the crash as watchdog timeout . The interrupt handler for packet parsing is modified to ensure that CPU is not overwhelmed with traffic packets. Scenario: A race condition triggered the controller crash in a high-traffic deployment. This issue was not specific to any controller models.
83738	Symptom: A crash was observed in all APs associated to the local controller, followed by Access Control Lists (ACLs) configuration loss. Updates to the banner delimiter fixes this issue. Scenario: This issue was caused by banner message-of-the-day (motd) with an exclamation point (!) as a delimiter, because the same character ! is used to exit from a sub-mode command. The issue was not limited to a specific versions of ArubaOS.
84825	Symptom: A 650 controller crashed or failed to respond. This issue is resolved by adding checks to deny access to invalid DRAM channels for the 650 controller. Scenario: This issue was observed on a 650 controller running ArubaOS 6.1.3.7.

DHCP

Table 74: *DHCP Fixed Issues*

Bug ID	Description
77280	Symptom: Issuing the show running-config command from the command-line interface of a controller running ArubaOS 6.2.0.1 triggered the error Module DHCP Daemon is busy. Please try later . Improvements to how DHCP pool user options are generated resolved this issue. Scenario: This issue occurred when controllers configured with DHCP pools used nonalphanumeric characters in the pool name, resulting in bad syntax when DHCP user options were generated in the configuration file.

Local Database

Table 75: *Local Database Fixed Issues*

Bug ID	Description
84494	<p>Symptom: A controller unexpectedly rebooted. The log files for the event listed the reason for the reboot as Nanny rebooted machine - udbserver process died. This issue is resolved by improvements to how MYSQL database failures are handled, in that ArubaOS better validates returned values and checks for missing values in certain failure scenarios.</p> <p>Scenario: This issue occurred on a standalone master 7210 controller with one associated AP-135 access point.</p>

OSPF

Table 76: *OSPF Fixed Issues*

Bug ID	Description
82730	<p>Symptom: A controller failed to add the default route when a neighboring router advertised the default route. This issue is resolved by ensuring that the default route is not missed while adding the route information.</p> <p>Scenario: This issue was not limited to a specific controller model and was observed in ArubaOS 6.2.1.0.</p>

Remote AP

Table 77: *Remote AP Fixed Issues*

Bug ID	Description
74024	<p>Symptom: When a client send DHCP packets along with 802.1X packets, an IP address is returned even if 802.1X is not authenticated. As a result, the slot/port information displayed in the user table is incorrect for wired users connected to a remote AP. This issue is resolved by improvements that correctly update the slot/port information.</p> <p>Scenario: This issue was observed in ArubaOS controllers, and RAP-3WN, and RAP-5 access points.</p>
78914	<p>Symptom: Stale user entries are present in the controller when a user moves from one AP coverage to another, if the new AP has a different VLAN configuration for the same Extended Service Set Identification (ESSID). This issue is resolved by removing the split-tunnel mobility that triggered the error.</p> <p>Scenario: This issue occurs if the first AP deletes the user entry without notifying the controller when the user moves from one AP to another. This issue was observed in APs running ArubaOS versions prior to 6.2.1.3.</p>
81245	<p>Symptom: The user table contained stale entries for users that aged out or disassociated from the network. Internal improvements to the user table resolve this issue.</p> <p>Scenario: This issue occurred when users associated to a AP in split-tunnel forwarding mode and used captive portal authentication roam to multiple APs exhibiting the same ESSID.</p>
84752 84391 84893 85160 85629 86217 86339 86372 86375 86738	<p>Symptom: Campus APs (CAPs) and Remote (RAPs) rebooted after upgrading the software to ArubaOS 6.2.1.3. Memory improvements resolve this issue.</p> <p>Scenario: This issue was triggered by to insufficient memory and was not specific to any controller or AP model.</p>

Table 77: Remote AP Fixed Issues

Bug ID	Description
86742 89701	
85499	<p>Symptom: In some instances, calls from IP phones connected to a RAP-3WN AP failed because the AP dropped packets. VLAN tagging improvements resolve this issue.</p> <p>Scenario: This issue occurred on IP phones connected to an AP in tunnel forwarding mode, and was first identified in ArubaOS 6.2.0.2.</p>
85053	<p>Symptom: A controller frequently stopped responding and rebooted in a topology with split-tunnel wired users in a configuration with the RADIUS accounting enabled. This issue occurred in Aruba 6000 controllers running ArubaOS 6.2.1.1.</p> <p>Scenario: This issue was identified in ArubaOS 6.2.1.1, when a RADIUS server was configured on the controller.</p>

RADIUS

Table 78: RADIUS Fixed Issues

Bug ID	Description
84060 85623	<p>Symptom: The source interface for a RADIUS server configured at a global level was not available after the controller rebooted. Changes that prevent source interface values from being lost after a reboot resolve this issue.</p> <p>Scenario: This was an intermittent issue and was not limited to a specific controller model or software version.</p>
85277	<p>Symptom: The AvgRspTm field in the output of the show aaa authentication-server radius statistics command was incorrectly set to 0 in a software image for a 7200 Series controller. This issue is resolved by changing parts of the software which were initially specific only to the M3 controller module platform, allowing the value of the AvgRspTm field to correctly update, and increasing controller stability.</p> <p>Scenario: This issue was identified in an ArubaOS 6.2.1.1 software image for a 7200 Series controller, when a RADIUS server was configured on the controller.</p>

Role/VLAN Derivation

Table 79: Role/VLAN Derivation Fixed Issues

Bug ID	Description
77242	<p>Symptom: Changes to the ArubaOS External Service Interface (ESI) Syslog parsing rule were not reflected in the user table, and changes to a user role was reflected only in the system table and controller datapath. This issue is fixed by updating the user table with the ESI role-change.</p> <p>Scenario: This issue was observed during a role-change event using ESI. This issue was observed in controllers and APs running ArubaOS 6.1.3.x.</p>

SNMP

Table 80: *SNMP Fixed Issues*

Bug ID	Description
77584 81499	<p>Symptom: An SNMP get request to poll <i>sysExtCardStatus</i> for the operational status of any installed cards could return the message “No such instance currently exists at this OID” and trigger an alert. Improvements to SNMP polling allow a get request to <i>sysExtCardStatus</i> to display the cached information from the previous poll status instead of an error message.</p> <p>Scenario: This issue was identified in ArubaOS 6.1.2.5, and occurred when the SNMP request was issued while the internal controller hardware monitor polled for hardware status. The SNMP request would time out, but the controller would return the error message instead of a timeout message.</p>

Station Management

Table 81: *Station Management Fixed Issues*

Bug ID	Description
83091 83547	<p>Symptom: Active APs of a local controller were not displayed on the master controller when the local controller showed the APs were active on the master controller. A change that introduces a new action to handle the race condition fixes this issue.</p> <p>Scenario: This issue was triggered by a race condition which resulted in creating session entries before IPsec tunnel and Network Address Translation (NAT) rules were created. The session removal mechanism could not remove the session entries without NAT flags. This issue was observed in controllers running ArubaOS 6.2.1.0.</p>
84718 84719 84725	<p>Symptom: The internal controller module that manages station authentication stopped responding and temporarily prevented clients from associating to the network. This issue is resolved by adding validations to prevent this controller module from crashing.</p> <p>Scenario: This issue was not limited to a specific controller model or release version.</p>

Voice

Table 82: *Voice Fixed Issues*

Bug ID	Description
83517 84723	<p>Symptom: The process that handles the AP management and user association crashed when voice clients were cleared. This impacted all the wireless clients and voice clients associated to the controller. Enhancements to the internal code fixed this issue in ArubaOS 6.2.1.3.</p> <p>Scenario: This issue occurred when the voice clients (SIP, H323, and SCCP) that were created as servers were getting deleted twice at every client timeout. This issue was observed on controllers running ArubaOS 6.2.1.1.</p>

WebUI

Table 83: *WebUI Fixed Issues*

Bug ID	Description
77933 85051 85740	<p>Symptom: The firewall rule count was not displayed correctly in the Configuration > Security > User Roles > Edit Role <role_name> page of the WebUI. Modifications to the parsing and calculation logic fixed this issue and now the WebUI displays the accurate firewall rule count.</p> <p>Scenario: The incorrect rule count was triggered by an issue in the parsing logic and calculation. This issue was observed in M3 controllers in a master-local topology running ArubaOS 6.1.3.5 and 6.2.1.1.</p>
84387	<p>Symptom: Clicking on the Locate button in the Security page for Valid Clients displayed the Internal error while executing query error. This issue is resolved by generating the correct locate query for the filter related to the client.</p> <p>Scenario: This issue was not limited to a specific controller model or release version.</p>
83744 85222 85646	<p>Symptom: Changes to the account start and end date fields did not take effect when adding a new guest user.</p> <p>Scenario: When the administrator changed the account start and end date fields under Guest User page of the controller's WebUI, the changes did not take effect. This issue was not limited to a specific controller model and was observed in ArubaOS 6.2.1.2 and later versions.</p>
85229	<p>Symptom: The Security Summary page in the WebUI timed out as the event table in the WMS database became very large. This issue is resolved by enabling periodic clean-up of the WMS event table entries.</p> <p>Scenario: This issue was observed when too many APs were terminating on a controller. This issue was not limited to any specific controller model.</p>
85784 76383	<p>Symptom: The Dashboard > Security page of the WebUI was not loaded in Microsoft IE 8 (Internet Explorer) or lower versions and displayed a JavaScript error. This issue is fixed in ArubaOS 6.2.1.3 for all the browsers.</p> <p>Scenario: This issue was triggered by JSON (JavaScript Object Notation) parser in IE. This issue was observed in ArubaOS 6.2.1.2 and not specific to any controller or release version.</p>

Resolved Issues in ArubaOS 6.2.1.2

The following issues were resolved in ArubaOS 6.2.1.2:

802.1X Authentication

Table 84: *802.1X Authentication Fixed Issues*

Bug ID	Description
83375	<p>Symptom: Client failed to connect to Lightweight Extensible Authentication Protocol (LEAP) SSID when operation mode was set to Dynamic-WEP and Use Session Key was enabled on the client. The issue occurred when some of the clients failed to negotiate a separate session key. Enhancements in the security protocols fixed this issue in ArubaOS 6.2.1.2.</p> <p>Scenario: This issue was observed in controllers running ArubaOS 6.2.1.0 and was not specific to any controller model.</p>

AP-Platform

Table 85: AP-Platform Fixed Issues

Bug ID	Description
71978 75776	Symptom: An AP model AP-68 unexpectedly rebooted due to a memory corruption. Memory improvements fixed this issue in ArubaOS 6.2.1.2. Scenario: This issue was observed in an AP-68 running ArubaOS 6.2.0.0.

AP-Wireless

Table 86: AP-Wireless Fixed Issues

Bug ID	Description
82493	Symptom: An AP crashed when a virtual AP configuration changed any downlink traffic from an AP to its associated the clients. Checks are added to the code to prevent and resolve this issue. Scenario: This issue is not specific to any AP model, and was identified in ArubaOS 6.1.3.7.

Base OS Security

Table 87: Base OS Fixed Issues

Bug ID	Description
55419 65936 79704	Symptom: An internal ArubaOS process (Certmgr) became busy when the OCSP server is unreachable. The issue is fixed by changes to the OCSP code base. Scenario: Users were unable to authenticate because this process was busy queuing the OCSP requests (clients using 802.1X, IKE, and management authentication can be affected). This issue was observed in ArubaOS 6.2.x.
68581	Symptom: When a mobile client roamed from a home agent (HA) controller to a foreign agent (FA) controller, issuing the CLI command show user-table from the FA controller incorrectly showed the client in an authenticated/derived role, whereas the output of the show datapath user command correctly showed the client in its dynamic role. The output of the show user-table command now shows correct information. Scenario: This issue was triggered when a mobile client roamed to a foreign agent controller running ArubaOS 6.2.x, and is not limited to any specific controller model.
83620 84429	Symptom: Clients using Temporal Key Integrity Protocol (TKIP) or Counter Cipher Mode with Block Chaining Message Authentication Code Protocol (CCMP) suddenly stopped receiving traffic. This issue is resolved by improvements to the process by which ArubaOS manages counters when new keys are installed. Scenario: This issue was observed on 7200 Series controllers running ArubaOS 6.2.1.1.
81426	Symptom: A memory leak was observed in wired clients with RADIUS accounting enabled. This issue is resolved by freeing the memory allocated for RADIUS context when a user was deleted. Scenario: This issue was observed when wired clients were connected to the APs with RADIUS accounting enabled on AAA profile. This issue was not specific to any controller model.
84077	Symptom: A controller unexpectedly rebooted. The log files for the event listed the reason for the reboot as Crypto Post Failure . This issue is resolved by enabling logs for the error message without automatically reloading the controller. Scenario: This issue is not specific to any controller model.

Command Line Interface

Table 88: *Command Line Interface Fixed Issues*

Bug ID	Description
62292	<p>Symptom: The controller stopped responding and rebooted due to an internal process failure. Changes to the way the command show hostname handles filters fixes the issue.</p> <p>Scenario: When users executed the command show hostname include <filter>, an internal process failed, causing the controller to crash. The issue was not specific to a controller model or a software version.</p>

Control Plane Security (CPsec)

Table 89: *Control Plane Security Fixed Issues*

Bug ID	Description
66413 67875 68010	<p>Symptom: Occasionally, the control plane security (CPsec) whitelist database entries did not synchronize between the master and local controller. ArubaOS 6.2.1.2 transmits smaller sized CPsec records resolving the issue.</p> <p>Scenario: This issue was observed when the CPsec whitelist database size was large. A lossy network between the master and local controller caused some whitelist synchronization fragments to be lost. This issue was not limited to a specific controller model or release version.</p>

Controller-Datapath

Table 90: *Controller-Datapath Fixed Issues*

Bug ID	Description
80625	<p>Symptom: A controller unexpectedly rebooted. Log files for the event listed the reason for the reboot as a Datapath timeout due to change in the tunnel MTU while processing a frame. This issue is resolved by ensuring that the same tunnel MTU is used for processing a given frame.</p> <p>Scenario: This issue was observed when tunnels were used on controllers running ArubaOS 6.1.3.x or later.</p>
83216	<p>Symptom: A controller generated proxy ARP responses out of the same trusted port from where it the controller learned the MAC address. Disabling the option bcmc-optimization in the VLAN interface resolves the issue.</p> <p>Scenario: The issue occurred when the trusted port was a port channel and the bcmc-optimization option was enabled on the VLAN interface. The issue was not specific to a controller model or a software version.</p>
83409	<p>Symptom: A controller rebooted due to missing heartbeats, and log files for the event listed the reason for the reboot as watchdog timeout. This issue is resolved by improvements to the communication infrastructure.</p> <p>Scenario: This issue was observed when a huge traffic hit the control plane causing loss of acknowledgments in the communication infrastructure. This is not specific to any controller model.</p>

Controller-Platform

Table 91: *Controller-Platform Fixed Issues*

Bug ID	Description
79719 81014 81086 81087 81181 81207 81368 81393 81479 81669 81853 82085 82232 82645 82708 82835	Symptom: A controller crashed and rebooted frequently after upgrading the software from ArubaOS 6.1.3.6 to ArubaOS 6.1.3.7. Improvements to packet processing fix this issue in ArubaOS 6.1.3.7. Scenario: A high amount of control traffic triggered this issue, which is not specific to any controller model.
80326 80780 81399 81462 82385 82775	Symptom: A controller failed to respond and rebooted without saving crash log tar files after upgrading to ArubaOS 6.1.3.7. The log files for the event listed the reason for the reboot as Control Processor Kernel Panic . This issue is resolved by improvements to the way internal datapath information is sent to the control plane security process in the event of a datapath module failure. Scenario: This issue was first observed in ArubaOS 6.1.3.7.

Controller-Software

Table 92: *Controller-Software Fixed Issues*

Bug ID	Description
84622	Symptom: Bridge Protocol Data Units (BPDUs) in tagged VLANs were not flooded by the controller when spanning tree is disabled on the controller. Improvements to how process packets with a BPDU MAC address are handled resolves this issue. Scenario: This issue occurred when spanning tree was disabled on the controller and spanning tree was enabled on the uplink switch on the tagged vlan.

Enhanced Voice-Data Optimized

Table 93: *Enhanced Voice-Data Optimized (EVDO) Fixed Issues*

Bug ID	Description
78034	Symptom: A client connected to a 3G uplink port was unable to connect to the Internet when the option firewall session-tunnel-fib was enabled. The issue is fixed by changing a flag set in the route cache entry and adding the static ARP entry. Scenario: When an uplink port on the controller was connected via 3G link, a NAT client was not able to connect to the Internet. The issue was not specific to a controller model or a software version.

IPv6

Table 94: IPv6 Fixed Issues

Bug ID	Description
76426 78962	<p>Symptom: An increase in CPU utilization by the user authentication process was observed on the controller. Creating a rule in the validuser Access Control List (ACL) to deny packets from the host source IPv6 address fe80::/128 fixed this issue in ArubaOS 6.2.1.2.</p> <p>Scenario: This issue was triggered when an HTC One X smartphone running Android version 4.1.1 generated a link-local IPv6 address fe80::/128, resulting in an increased CPU utilization on the controller. This issue was not limited to any specific version of ArubaOS.</p>
79452 77012	<p>Symptom: IPv6 traffic from L3 mobility clients sent from a foreign agent (FA) to a home agent (HA) was double encrypted and sent through an IPsec tunnel instead of a Generic Routing Encapsulation (GRE) tunnel without encryption. ArubaOS 6.2.1.2 updates the packets with tunnel flag so that data traffic doesn't get double encryption in an IPsec tunnel.</p> <p>Scenario: This issue was triggered by an internal flag that determines whether the packets parsed into the GRE tunnel should be encrypted. This issue was observed in all controller platforms running ArubaOS 6.2.x.</p>

Mobility

Table 95: Mobility Fixed Issues

Bug ID	Description
82673	<p>Symptom: DHCP packets from the clients at foreign agent were getting redirected through IPIP tunnel due to wrong order of the ACL. This caused a delay in allocating a valid IP address to the clients. This issue is resolved by correcting the order of the ACL.</p> <p>Scenario: This issue was observed when L3 mobility was enabled on controllers running ArubaOS 6.1.x.</p>

RADIUS

Table 96: RADIUS Fixed Issues

Bug ID	Description
76484	<p>Symptom: RADIUS authentication failed in networks that had different Maximum Transmission Values (MTUs).</p> <p>Scenario: The RADIUS authentication failed when the MTU value in the network between the controller and RADIUS server was different. This issue was observed in controllers running ArubaOS 6.2.1.2 or earlier and was not specific to any controller model.</p>

SNMP

Table 97: SNMP Fixed Issues

Bug ID	Description
77225 82330 82560 88618	<p>Symptom: A 3000 Series controller running ArubaOS 6.2.1.0 was unable to use an SNMP MIB walk to determine values in the table wlsxSysXMemoryTable. Improvements to how file descriptors are managed resolve this issue.</p> <p>Scenario: This issue was triggered by an SNMP MIB walk on a 3000 Series controller.</p>

Voice SIP

Table 98: *Voice SIP Fixed Issues*

Bug ID	Description
81487 83707 83757 84631	Symptom: Voice clients registered as SIP clients were overridden with the application-level gateway (ALG) value as Vocera or New Office Environment (NOE). This issue is resolved by improvements that prevent subsequent updates to the initially configured ALG value. Scenario: This issue was observed in 7200 Series controllers running ArubaOS 6.1.3.3 or later.

WebUI

Table 99: *WebUI Fixed Issues*

Bug ID	Description
76451	Symptom: When guest users were imported using a .CSV file in the Configuration > Security > Authentication > Internal DB > Guest User page of the WebUI, the sponsor's email address was not imported. Scenario: The issue was observed in controllers running ArubaOS 6.1.3.4 and 6.2.x.
80269	Symptom: The Gigabit Ethernet interface 10 option was missing in the VRRP tracking Interface dropdown under Advanced Services > Redundancy > Add virtual Router > Tracking Interface table of the WebUI. ArubaOS 6.2.1.2 now includes the Gigabit Ethernet interface 10 option in the VRRP tracking Interface. Scenario: This issue was observed in M3 controller modules running ArubaOS 6.1.3.1.
82959	Symptom: User was not able to navigate to the fields properly using the tab key in the Configuration > Security > Authentication > Internal DB > Guest User page of the WebUI and use the options: create New, import, delete, print, and cancel . Adding code to the guest provisioning page to create an appropriate tab index for new, import, and edit windows fixed this issue in ArubaOS 6.2.1.2. Scenario: This issue was observed in ArubaOS 6.2.x and is not specific to any controller model.

Resolved Issues in ArubaOS 6.2.1.1

The following issues were resolved in ArubaOS 6.2.1.1:

802.1X Authentication

Table 100: 802.1X Authentication Fixed Issues

Bug ID	Description
77154	<p>Symptom: If the Use Server provided Reauthentication Interval setting was enabled in an AP's 802.11X authentication profile, clients associated with that AP did not reauthenticate when the client roamed to a different AP. This issue is resolved by a change that allows the controller to store the session timeout reauthentication interval returned from the RADIUS server.</p> <p>Scenario: This issue occurred in ArubaOS 6.1.2.4, when clients authenticating with a RADIUS server roamed between APs.</p>
80841	<p>Symptom: A controller configured to use both 802.1X and MAC authentication ignored the eapol-start request sent by client before the completion of the MAC authentication process, Improvements to how the key cache is managed during the MAC authentication process fix this issue in ArubaOS 6.2.1.1.</p> <p>Scenario: When MAC authentication and 802.1X is configured and an eapol-start request from the client came between MAC authentication and 802.1X authentication, the 4-way key exchange was started instead of full 802.1X authentication. This issue was observed in controllers running ArubaOS 6.1.3.5.</p>
83375	<p>Symptom: Client failed to connect to Lightweight Extensible Authentication Protocol (LEAP) SSID when operation mode was set to Dynamic-WEP and Use Session Key was enabled on the client. The issue occurred when some of the clients failed to negotiate a separate session key. Enhancements in the security protocols fixed this issue in ArubaOS 6.2.1.1.</p> <p>Scenario: This issue was observed in controllers running ArubaOS 6.2.1.0 and was not specific to any controller model.</p>

Air Management - IDS

Table 101: Air Management - IDS Fixed Issues

Bug ID	Description
81073	<p>Symptom: An Air Monitor (AM) stopped scanning when it had been up for more than 50 days. This uptime threshold was reached when the AM's milli-tick counter, which counts the uptime in milliseconds, rolled over and the counter returned to zero.</p> <p>Scenario: This issue was identified on ArubaOS 6.1.3.2 and was not limited to a specific controller or AP model. This rollover is expected behavior and a side effect of the roll over caused the issue. A fix has been made to check for and correctly handle the rollover to avoid this issue.</p>

AMON

Table 102: AMON Fixed Issues

Bug ID	Description
81759	<p>Symptom: Upon upgrade to ArubaOS 6.2.0.2, a controller rebooted unexpectedly due to an internal process (fw_visibility) crash. This issue is resolved in ArubaOS 6.2.1.1.</p> <p>Scenario: This issue was identified on ArubaOS 6.2.0.2 and not limited to any specific controller model.</p>

Resolved Issues in ArubaOS 6.2.1.0

The following issues were resolved in ArubaOS 6.2.1.0:

3G/4G

Table 103: 3G/4G Fixed Issue

Bug ID	Description
77928	<p>Symptom: An AP failed to complete a DNS query when it was configured to use a UML290 USB modem uplink. Improvements to multicast IP address checks resolves this issue in ArubaOS 6.2.1.0</p> <p>Scenario: This issue occurred when a UML290 uplink was configured on an Instant AP that was provisioned to use a wired interface and a DNS host name for a VPN. Due to this issue, DNS host names could not be resolved on the IAP or its clients. This issue was identified on RAP-3WN, RAP-108 and RAP-109 access points running ArubaOS 6.2.0.0.</p>

802.1X Authentication

Table 104: 802.1X Authentication Fixed Issues

Bug ID	Description
77705 78658 78559	<p>Symptom: Clients using WPA-TKIP encryption were unable to complete 802.1x authentication. Changes in how TX sequence numbers are reset resolves this issue in ArubaOS 6.2.1.0.</p> <p>Scenario: This issue occurred on 7200 Series controllers running ArubaOS 6.2.0.2.</p>
79546	<p>Symptom: An internal controller module stopped responding, causing the controller to unexpectedly reboot. The log file for the event listed the reason for the reboot as “datapath exception. Memory buffer improvements resolve this issue in ArubaOS 6.2.1.0.</p> <p>Scenario: This issue occurred on M3 controllers running ArubaOS 6.1.3.7.</p>

Air Management-IDS

Table 105: Air Management-IDS Fixed Issues

Bug ID	Description
76936	<p>Symptom: Rogue APs operating in Greenfield mode were not contained by Air Monitors (AMs). Improvements to AP containment processes resolve this issue in ArubaOS 6.2.1.0.</p> <p>Scenario: This issue was first identified in ArubaOS 6.1.3.5, and was not limited to any specific controller or AP model.</p>
76808	<p>Symptom: Some internal processes on the controller were unusually busy, while overall CPU utilization remained within expected levels. ArubaOS 6.2.1.0 introduces changes that prevent APs from sending excessive containment event messages to the controller, so these internal processes do not become overloaded.</p> <p>Scenario: This issue was triggered when the wireless containment parameter in the IDS General profile was set to tarpit all-sta or tarpit-non-valid-sta, and one or more IDS Protection features are enabled such that active containment occurred.</p>

AP-Platform

Table 106: *AP-Platform Fixed Issues*

Bug ID	Description
76021	<p>Symptom: A core file from an AP with a special character in the AP name included the special character in the core file name, causing TFTP dump servers to reject that file. ArubaOS 6.2.1.0 resolves this issue by removing special characters from the core file name before it sends the file to the dump server.</p> <p>Scenario: This issue occurred when an internal process crashed on an AP, and a core file of troubleshooting data was sent to the dump server defined in the AP's system profile. This issue was seen on APs with one or more special characters in the AP name, and was not limited to a specific AP model.</p>
77183	<p>Symptom:An AP-61 associated with a 7200 Series controller running ArubaOS 6.2.0.1 unexpectedly rebooted. The log files on the controller listed the reason for the AP reboot as "watchdog timeout." Changes to channel reuse processing resolves this issue in ArubaOS 6.2.1.0.</p> <p>Scenario: This issue occurred when the RX Sensitivity Tuning Based Channel Reuse setting in the dot11x radio profile was set to dynamic.</p>
77645	<p>Symptom: APs associated to a 7200 Series controller rebooted, forcing clients to reassociate. Changes in how the controller manages duplicate MAC addresses resolves this issue in ArubaOS 6.2.1.0.</p> <p>Scenario: This issue occurred on a 7200 Series controller in a master-local topology where the APs failed over between two controllers.</p>

AP-Wireless

Table 107: *AP-Wireless Fixed Issue*

Bug ID	Description
77946	<p>Symptom: ArubaOS did not support mixed encryption modes for static-WEP and WPA-PSK-TKIP, or for dynamic-WEP and WPA-TKIP. This issue is fixed in ArubaOS 6.2.1.0 and these combinations are now in the list of allowed modes.</p> <p>Scenario: When editing the SSID profile in the WebUI, the system displayed the error message "invalid opmode combination", even though dynamic-WEP WPA-TKIP was available for selection in the WebUI. This issue was observed in ArubaOS 6.1 and later versions, and was not limited to any specific controller model.</p>

Controller-Datapath

Table 108: *Controller-Datapath Fixed Issues*

Bug ID	Description
75843 72359 73246 73256 74575 75700 75753	<p>Symptom: Errors in the internal datapath module on a controller caused it to stop responding. The crash logs for this error listed the reason for the crash as Datapath Timeout. This issue is resolved in ArubaOS 6.1.3.7 and ArubaOS 6.2.1.0.</p> <p>Scenario: This issue occurred when an M3 controller experienced heavy traffic between the control plane module and the network.</p>
77535 77537 77024	<p>Symptom: Android, iOS, and Mac OS devices were incorrectly blacklisted, and the log files for the event listed the reason as IP spoofing. Improvements to the ARP-spoofing feature resolved this issue in ArubaOS 6.1.3.6.</p> <p>Scenario: The iOS, Mac OS, and Android devices sent ARP packets to receive the MAC address of the gateway to all the networks. When the previously connected networks assigned these devices a leased out IP address, these clients were blacklisted.</p>
76307	<p>Symptom: A local controller crashed after a user added a VLAN ID in the master controller. Changes to how the controller decodes encrypted packets has resolved this issue in 6.2.1.0.</p> <p>Scenario: When a user added a VLAN ID to the master controller and executed the command <code>write-mem</code>, the local controller crashed due to an internal process failure. This issue was not specific to any controller or software version.</p>
77484 78181 78667 78873 79682	<p>Symptom: Under very high load conditions, the controller datapath module can prevent users from associating or prevent associated users from passing traffic. In most cases, the controller will automatically reboot to recover from this scenario. Improvements to this internal controller module resolves this issue in ArubaOS 6.2.1.0.</p> <p>Scenario: This occurred on 7200 Series controllers running ArubaOS 6.2.0.x.</p>
77814	<p>Symptom: Errors in the internal control plane module caused a 3000 Series or M3 controller to unexpectedly reboot. The controller log files listed the reason for the reboot as watchdog timeout. Changes to CPU register access has resolved this issue in ArubaOS 6.2.1.0</p> <p>Scenario: This issue occurred on M3 or 3000 Series controllers in a master-local topology running ArubaOS 6.1.x.</p>
78326	<p>Symptom: A local M3 controller unexpectedly rebooted. The log files on the controller listed the reason for the reboot as Datapath timeout. Changes to unicast forwarding checks prevent this issue from occurring in ArubaOS 6.2.1.0.</p> <p>Scenario: This issue was triggered when a controller that receives GRE-type PPP packets has a user role that enables source NAT.</p>
78593 79897	<p>Symptom: A controller running ArubaOS 6.2.0.1 stopped responding and reset. The controller crash logs lists reason for the reboot as User Reboot. Improvements to how in ArubaOS 6.2.1.0 manages core dumps resolves this issue.</p> <p>Scenario: This issue was observed in a 7200 Series controller in a master-local topology.</p>

Controller-Platform

Table 109: *Controller-Platform Fixed Issues*

Bug ID	Description
62096	<p>Symptom: M3 controllers unexpectedly rebooted, and the log files for the event listed the reason as “User pushed reset”. This issue is resolved in ArubaOS 6.2.1.0.</p> <p>Scenario: This issue was observed on an M3 controller when there was high traffic between the control plane and the datapath.</p>
75232	<p>Symptom: An internal system error occurred in the M3 controller and APs failed to connect to the controller.</p> <p>Scenario: The issue was seen in large deployments, where the size of the config file was more than 360 KB and there were large number of references to one profile instance. Due to this there was an internal system error and the APs were unable to connect to the controller. This issue occurred in ArubaOS 5.0.4.6 and is not specific to any controller model.</p>
75411	<p>Symptom: 10GE ports on 7200 Series controllers report sporadic packets being dropped with CRC errors. This issue is resolved in ArubaOS 6.2.1.0.</p> <p>Scenario: This is an infrequent occurrence on these controllers.</p>
76852	<p>Symptom: The phonehome process sent incorrect user credentials to the corporate office. The issue is resolved by removing extra spaces from the user credentials sent via the command-line interface.</p> <p>Scenario: When the phonehome process was configured with SMTP credentials, it did not send the user credentials successfully to the corporate office. The issue occurred on controllers running ArubaOS 6.2.0.0 or later, and was not limited to any specific controller model.</p>
79385	<p>Symptom: A RAP-5WN associated to a 3200XM controller failed to come up. The controller log files listed the reason as “AP-Group is not present in the RADIUS server.” Improvements to how remote AP route-cache entries are created resolves this issue in ArubaOS 6.2.1.0.</p> <p>Scenario: The issue by a gateway failover, and was seen on a RAP-5WN associated to a controller running ArubaOS 6.2.0.2 in a redundant (active/standby) gateway topology.</p>

Base OS Security

Table 110: *Base OS Fixed Issue*

Bug ID	Description
75754	<p>Symptom: The user table showed that some 802.1X authenticated clients managed by an external XML-API server were using Web authentication, even though there was no captive portal authentication configured for those clients. This display issue is resolved in ArubaOS 6.2.1.0.</p> <p>Scenario: This issue occurred on a controller configured with a 802.1X default role with an ACL that sent traffic through the GRE tunnel to a SafeConnect appliance. In this scenario, L3 authentication was managed by the SafeConnect XML API, which updated the user role to an L3-authenticated role.</p>
76401 76403 82540 82060	<p>Symptom: The internal controller module that manages handles user authentication stopped responding, preventing users from authenticating until the process automatically restarted.</p> <p>Scenario: This issue occurred on a M3 controller module running ArubaOS 6.2.0.2 in a master-local topology.</p>

IPSec

Table 111: *IPsec Fixed Issues*

Bug ID	Description
68035	<p>Symptom: When site-to-site VPN was enabled between two controllers, static routes were not removed from the routing table when site-to-site VPN went down. Improvements to the way controllers add and delete static routes resolves this issue in ArubaOS 6.2.1.0.</p> <p>Scenario: This occurred when site-to-site VPN was enabled and a static route was added to a remote subnet with an IPsec map.</p>
76301	<p>Symptom: An AP continually rebooted. The log files for the event listed the reason for the reboot as Send failed in function sapd_keepalive_cb. This issue is resolved in ArubaOS 6.2.1.0</p> <p>Scenario: This issue occurred on both campus APs (CAPs) and remote APs (RAPs) with IPsec tunnel to the controller.</p>

Management Authentication

Table 112: *Management Authentication Fixed Issues*

Bug ID	Description
75665 75860	<p>Symptom: A 3rd generation iPad running iOS 6.0.1 was incorrectly assigned to the default VLAN. Changes to how the controller manages PMKID data resolves this issue in ArubaOS 6.2.1.0.</p> <p>Scenario: This issue occurred in ArubaOS 6.1.3.5, when a Virtual AP was configured with both MAC authentication and 802.1x authentication, a VLAN derivation rule was configured on the MAC authentication server, and the derived VLAN was different from the default VLAN of the virtual AP.</p>

Mesh

Table 113: *Mesh Fixed Issue*

Bug ID	Description
71371	<p>Symptom: AnAP-85 configured as a mesh portal unexpectedly rebooted. The log files for the event listed the reason for the reboot as "kernel page fault." This issue was caused by memory corruption, and is resolved in ArubaOS 6.2.1.0 by changes to how internal controller modules restart.</p> <p>Scenario: This issue occurred in anAP-85 mesh portal associated to an M3controller in a master-local topology.</p>

RADIUS

Table 114: *RADIUS Fixed Issue*

Bug ID	Description
71836	<p>Symptom: A controller sent incorrect class attributes to a RADIUS server, causing that server to show incorrect user statistics. Changes in how the controller sends class attributes in accounting requests has resolved this issue.</p> <p>Scenario: This issue occurred when multiple users with the same MAC address tried to connect to the controller using a wired connection.</p>

Remote AP

Table 115: *Remote AP Fixed Issue*

Bug ID	Description
72454	<p>Symptom: When a UML290 USB modem was provisioned as a remote AP (RAP) uplink with the cellular_nw_preference parameter set to auto, the RSSI value for the 3G/4G uplink was not fetched dynamically. This issue is resolved by changes in ArubaOS 6.2.1.0 that enable an explicit dynamic RSSI check.</p> <p>Scenario: This issue was identified on RAPs with a UML290 modem uplink running ArubaOS 6.1.3.3.</p>

Spectrum-Infrastructure

Table 116: *Spectrum-Infrastructure Fixed Issue*

Bug ID	Description
79144	<p>Symptom: AP-105, AP-92, and AP-93 access points running ArubaOS 6.2.x and later versions unexpectedly stopped responding and rebooted. This issue is resolved in ArubaOS 6.2.1.0.</p> <p>Scenario: This issue occurred when the spectrum monitoring option was enabled in the AP's 802.11a or 802.11g radio profile, allowing the AP to operate as a hybrid AP that both serves clients and performs spectrum analysis on a single radio channel.</p>

Station Management

Table 117: *Station Management Fixed Issues*

Bug ID	Description
74455	<p>Symptom: Incorrect information was present in the CLI help for the local-probe-req-threshold CLI command, suggesting that the local probe response feature had to be enabled before setting the local probe request threshold. This additional help string is removed in ArubaOS 6.2.1.0, as the local probe response feature is now enabled by default and this help message is no longer required.</p> <p>Scenario: This issue was not limited to any controller model, and appeared in the output of the wlan ssid-profile <profile> local-probe-req-threshold ? command.</p>

WebUI

Table 118: *WebUI Fixed Issues*

Bug ID	Description
74227	<p>Symptom: The Monitoring tab of the WebUI and the output from the show ap active command did not match. The WebUI showed more APs than were actually up and the output of show ap active displayed the correct number. This issue is resolved in ArubaOS 6.2.1.0.</p> <p>Scenario: This occurred on master controllers running ArubaOS 6.1.3.2 or later if the bootstrap threshold in the ap system profile was set to over 40 minutes. In this instance, these APs were powered off when the controller attempted to send a configuration update. The APs failed to receive the update, and the controller marked the APs as down but did not update the AP database as well.</p>
76348	<p>Symptom: When an AP provisioned with a Fully Qualified Domain Name FQLN parameter using the format <i><floor>.<building>.<campus></i> was then reprovisioned, the AP provisioning page in the WebUI displayed the incorrect building value. This issue is resolved in ArubaOS 6.2.1.0.</p> <p>Scenario: This issue occurred on APs provisioned with the FQLN parameter, and was not limited to any specific controller or AP model.</p>
76335	<p>Symptom: In the ArubaOS 6.2.0.x Dashboard tab the WebUI, the y-scale of the Noise Floor graph was inverted compared to previous versions of ArubaOS. This has been changed in ArubaOS 6.2.1.0, so -110 dBm is now shown at the bottom of the y-scale instead of the top.</p> <p>Scenario: This issue occurred on controllers running ArubaOS 6.2.0.x, and was not limited to a specific controller model.</p>

The following issues and limitations are observed in ArubaOS 6.2.1.x releases. Applicable workarounds are included.

Known Issues and Limitations in ArubaOS 6.2.1.8

The following issues and limitations observed in ArubaOS 6.2.1.8. Applicable workarounds are included.

AP-Datapath

Table 119: *AP-Datapath Known Issues*

Bug ID	Description
99655	<p>Symptom: Gratuitous ARP triggers responses which causes station buffer overflow.</p> <p>Scenario: This issue is observed when a Gratuitous ARP is sent from a RAP to update the uplink switch/router MAC table. This causes devices in the same network to send ARP responses which leads to client MAC table overflow. This issue is observed in ArubaOS 6.2.1.5.</p> <p>Workaround: None.</p>

AP-Platform

Table 120: *AP-Platform Known Issues*

Bug ID	Description
98915	<p>Symptom: RAP-2WG fails to boot after upgrading the controller from ArubaOS 6.1.3.4 to 6.2.1.7.</p> <p>Scenario: This issue occurs on a RAP-2WG in a master-local topology and is caused by IPsec setup failure.</p> <p>Workaround: None.</p>

Base OS Security

Table 121: *Base OS Security Known Issues*

Bug ID	Description
97460	<p>Symptom: Station table entries do not age out for split-tunnel mode clients.</p> <p>Scenario: Stale station split-tunnel mode entries exist in the station table even after stations have left. This can be verified by issuing the show station-table command on the controller's CLI. Those stale station entries have a long time (more than several days) on the Age column .</p> <p>Workaround: None.</p>

Captive Portal

Table 122: *Captive Portal Known Issues*

Bug ID	Description
94675	<p>Symptom: Clients attempting to log out of captive portal authentication incorrectly receive the error message, User not logged in.</p> <p>Scenario: This issue occurs in ArubaOS 6.2.1.3, when a client that has completed captive portal authentication tries to log out of the captive portal. The controller user table shows the client is still authenticated and able to pass traffic.</p> <p>Workaround: None.</p>

Configuration

Table 123: *Configuration Known Issues*

Bug ID	Description
94286	<p>Symptom: When the user tries to upgrade to ArubaOS 6.3.1.1 it fails with the following error Not enough flash/memory available (60 MB needed).</p> <p>Scenario: This issue occurs when a user tries to upgrade to ArubaOS 6.3.1.1 and is caused by an invalid temporary file in the flash directory. This issue is observed on 600 Series controllers.</p> <p>Workaround: This issue is resolved by deleting the invalid temporary file before upgrading to ArubaOS 6.3.1.3.</p>

Controller-Datapath

Table 124: *Controller-Datapath Known Issues*

Bug ID	Description
95706	<p>Symptom: A 7200 Series controller unexpectedly stops passing network traffic.</p> <p>Scenario: This issue is triggered by a hardware error on a 7200 Series controller using auto-negotiated Ethernet speeds.</p> <p>Workaround: Manually define ethernet speeds for each port on the 7200 Series controller.</p>
100375	<p>Symptom: The local 7240 controller is unable to pass the packets in the Last in First Out (LIFO) mode and goes offline.</p> <p>Scenario: This issue is observed when the ingress NAE free LIFO buffers are zero and the SOS didn't lease the buffers at the same time. This causes the ingress NAE stall. This issue is observed in 7240 controllers running ArubaOS 6.2.1.4.</p> <p>Workaround: Upgrade to ArubaOS 6.2.1.6 to detect the reload issue on the controller.</p>

Controller-Platform

Table 125: *Controller-Platform Known Issues*

Bug ID	Description
76059 85289 92255 93467 93827 95431 96293 96791 96827 98196 99287 99360 99362 99472 99568	Symptom: A controller reboots unexpectedly. The log files for the event listed the reason as Reboot Cause: kernel panic . Scenario: This issue is seen in 7200 Series controller having a high density of IPv4 captive-portal users configured. This results in a high number of httpd processes running on the controller. This issue observed in ArubaOS 6.2.0.0 or later versions. Workaround: None.
96115	Symptom: A local controller crashes unexpectedly and the log files for the event lists the reason for the reboot as Kernel panic. Scenario: This issue is observed in 7220 controllers running ArubaOS 6.2.1.4. Workaround: None.

LLDP

Table 126: *LLDP Known Issues*

Bug ID	Description
100439	Symptom: Clients are unable to disable the 802.3 TLV power in the AP LLDP configuration. This results in PoE allocation issue on the switches. Scenario: This issue is observed in 7210 controllers running ArubaOS 6.2.1.7. Workaround: None.

Remote AP

Table 127: *Remote AP Known Issues*

Bug ID	Description
99343	Symptom: RAP randomly reestablishes a GRE tunnel. Scenario: This issue is observed on a device connected to an untrusted RAP wired port that has the same IP address as another RAP's default gateway. Workaround: Include the RAP default gateway IP in validuser ACL. Enable enforce-dhcp.

WebUI

Table 128: *WebUI Known Issues*

Bug ID	Description
76432	Symptom: In the Client detail page, the trend is not displayed for Frame Rates To Client or Frame Rates From Client. Scenario: This issue is not limited to a specific controller model or release version. Workaround: None.
89070	Symptom: The controller WebUI fails to respond when you navigate to the Monitoring > Clients window, and attempt to view the status of a windows client that has been misclassified as an iPhone client. Scenario: This issue is observed in controllers running ArubaOS 6.2.1.3. It occurs only when viewing the status for misclassified clients. This issue does not occur when viewing status information for Windows clients that are correctly classified. Workaround: None

Known Issues and Limitations in ArubaOS 6.2.1.7

The following issues have been reported in ArubaOS 6.2.1.7 and are being investigated.

Controller-Platform

Table 129: *Controller-Platform Known Issues*

Bug ID	Description
94304	Symptom: A controller running ArubaOS 6.2.1.2 unexpectedly rebooted. Log files for the event listed the reason for the reboot as Control Processor Kernel Panic . Scenario: This issues occurs on controllers running ArubaOS 6.2.1.2 or later. Workaround: None

Known Issues and Limitations Prior to ArubaOS 6.2.1.7

The following issues and limitations were observed in releases prior to ArubaOS 6.2.1.7. Applicable workarounds are included.

802.1X Authentication

Table 130: *802.1X Authentication Known Issues*

Bug ID	Description
74663	Symptom: Clients are not able to reauthenticate after rebooting or logging off the network. Scenario: This issue is observed on a client running Windows 7 with machine authentication, and connected to a Cisco phone. This issue only occurs when the eapol-logoff feature that handles EAPOL-LOGOFF messages is enabled in the controller's 802.11X authentication profile. Workaround: Disable the Handle EAPOL-Logoff setting in the 802.11X authentication profile (This setting is disabled by default).

AMON

Table 131: *AMON Known Issues*

Bug ID	Description
94570	<p>Symptom: The Dashboard tab of the controller WebUI can display the incorrect user role for clients.</p> <p>Scenario: This issue occurred in ArubaOS 6.2.1.4, when clients connected to a remote AP configured to use split-tunnel forwarding mode.</p> <p>Workaround: View client role information on the Monitoring tab of the controller WebUI, or issue the command show user-table in the command-line interface.</p>

AP-Wireless

Table 132: *AP-Wireless Known Issues*

Bug ID	Description
75564	<p>Symptom: An internal process in an AP-135 running ArubaOS 6.1.3.3 restarts, causing that AP to unexpectedly reboot.</p> <p>Scenario: This issue can occur if the Collect Stats parameter is enabled in the WMS General profile, and the Monitored Device Stats Update Interval parameter in the IDS General profile is set to a non-zero value.</p> <p>Workaround: Set the Monitored Device Stats Update Interval in the IDS General profile to 0, its default value.</p>
69424 75874 78978 78981 79891 80054 87250 88619 88620 88989 89537 91689 93455 93811 94396	<p>Symptom: When upgraded to ArubaOS 6.2, an AP-125 crashed and rebooted.</p> <p>Scenario: This issue was observed when upgrading to ArubaOS 6.2 from ArubaOS 6.1.3.2 and later in any deployment with an AP-125.</p> <p>Workaround: None.</p>

AP-Platform

Table 133: AP-Platform Known Issues

Bug ID	Description
58011 60846 60850 61100 61196 61537 61539 61540 63004 64156 64517 64524 64526 66118 66128 66133 66135 66185 66596 66659 67435 67670 67671 67673 67871 67872 67977 67978 67980 68875 68889 68934 68937 72069 74142 75366 75368 75369 75370 75539 75703 79854	<p>Symptom: A 650 controller reboots unexpectedly after enabling the internal AP.</p> <p>Scenario: This issue is observed in 650 controllers running ArubaOS 5.0 or later. The internal AP is disabled when a 650 controller upgrades to ArubaOS 6.2.1.x.</p> <p>Workaround: None.</p>
89741 88763 89538 92872 92876 95060	<p>Symptom: AP-125 access points unexpectedly rebooted.</p> <p>Scenario: This issue was observed in AP-125 access points associated to a 7200 Series, 6000, or 3400 controller running ArubaOS 6.2.1.3.</p> <p>Workaround: None.</p>
89916	<p>Symptom: AP-125 access points unexpectedly rebooted, and log files for the event indicate that the APs reboot because they are out of memory.</p> <p>Scenario: This issue is observed AP-125 access points associated to a local controller running ArubaOS 6.2.1.x.</p> <p>Workaround: None.</p>
93955	<p>Symptom: Windows Surface Pro does not allow traffic with MPDU aggregation disabled.</p> <p>Scenario: This issue occurs on AP-105 running ArubaOS 6.2.1.2.</p> <p>Workaround: Enable MPDU aggregation.</p>

Air Management -IDS

Table 134: Air Management - IDS Known Issues

Bug ID	Description
93516	<p>Symptom: An AP incorrectly reported a Overflow IE detection warning.</p> <p>Scenario: This issue occurred when an AP associated to a controller running ArubaOS 6.2.1.2 in a master-local topology incorrectly detected its own MAC address as a device sending malformed IE.</p> <p>Workaround: None.</p>

Authentication

Table 135: *Authentication Known Issues*

Bug ID	Description
55867	<p>Symptom: The client is placed in the VLAN provided by 802.1X default role, instead of the VLAN defined by the Vendor Specific Attributes (VSA).</p> <p>Scenario: This issue is found in controllers where the role-based VLAN derivation is configured for a machine role and 802.1X default role, with a RADIUS server sending the VLAN through the VSA. The client is placed in the VLAN provided by the 802.1X default role, because the VLAN provided by the 802.1x default role overrides the VLAN sent through the VSA. This issue is found in controllers running ArubaOS 6.0.0.0 and later with 802.1X configured and machine authentication enabled.</p> <p>Workaround: Remove the VLAN from the 802.1X authenticated role and machine authentication.</p>

Base OS Security

Table 136: *Base OS Security Known Issues*

Bug ID	Description
85453	<p>Symptom: An internal controller process (resolvwrap) stops responding at random intervals when a RADIUS authentication server is configured with a host name.</p> <p>Scenario: This crash does not have any impact on the ArubaOS operation as the resolvwrap process is used only for resolving the host name configured for authentication server periodically. If host-name resolution fails due to a crash then subsequent attempts to resolve the host name are successful.</p> <p>Workaround: If this crash is observed continually, use an IP address is used instead of a host name in the server authentication profile.</p>
76424	<p>Symptom: Issuing the CLI command aaa user delete all on a 7200 Series controller managing over 14,000 users causes internal controller process modules that manage AP management, user association and user authentication to become busy and cause the controller to become unresponsive.</p> <p>Scenario: This issue occurred on a 7200 Series controller running ArubaOS 6.2.x.x.</p> <p>Workaround: Delete fewer users at a time.</p>
79467	<p>Symptom: User table entries for users that disconnect from the network are not correctly aging out and getting removed from the controller user table.</p> <p>Scenario: This issue was observed on a 7240 local controller running ArubaOS 6.2.0.2 in a master/local topology.</p> <p>Workaround: None.</p>
81243	<p>Symptom: When an AP boots up, the controller log files display the message <i>AP-Group is not present in the RADIUS server for username=<mac address>; AP will take the ap-group as provisioned in the AP.</i></p> <p>Scenario: This message appears when an AP boots, and although it does not indicate a problem with the boot process, the current wording of the message can be confusing. The error message is not limited to any specific AP model or software version.</p> <p>Workaround: No workaround is needed since this error message does not indicate a functionality issue.</p>
86867	<p>Symptom: When a user role and an ACL configured as the ip access-group on an AP or remote AP (RAP) interface have the same name, the AP/RAP traffic is assigned the user role ACL instead of the ip access-group ACL.</p> <p>Scenario: This issue was observed on a controller running ArubaOS 6.2.1.2.</p> <p>Workaround: Do not create an ACL for the IP access-group that has a name matching that of any user-role in the configuration.</p>
95546	<p>Symptom: The 7210 controller reboots frequently and the log files for the event display the reason for the reboot as Datapath Timeout.</p> <p>Scenario: The trigger of this issue is not known. This issue is observed in 7210 controllers running ArubaOS 6.3.1.2.</p> <p>Workaround: None.</p>

Captive Portal

Table 137: *Captive Portal Known Issues*

Bug ID	Description
94675	<p>Symptom: Clients attempting to log out of captive portal authentication incorrectly receive the error message "User not logged in"</p> <p>Scenario: This issue occurs in ArubaOS 6.2.1.3 when a client that has completed captive portal authentication tries to log out of the captive portal. The controller user table shows the client is still authenticated and able to pass traffic.</p> <p>Workaround: None.</p>

Controller-Datapath

Table 138: *Controller-Datapath Known Issues*

Bug ID	Description
82402 84212 86636 87552 89437 90466 91280 93591 94721 94727 95074 95624 95643 95644	<p>Symptom: A controller unexpectedly rebooted. The controller log files listed the reason for the event as Nanny rebooted machine - httpd_wrap process died.</p> <p>Scenario: This issue occurs on a controllers running ArubaOS 6.2.x.x.</p> <p>Workaround: None.</p>
84585 92227 92228 92883	<p>Symptom: Traffic can fail to pass a network with heavy traffic (such as high levels of packet replication), and AES-CCM or one another encryption/decryption modes is enabled.</p> <p>Scenario: This issue was identified on a 7200 Series controller connected to 2000 APs when Gratuitous ARP messages were replicated and sent to clients.</p> <p>Workaround: None</p>
90923	<p>Symptom: When VLAN 1 on the controller uses source network address translation (NAT) for all traffic routed from VLAN 1, and the controller uses a different uplink VLAN to connect to remote and campus APs, the APs on the controller come up with ID flags, indicating that the APs are inactive and have not downloaded a configuration. The APs are not be operational in this state.</p> <p>Scenario: This issue occurs in ArubaOS 6.2.x.x in deployments using control plane security</p> <p>Workaround: Issue the command interface vlan 1 no ip nat inside to disable NAT for all traffic routed from VLAN 1.</p>

Controller-Platform

Table 139: *Controller-Platform Known Issues*

Bug ID	Description
69277	<p>Symptom: The Point-to-Point Tunneling Protocol (PPTP) VPN connection is lost when a user tries to connect to the PPTP server using a Windows 7 client as the VPN client, then switches to split-tunnel forwarding mode.</p> <p>Scenario: This issue is seen in ArubaOS 6.1.3.2.</p> <p>Workaround: None.</p>
74428 88758	<p>Symptom: On the dual-personality RJ45 ports 0/0/0 and 0/0/1, if the port speed is forced from/to 1 Gbps to/from 10/100 Mbps when traffic is flowing, traffic forwarding on the port can stop in an unintended manner.</p> <p>Scenario: This issue has been observed in 7200 Series controller running ArubaOS 6.2.x.x in configurations or topologies where traffic is flowing. The trigger is unknown.</p> <p>Workaround: Change the speed on the port by shutting the port., changing the speed on the port, then opening the port.</p>
76220	<p>Symptom: A controller crashes due to a virtual AP configuration change.</p> <p>Scenario: In a high traffic deployment, when a virtual AP with active client associations is removed from an AP group, a race condition may trigger a controller crash.</p> <p>Workaround: Before removing a virtual AP profile from an AP group, wait for all active associated clients to disassociate or time out. Use the show ap association command to verify the virtual AP client association status.</p>
84597 83623	<p>Symptom: Campus APs may not come up properly in a topology where a firewall between the AP and controller only allow communications from certain IP address through the firewall. The issue occurs if the AP communicates to the controller using the VRRP address, and this is communication is allowed through the firewall, but the control plane security feature causes the controller to communicate to the AP using its controller IP as its source IP address, which fails to pass the firewall.</p> <p>Scenario: This issue is not limited to any specific controller model or software version, and can occur in networks. Controller are using VRRP redundancy, there is a firewall between the controllers and the campus AP, and the campus AP terminates at the VRRP IP</p> <p>Workaround: In the event that only the VRRP to AP communications are allowed, allowing the controller-ip address through the firewall may resolve this issue.</p>
86903	<p>Symptom: An M3 controller module may not consistently respond to ping messages for the first 1-2 minutes after that module reboots.</p> <p>Scenario: This issue occurs if the management port on an M3 controller module running ArubaOS 6.2.1.2 is connected to a VLAN that sees very low levels of broadcast or multicast traffic (less than 1 packet/second). This issue is not seen with M3 controller modules connected to VLANs with higher levels of traffic.</p> <p>Workaround: None.</p>
93005	<p>Symptom: The controller WebUI and CLI stops responding. The log files list the reason for the event as a crash in the internal process that manages the command-line interface.</p> <p>Scenario: This issue was observed in a 7240 controller running ArubaOS 6.2.1.x in a master-local topology.</p> <p>Workaround: None.</p>
93011	<p>Symptom: Users may be unexpectedly logged out of the controller WebUI.</p> <p>Scenario: This issue was observed in ArubaOS 6.2.1.4, when users accessed the controller using the WebUI.</p> <p>Workaround: Access the controller through the command-line interface..</p>

DHCP

Table 140: *DHCP Known Issues*

Bug ID	Description
91099	<p>Symptom: Clients connected to the wired port on a remote AP occasionally fail to get an IP address. This issue is under investigation, and the root cause is not yet identified.</p> <p>Scenario: This issue occurred in 7200 Series controllers running ArubaOS 6.2.1.1, and was triggered when the controller failed to send DHCP offers to the AP via a GRE tunnel.</p> <p>Workaround: None.</p>

IDS

Table 141: *IDS Known Issues*

Bug ID	Description
90630	<p>Symptom: Log messages incorrectly warn of a blocked ACK DoS attack from a valid client.</p> <p>Scenario: This issue was identified in a 6000 controller running ArubaOS 6.2.0.2 in a master-local topology.</p> <p>Workaround: None.</p>

IPsec

Table 142: *IPsec Known Issues*

Bug ID	Description
75891	<p>Symptom: When an idle user times out, the controller does not send a ping request before aging out the user. The user is aged out immediately. This applies to VPN and VIA-VPN users as well. When the users age out, the VPN tunnel will also go down.</p> <p>Scenario: This occurs on controllers running ArubaOS 6.2.x.x, when there is no data for the user during the ageout time period. For VPN and VIA-VPN users, if the IPsec tunnel does not have any data for the configured user ageout time, the user will age out and the tunnel will be deleted.</p> <p>Workaround: Increase the value of the user ageout time. The default value is five minutes. This issue can also be avoided if you ensure that there is always some data sent from the user.</p>

IPv6

Table 143: *IPv6 Known Issues*

Bug ID	Description
74367	<p>Symptom: Clients using temporary IPv6 addresses are not be able to communicate as traffic is getting dropped.</p> <p>Scenario: A client can support up to four IPv6 addresses. The usage of temporary IPv6 addresses on the clients generates additional IPv6 addresses and sends traffic using all these IPv6 addresses, which exceeds the limitation of four IPv6 entries for the client in the user-table. The issue occurs on the controllers that support IPv6 clients.</p> <p>Workaround: Delete unused IPv6 addresses from the user-table with the command aaa ipv6 user delete <ip address>, increase the time that a client keeps the temporary IPv6 address before changing to a new address, or Avoid the usage of temporary IPv6 addresses.</p>

Management Authentication

Table 144: *Management Authentication Known Issues*

Bug ID	Description
81517	<p>Symptom: The controller log files are being flooded with the error <i>Datapath-UserRem (IPv4/L2) failed: mac=<controller-mac-addr></i>.</p> <p>Scenario: This issue occurred in ArubaOS 6.2.0.0 on an M3 controller and an AP-93 remote AP operating in split-tunnel forwarding mode and configured to support captive portal authentication.</p> <p>Workaround: None</p>

Master-Redundancy

Table 145: *Master-Redundancy Known Issues*

Bug ID	Description
70343	<p>Symptom: Custom captive portal pages are not synced between a master and standby controller when set up to do so.</p> <p>Scenario: For all software versions, when the standby becomes the master, the custom captive portal page will no longer show up during CP authentication. The database synchronize command only copies database files and RF plan floor plan backgrounds.</p> <p>Workaround: None</p>
75367	<p>Symptom: Enabling web-server debug logging using the CLI command logging level debugging system subcat webserver does not take effect until you restart the HTTPD process.</p> <p>Scenario: This happens on all controller models running ArubaOS 3.x, 5.x and 6.x software versions when web-server debug logging mode is enabled.</p> <p>Workaround: Restart the HTTPD process in order to enable debug logging.</p>

Mobility

Table 146: *Mobility Known Issues*

Bug ID	Description
58883 60328	<p>Symptom: In a Layer-3 IP mobility enabled network, when the client moves from a Home Agent network to a Foreign Agent network, the IPv4 address of the client changes. This prevents the client from sending traffic.</p> <p>Scenario: Layer-3 IP mobility does not work when IPv6 packet processing is enabled on the controller. This issue is found in controllers running ArubaOS 6.2.x.x..</p> <p>Workaround: Do not issue the router enable command along with the ipv6 enable command in the controller.</p>
92453	<p>Symptom: Users connecting to an AP or controller with IP mobility enabled are unable pass any traffic</p> <p>Scenario: This issue was first identified in ArubaOS 6.2.1.3, and is not specific to any controller model. This issue is triggered when client roams between an ESSID with IP mobility enabled and an ESSID with IP mobility disabled.</p> <p>Workaround: Clear the IP mobile host entry using by issuing the CLI command clear ip mobile host <client-mac-address>. After clearing the client IP mobile host entry, the client is able to pass traffic.</p>

Remote AP

Table 147: *Remote AP Known Issues*

Bug ID	Description
83002	<p>Symptom: A wireless client connected to a backup virtual AP configured in bridge forwarding mode is unable to get an IP address from an assigned VLAN.</p> <p>Scenario: This issue occurred when the controller upgraded to ArubaOS 6.2.x.x.</p> <p>Workaround: Once the AP connects to the controller, remove the virtual AP profile from the ap-group/ap-name configuration, then return the virtual AP profile to the ap-group/ap-name settings.</p>
84004 85499	<p>Symptom: In some instances calls from IP phones connected to a RAP-3WN AP fail because the AP drops packets.</p> <p>Scenario: This issue occurs on IP phones connected to an AP in tunnel forwarding mode, and was first identified in ArubaOS 6.2.0.2.</p> <p>Workaround: None.</p>

Station Management

Table 148: *Station Management Known Issues*

Bug ID	Description
72194	<p>Symptom: When VLAN pooling is used with the assignment type EVEN, the user VLAN changes when the client roams from AP to AP, but the IP address remains the same until a release/renew is executed on the client device.</p> <p>Scenario: This issue occurs on any controller model with the VLAN mobility and preserve VLAN features enabled. When these features are enabled, the bridge table of the controller keeps user entries for 12 hours. This issue occurs when the STM module (an internal process) of the controller does not find the entry in the bridge lookup result.</p> <p>Workaround: Disable VLAN mobility and the preserve VLAN feature.</p>
86620 88646	<p>Symptom: The output of the following commands incorrectly display entries that should have aged out.</p> <ul style="list-style-type: none">• show ap debug client-table• show ap remote debug association• show ap association• show user <p>Scenario: This issue was observed in networks where controllers are managing a heavy traffic load and many users are roaming between APs.</p> <p>Workaround: This is a display issue only, and does not impact controller or AP functions.</p> <ul style="list-style-type: none">• To remove for stale entries in the client table, reboot the AP.• To remove stale entries in the AP association tables, issue the command process restart stm.• To remove stale entries in the user table, issue the command process restart auth.
90390	<p>Symptom: IP phones connected to the wired port on a remote AP get disconnected.</p> <p>Scenario: This issue was identified in ArubaOS 6.2.1.x, and is triggered when GRE tunnels from the wired port get dropped.</p> <p>Workaround: Reboot the remote AP to restore connectivity to the IP phones.</p>
91224	<p>Symptom: An AP unexpectedly reboots. The controller log files list the reason for the event as Unexpected stm (Station management) runtime error.</p> <p>Scenario: This issue occurred on M3 controller modules running ArubaOS 6.2.1.4 in a master-local topology.</p>
100799	<p>Symptom: Wireless clients fail to associate to an SSID. The controller log files for the event listed the reason as Capability requested by STA unsupported by AP.</p> <p>Scenario: This issue is seen for a Virtual AP profile that does not have a VLAN configured. This issue is observed in controllers running ArubaOS 6.2.1.5.</p> <p>Workaround: Add a VLAN ID to the Virtual AP profile.</p>

Startup Wizard

Table 149: *Startup Wizard Known Issues*

Bug ID	Description
72740	<p>Symptom: The Controller Wizard, Campus AP Wizard, and Remote AP Wizard display a blank page when the LDAP server attributes contain special characters.</p> <p>Scenario: This issue occurs on controllers running ArubaOS 6.2.x.x when the LDAP server attributes contains special characters.</p> <p>Workaround: Ensure that the LDAP server attributes do not have special characters.</p>
77057	<p>Symptom: In the Remote AP Wizard, the Split Tunnel role configuration requires an additional ACL to automatically generate roles.</p> <p>Scenarios: This issue occurs on controllers running ArubaOS 6.2.x.x if the svc-dhcp permit rule is missing in the access list of \$APGROUPNAME_default_role in the Remote AP Wizard. Due to this, the IP addresses cannot be assigned to the clients.</p> <p>Workaround: Add the any any svc-dhcp permit ACL rule under the ACL in position 1.</p>
81063	<p>Symptom: The Authentication port configuration cannot be applied to the LDAP server.</p> <p>Scenario: This issue occurs on controllers running ArubaOS 6.2.x.x when an invalid command is sent to the controller from Campus AP or WLAN Wizards.</p> <p>Workaround: Manually configure the authentication port for the LDAP server under Configuration > Security > Authentication > Servers > LDAP.</p>

WebUI

Table 150: *WebUI Known Issues*

Bug ID	Description
55981	<p>Symptom: When a user views the Spectrum UI with saved preferences from a newer version of ArubaOS, the UI will display charts incorrectly.</p> <p>Scenario: Downgrading from a newer version of ArubaOS, such as from 6.2.x.x to 6.1.x.x with saved Spectrum preferences, will cause the Spectrum UI to display charts incorrectly. This is due to the difference between the Spectrum UI in 6.2.x.x and previous versions.</p> <p>Workaround: Use the command ap spectrum clear-webui-view-settings on the controller to delete the saved preferences.</p>
66521	<p>Symptom: Two Apply buttons are displayed in the WebUI when adding users to the internal database.</p> <p>Scenario: While creating a new user in the WebUI, two Apply buttons appear in the Configuration > Security > Authentication > Internal DB page due to incorrect labeling of the buttons. This issue is not limited to a specific controller model.</p> <p>Workaround: Use the Apply button at the top to add a new user. Use the Apply button at the bottom to apply any user list changes.</p>
75836	<p>Symptom: An incorrect label is displayed on the AP Details page on clicking the AP Name hyperlink on the Client and Performance page of the WebUI Dashboard.</p> <p>Scenario: This issue occurs on controllers running ArubaOS 6.2.x.x. When the users navigate to the AP Details page from the Client and Performance page of the WebUI Dashboard, the client filter is applied instead of the AP filter.</p> <p>Workaround: None.</p>
75857	<p>Symptom: An incorrect label is displayed on the WLAN Details page when the WLAN hyperlink is selected from the Client page.</p> <p>Scenario: This issue occurs on controllers running ArubaOS 6.2.x.x, when WLAN detail page is navigated from Client page, Client filter gets applied instead of the WLAN filter.</p> <p>Workaround: None.</p>

Table 150: WebUI Known Issues

Bug ID	Description
76836	<p>Symptom: A Javascript error occurs when trying to view the trend on the WLAN Summary page.</p> <p>Scenario: This issue occurs on controllers running ArubaOS 6.2.x.x, when the trend is performed on the Client entry hyperlink or distribution charts of Frame rates in Default or Tx/Rx Stats section. A blank screen with JS error is seen in Firebug.</p> <p>Workaround: None.</p>
77274	<p>Symptom: An error occurs when creating an access control list using the WebUI when the invert option is enabled in netdestination.</p> <p>Scenario: This issue occurs on controllers running ArubaOS 6.2.x.x, where an error occurs while creating the ACLs with netdestination created with invert option.</p> <p>Workaround: None.</p>
77542	<p>Symptom: The 600 Series controller is unable to upgrade from a local file.</p> <p>Scenario: For the local file upgrade to be successful, the controller must have at least 75 MB of free memory. When upgraded to ArubaOS 6.2.x.x, the 600 Series controller has only 77 MB of free memory remaining. And when the browser UI is launched, the free memory is decreased to 75 MB. In this case, the local file upgrade will fail. It is recommended that you do not use the local file upgrade function in the controller has less than 80 MB of free memory.</p> <p>Workaround: None. Use the USB, TFTP, SCP, or CLI option to upgrade instead.</p>
79146	<p>Symptom: The SSID does not display properly if the SSID name contains special characters.</p> <p>Scenario: This issue occurs on controllers running ArubaOS 6.2.x.x, when the cursor is placed on the WLAN.</p> <p>Workaround: Do not configure an SSID name with special characters.</p>
80260	<p>Symptom: Users cannot add use the WebUI to add a netdestination to a whitelist or blacklist in the Captive Portal profile.</p> <p>Scenario: This issue occurs on controllers running ArubaOS 6.2.x.x, where the whitelist and blacklist details do not contain any data on the Configuration > Security > Authentication > L3 Authentication > Captive Portal Profile page in the WebUI.</p> <p>Workaround: None.</p>
92770 94692	<p>Symptom: The Advanced Services > Stateful Firewall > Global Settings section of the WebUI do not correctly display settings defined in the following fields:</p> <ul style="list-style-type: none"> ● Monitor Ping Attack (per sec) ● Monitor TCP SYN Attack rate (per sec) ● Monitor IP Session Attack (per sec) <p>Scenario: This issue is triggered when ArubaOS 6.2.1.4 incorrectly overrides the configured values for the Monitor ping attack, Monitor TCP SYN attack, and Monitor IPv6 sessionsattack features.</p> <p>Workaround: None.</p>
95269	<p>Symptom: The controller WebUI does not display all entries in the remote AP whitelist.</p> <p>Scenario: This issue is observed in ArubaOS 6.2.1.4, when the remote AP whitelist contains more than 100 entries.</p> <p>Workaround: View the remote ap whitelist by accessing the command-line interface in enable mode, and issuing the command show whitelist-db rap.</p>

WMM

Table 151: *WMM Known Issues*

Bug ID	Description
68503	Symptom: The controller chooses an incorrect WMM priority (background instead of best-effort) in the downstream traffic. When same DSCP value is mapped to two different access categories, the lower of the two is used for the downstream traffic. Scenario: This issue is observed on controllers running ArubaOS 6.2.x.x or earlier in Tunnel and D-Tunnel modes. Workaround: None.

Issues Under Investigation

The following issues have been reported in ArubaOS 6.2.1.8 and are being investigated.

WebUI

Table 152: *WebUI Issues Under Investigation*

Bug ID	Description
93011	Symptom: Users may be unexpectedly logged out of the controller WebUI.

Maximum DHCP Leases Per Platform

Exceeding the following limits may result in excessive CPU utilization, and unpredictable negative impact on controller operations:

Table 153: *Maximum DHCP Lease Per Platform*

Platform	Maximum
7200 Series	5000
M3	512
3200XM	512
3400	512
3600	512
600 Series	512

This chapter details software upgrade procedures. It is recommended that you schedule a maintenance window for upgrading your controllers.



Read all the information in this chapter before upgrading your controller.

Topics in this chapter include:

- [Upgrade Caveats on page 81](#)
- [Important Points to Remember and Best Practices on page 82](#)
- [Memory Requirements on page 83](#)
- [Backing up Critical Data on page 83](#)
- [Upgrading in a Multi-Controller Network on page 84](#)
- [Upgrading to 6.2.x.x on page 85](#)
- [Downgrading on page 88](#)
- [Before You Call Technical Support on page 90](#)

Upgrade Caveats

Before upgrading to any version of ArubaOS 6.2.x.x, take note of these known upgrade caveats.

- Beginning with ArubaOS 6.2.0.0, the default **NAS-port-type** for management authentication using MSCHAPv2 is **Virtual** instead of **Wireless**. If your configuration uses the NAS-port-type in any derivation or access rules, this value will change for management user requests from the controller. This behavior is in line with IEEE RFC 2865. There is no change in behavior for management authentication using PAP.
- Beginning with ArubaOS 6.2.0.0, you cannot create redundant firewall rules in a single ACL. ArubaOS will consider a rule redundant if the primary keys are the same. The primary key is made up of the following variables:
 - source IP/alias
 - destination IP/alias
 - proto-port/service

If your pre-6.2 configuration contains an ACL with redundant firewall rules, upon upgrading, only the last rule will remain.

For example, in the below ACL, both ACE entries could not be configured in ArubaOS 6.2.x.x. Once the second ACE entry is added, the first would be over written.

```
(host) (config) #ip access-list session allowall-laptop
(host) (config-sess-allowall-laptop)# any any any permit time-range test_range
(host) (config-sess-allowall-laptop)# any any any deny
(host) (config-sess-allowall-laptop)#end
(host) #show ip access-list allowall-laptop

ip access-list session allowall-laptop
allowall-laptop
-----
Priority  Source  Destination  Service  Action  TimeRange
-----
1         any    any          any      deny
```

- ArubaOS 6.2.x.x is supported only on 7200 Series, M3, 3400, 3600, 600 Series, and 3200XM controllers. When upgrading the software in a multi-controller network (one that uses two or more controllers), special care must be taken to upgrade all the controllers in the network and to upgrade them in the proper sequence (See [Upgrading in a Multi-Controller Network on page 84](#)).
- For 600 Series and 7200 Series controllers, the local file upgrade option in the WebUI does not work when upgrading from ArubaOS 6.2 or later. When this option is used, the controller displays the error message **Content Length exceeds limit** and the upgrade fails. All other upgrade options work as expected.
- Upon upgrading to ArubaOS 6.2.x.x, the internal AP of the 650 controller is disabled. The controller then operates as a 650 controller.
- 3200XM controllers with 1GB of memory can be upgraded to ArubaOS 6.2.x.x. The 3200XM controller with 512MB of memory does not support ArubaOS 6.2.x.x.

Important Points to Remember and Best Practices

Ensure a successful upgrade and optimize your upgrade procedure by taking the recommended actions listed below. You should save this list for future use.

- Schedule the upgrade during a maintenance window and notify your community of the planned upgrade. This prevents users from being surprised by a brief wireless network outage during the upgrade.
- Avoid making any other changes to your network during the upgrade, such as configuration changes, hardware upgrades, or changes to the rest of the network. This simplifies troubleshooting.
- Know your network. Verify the state of your network by answering the following questions.
 - How many APs are assigned to each controller? Verify this information by navigating to the **Monitoring > Network All Access Points** section of the WebUI, or by issuing the **show ap active** and **show ap database** CLI commands.
 - How are those APs discovering the controller (DNS, DHCP Option, Broadcast)?
 - What version of ArubaOS is currently on the controller?
 - Are all controllers in a master-local cluster running the same version of software?
 - Which services are used on the controllers (employee wireless, guest access, remote AP, wireless voice)?
- Resolve any existing issues (consistent or intermittent) before you upgrade.
- If possible, use FTP to load software images to the controller. FTP is faster than TFTP and offers more resilience over slow links. If you must use TFTP, ensure the TFTP server can send over 30 MB of data.
- Always upgrade the non-boot partition first. If problems occur during the upgrade, you can restore the flash, and switch back to the boot partition. Upgrading the non-boot partition gives you a smoother downgrade path should it be required.

- Before you upgrade to the current version of ArubaOS, assess your software license requirements and load any new or expanded licenses you require. For a detailed description of these new license modules, refer to the “Software Licenses” chapter in the user guide.

Memory Requirements

All Aruba controllers store critical configuration data on an onboard compact flash memory module. Ensure that there is always free flash space on the controller. Loading multiple large files such as JPEG images for RF Plan can consume flash space quickly. To maintain the reliability of your WLAN network, Aruba recommends the following compact memory best practices:

- Issue the **show memory** command to confirm that there is at least 40 MB of free memory available for an upgrade using the CLI, or at least 60 MB of free memory available for an upgrade using the WebUI. Do not proceed unless this much free memory is available. To recover memory, reboot the controller. After the controller comes up, upgrade immediately.
- Issue the **show storage** command to confirm that there is at least 60 MB of flash available for an upgrade using the CLI, or at least 75 MB of flash available for an upgrade using the WebUI.



In certain situations, a reboot or a shutdown could cause the controller to lose the information stored in its compact flash card. To avoid such issues, it is recommended that you issue the **halt** command before power cycling.

If the output of the **show storage** command indicates that insufficient flash memory space is available, you must free up additional memory. Any controller logs, crash data or and flash backups should be copied to a location off the controller, then deleted from the controller to free up flash space. You can delete the following files from the controller to free memory before upgrading:

- **Crash Data:** Issue the **tar crash** command to compress crash files to a file named **crash.tar**. Use the procedures described in [Backing up Critical Data on page 83](#) to copy the **crash.tar** file to an external server, then issue the command **tar clean crash** to delete the file from the controller.
- **Flash Backups:** Use the procedures described in [Backing up Critical Data on page 83](#) to back up the flash directory to a file named **flash.tar.gz**, then issue the command **tar clean flash** to delete the file from the controller.
- **Log files:** Issue the **tar logs** command to compress log files to a file named **logs.tar**. Use the procedures described in [Backing up Critical Data on page 83](#) to copy the **logs.tar** file to an external server, then issue the command **tar clean logs** to delete the file from the controller.

Backing up Critical Data

It is important to frequently back up all critical configuration data and files on the compact flash file system to an external server or mass storage device. At the very least, you should include the following files in these frequent backups:

- Configuration data
- WMS database
- Local user database
- Licensing database
- Floor plan JPEGs
- Custom captive portal pages
- x.509 certificates

- Controller Logs

Back Up and Restore Compact Flash in the WebUI

The WebUI provides the easiest way to back up and restore the entire compact flash file system. The following steps describe how to back up and restore the compact flash file system using the WebUI on the controller:

1. Click on the **Configuration** tab.
2. Click the **Save Configuration** button at the top of the page.
3. Navigate to the **Maintenance > File > Backup Flash** page.
4. Click **Create Backup** to back up the contents of the compact flash file system to the flashbackup.tar.gz file.
5. Click **Copy Backup** to copy the file to an external server.

You can later copy the backup file from the external server to the compact flash file system using the file utility in the **Maintenance > File > Copy Files** page.

6. To restore the backup file to the Compact Flash file system, navigate to the **Maintenance > File > Restore Flash** page. Click **Restore**.

Back Up and Restore Compact Flash in the CLI

The following steps describe the back up and restore procedure for the entire compact flash file system using the controller's command line:

1. Enter enable mode in the CLI on the controller, and enter the following command:
(host) # write memory
2. Use the **backup** command to back up the contents of the Compact Flash file system to the flashbackup.tar.gz file.

```
(host) # backup flash
wait while we tar relevant files from flash...
wait while we compress the tar file...
Checking for free space on flash...
Copying file to flash...
File flashbackup.tar.gz created successfully on flash.
```

3. Use the **copy** command to transfer the backup flash file to an external server or storage device:

```
(host) copy flash: flashbackup.tar.gz ftp: <ftphost> <ftpusername> <ftpuserpassword>
<remote directory>
(host) copy flash: flashbackup.tar.gz usb: partition <partition-number>
```

You can later transfer the backup flash file from the external server or storage device to the Compact Flash file system with the copy command:

```
(host) # copy tftp: <tftphost> <filename> flash: flashbackup.tar.gz
(host) # copy usb: partition <partition-number> <filename> flash: flashbackup.tar.gz
```

4. Use the **restore** command to untar and extract the *flashbackup.tar.gz* file to the compact flash file system:
(host) # restore flash

Upgrading in a Multi-Controller Network

In a multi-controller network (a network with two or more Aruba controllers), special care must be taken to upgrade all controllers based on the controller type (master or local). Be sure to back up all controllers being upgraded, as described in [Backing up Critical Data on page 83](#).



For proper operation, all controllers in the network must be upgraded with the same version of ArubaOS software. For redundant (VRRP) environments, the controllers should be the same model.

To upgrade an existing multi-controller system to the current version of ArubaOS:

1. Load the software image onto all controllers (including redundant master controllers).
2. If all the controllers cannot be upgraded with the same software image and reloaded simultaneously, use the following guidelines:
 - a. Remove the link between the master and local mobility controllers.
 - b. Upgrade the software image, then reload the master and local controllers one by one.
 - c. Verify that the master and all local controllers are upgraded properly.
 - d. Connect the link between the master and local controllers.

Upgrading to 6.2.x.x

Install Using the WebUI



Confirm that there is at least 60 MB of free memory and at least 75 MB of flash available for an upgrade using the WebUI.



600 Series and 7200 Series controllers running ArubaOS 6.2.x.x cannot use the Local File upgrade option in the WebUI for further upgrades due to insufficient memory. Use other upgrade options in the WebUI.

Upgrading From an Older Version of ArubaOS

Before you begin, verify the version of ArubaOS currently running on your controller. If you are running one of the following versions of ArubaOS, you must download and upgrade to an interim version of ArubaOS before upgrading to the current version of ArubaOS.

- For ArubaOS 3.x versions earlier than ArubaOS 3.4.4.1, download the latest version of ArubaOS 3.4.5.x.
 - For ArubaOS RN-3.x or ArubaOS 5.0.x versions earlier than ArubaOS 5.0.3.1, download the latest version of ArubaOS 5.0.4.x.
 - For ArubaOS 6.0.0.x, download the latest version of ArubaOS 6.0.2.x.
1. Follow step 1-step 11 of the procedure described in [Upgrading From a Recent version of ArubaOS on page 85](#) to install the interim version of ArubaOS, then
 2. Repeat step 1-step 11 of the same procedure to download and install the current version of ArubaOS.

Upgrading From a Recent version of ArubaOS

The following steps describe the procedure to upgrade from one of the following versions of ArubaOS:

- ArubaOS 6.0.1.x or later 6.x
- ArubaOS 5.0.3.1 or later 5.0.x (If you are running ArubaOS 5.0.3.1 or a later 5.0.x release, review [Upgrading With RAP-5 and RAP-5WN APs on page 86](#) before proceeding further.)
- ArubaOS 3.4.4.1 or later 3.4.x releases.

Install the ArubaOS 6.2.1.8 software image from a PC or workstation using the Web User Interface (WebUI) on the controller. You can also install the software image from a TFTP or FTP server using the same WebUI page.

1. Download the current version of ArubaOS from the customer support site.
2. Upload the new software image(s) to a PC or workstation on your network.
3. Log in to the ArubaOS WebUI from the PC or workstation.
4. Navigate to the **Maintenance > Controller > Image Management** page. Select the **Upload Local File** option, then click **Browse** to navigate to the saved image file on your PC or workstation.

5. Select the downloaded image file.
6. In the **partition to upgrade** field, select the non-boot partition.
7. In the **Reboot Controller After Upgrade** option field, best practices is to select **Yes** to automatically reboot after upgrading. If you do not want the controller to reboot immediately, select **No**. Note however, that the upgrade will not take effect until you reboot the controller.
8. In **Save Current Configuration Before Reboot** field, select **Yes**.
9. Click **Upgrade**.
10. When the software image is uploaded to the controller, a popup window displays the message **Changes were written to flash successfully**. Click **OK**. If you chose to automatically reboot the controller in step 7, the reboot process starts automatically within a few seconds (unless you cancel it).
11. When the reboot process is complete, log in to the WebUI and navigate to the **Monitoring > Controller > Controller Summary** page to verify the upgrade.

Once your upgrade is complete, perform the following steps to verify that the controller is behaving as expected.

1. Log in into the WebUI to verify all your controllers are up after the reboot.
2. Navigate to **Monitoring > Network Summary** to determine if your APs are up and ready to accept clients.
3. Verify that the number of access points and clients are what you would expected.
4. Test a different type of client for each access method that you use and in different locations when possible.
5. Complete a back up of all critical configuration data and files on the compact flash file system to an external server or mass storage facility. See [Backing up Critical Data on page 83](#) for information on creating a backup.

Upgrading With RAP-5 and RAP-5WN APs

If you have completed the first upgrade hop to the latest version of ArubaOS 5.0.4.x and your WLAN includes RAP-5/RAP-5WN APs, do not proceed until you complete the following process. Once complete, proceed to [step 5 on page 86](#). Note that this procedure can only be completed using the controller's command line interface.

1. Check the provisioning image version on your RAP-5/RAP-5WN Access Points by executing the **show ap image version** command.
2. If the flash (Provisioning/Backup) image version string shows the letters *rn*, for example, 3.3.2.11-rn-3.0, note those AP names and IP addresses.
3. For each of the RAP-5/RAP-5WN APs noted in the step 2, upgrade the provisioning image on the backup flash partition by executing the following command:

```
apflash ap-name <Name_of_RAP> backup-partition
```

The RAP-5/RAP-5WN reboots to complete the provisioning image upgrade.

4. When all the RAP-5/RAP-5WN APs with a 3.3.2.x-based RN provisioning image have successfully upgraded, verify the provisioning image by executing the following command:

```
show ap image version
```

The flash (Provisioning/Backup) image version string should now show a version that does not contain the letters "rn", for example, 5.0.4.8.

If you omit the above process or fail to complete the flash (Provisioning/Backup) image upgrade to 5.0.4.x and the RAP-5/RAP-5WN was reset to factory defaults, the RAP will not be able to connect to a controller running the current version of ArubaOS and upgrade its production software image.

Install Using the CLI



Confirm that there is at least 40 MB of free memory and at least 60 MB of flash available for an upgrade using the CLI.

Upgrading From an Older version of ArubaOS

Before you begin, verify the version of ArubaOS currently running on your controller. If you are running one of the following versions of ArubaOS, you must download and upgrade to an interim version of ArubaOS.

- For ArubaOS 3.x versions earlier than ArubaOS 3.4.4.1, download the latest version of ArubaOS 3.4.5.x.
 - For ArubaOS RN-3.x or ArubaOS 5.0.x versions earlier than ArubaOS 5.0.3.1, download the latest version of ArubaOS 5.0.4.x.
 - For ArubaOS 6.0.0.x, download the latest version of ArubaOS 6.0.2.x.
1. Download the interim version of ArubaOS, then follow step 2-step 7 of the procedure described in [Upgrading From a Recent version of ArubaOS on page 87](#) to install that interim version.

Upgrading From a Recent version of ArubaOS

The following steps describe the procedure to upgrade from one of the following versions of ArubaOS:

- ArubaOS 6.0.1.x or later 6.x
- ArubaOS 5.0.3.1 or later 5.0.x.x (If you are running ArubaOS 5.0.3.1 or a later 5.0.x release, review [Upgrading With RAP-5 and RAP-5WN APs on page 86](#) before proceeding further.)
- ArubaOS 3.4.4.1 or later 3.4.x releases.

To install the ArubaOS software image from a PC or workstation using the Command-Line Interface (CLI) on the controller:

1. Download the latest version of ArubaOS from the customer support site.
2. Open a Secure Shell session (SSH) on your master (and local) controllers.
3. Execute the **ping** command to verify the network connection from the target controller to the SCP/FTP/TFTP server:

```
(hostname) # ping <ftphost>
```

or

```
(hostname) # ping <tftphost>
```

or

```
(hostname) # ping <scphost>
```

4. Use the **show image version** command to check the ArubaOS images loaded on the controller's flash partitions. The partition number appears in the **Partition** row; **0:0** is partition 0, and **0:1** is partition 1. The active boot partition is marked as **Default boot**.

```
(hostname) #show image version
```

```
-----  
Partition           : 0:0 (/dev/ha1)  
Software Version    : ArubaOS 6.1.1.0 (Digitally Signed - Production Build)  
Build number        : 28288  
Label               : 28288  
Built on            : Thu Apr 21 12:09:15 PDT 2012  
-----
```

```
Partition           : 0:1 (/dev/ha1)**Default boot**  
Software Version    : ArubaOS 6.1.3.2 (Digitally Signed - Production Build)  
Build number        : 33796  
Label               : 33796  
Built on            : Fri May 25 10:04:28 PDT 2012
```

5. Use the **copy** command to load the new image onto the non-boot partition:

```
(hostname) # copy ftp: <ftphost> <ftpusername> <image filename> system: partition <0|1>
```

or

```
(hostname) # copy tftp: <tftphost> <image filename> system: partition <0|1>
```

or

```
(hostname)# copy scp: <scphost> <scpusername> <image filename> system: partition <0|1>
```

or

```
(hostname)# copy usb: partition <partition-number> <image filename> system: partition <0|1>
```

6. Execute the **show image version** command to verify the new image is loaded:

```
(hostname)# show image version
```

7. Reboot the controller:

```
(hostname)# reload
```

8. Execute the **show version** command to verify the upgrade is complete.

```
(hostname)# show version
```

Once your upgrade is complete, perform the following steps to verify that the controller is behaving as expected.

1. Log in into the command-line interface to verify all your controllers are up after the reboot.
2. Issue the command **show ap active** to determine if your APs are up and ready to accept clients.
3. Issue the command **show ap database** to verify that the number of access points and clients are what you would expected.
4. Test a different type of client for each access method that you use and in different locations when possible.
5. Complete a backup of all critical configuration data and files on the compact flash file system to an external server or mass storage facility. See [Backing up Critical Data on page 83](#) for information on creating a backup.

Downgrading

If necessary, you can return to your previous version of ArubaOS.



If you upgraded from 3.3.x to 5.0, the upgrade script encrypts the internal database. New entries created in the current release are lost after the downgrade (this warning does not apply to upgrades from 3.4.x to 6.1).



If you do not downgrade to a previously-saved pre-6.1 configuration, some parts of your deployment may not work as they previously did. For example, when downgrading from the current version of ArubaOS to 5.0.3.2, changes made to WIPS in 6.x prevents the new predefined IDS profile assigned to an AP group from being recognized by the older version of ArubaOS. This unrecognized profile can prevent associated APs from coming up, and can trigger a profile error.

These new IDS profiles begin with **ids-transitional**, while older IDS profiles do not include transitional. If you think you have encountered this issue, use the **show profile-errors** and **show ap-group** commands to view the IDS profile associated with AP Group.



When reverting the controller software, whenever possible, use the previous version of software known to be used on the system. Loading a release not previously confirmed to operate in your environment could result in an improper configuration.

Before you Begin

Before you reboot the controller with the pre-upgrade software version, you must perform the following steps:

1. Back up your controller. For details, see [Backing up Critical Data on page 83](#).
2. Verify that control plane security is disabled.
3. Set the controller to boot with the previously-saved pre-6.2 configuration file.
4. Set the controller to boot from the system partition that contains the previously running ArubaOS image.

When you specify a boot partition (or copy an image file to a system partition), the software checks to ensure that the image is compatible with the configuration file used on the next controller reload. An error message displays if system boot parameters are set for incompatible image and configuration files.

5. After downgrading the software on the controller:
 - Restore pre-6.2 flash backup from the file stored on the controller. Do not restore the current version of the flash backup file.
 - You do not need to re-import the WMS database or RF Plan data. However, if you have added changes to RF Plan in the current version of ArubaOS, the changes do not appear in RF Plan in the downgraded ArubaOS version.
 - If you installed any certificates while running the current version of ArubaOS, you need to reinstall the certificates in the downgraded ArubaOS version.

Downgrading Using the WebUI

The following sections describe how to use the WebUI to downgrade the software on the controller.

1. If the saved pre-upgrade configuration file is on an external FTP/TFTP server, copy the file to the controller by navigating to the **Maintenance > File > Copy Files** page.
 - a. For **Source Selection**, select FTP/TFTP server, and enter the IP address of the FTP/TFTP server and the name of the pre-upgrade configuration file.
 - b. For **Destination Selection**, enter a filename (other than default.cfg) for Flash File System.
2. Set the controller to boot with your pre-upgrade configuration file by navigating to the **Maintenance > Controller > Boot Parameters** page.
 - a. Select the saved pre-upgrade configuration file from the Configuration File menu.
 - b. Click **Apply**.
3. Determine the partition on which your previous software image is stored by navigating to the **Maintenance > Controller > Image Management** page. If there is no previous software image stored on your system partition, load it into the backup system partition (you cannot load a new image into the active system partition):
 - a. Enter the FTP/TFTP server address and image file name.
 - b. Select the backup system partition.
 - c. Click **Upgrade**.
4. Navigate to the **Maintenance > Controller > Boot Parameters** page.
 - a. Select the system partition that contains the pre-upgrade image file as the boot partition.
 - b. Click **Apply**.
5. Navigate to the **Maintenance > Controller > Reboot Controller** page. Click **Continue**. The controller reboots after the countdown period.
6. When the boot process is complete, verify that the controller is using the correct software by navigating to the **Maintenance > Controller > Image Management** page.

Downgrading using the CLI

The following sections describe how to use the CLI to downgrade the software on the controller.

1. If the saved pre-upgrade configuration file is on an external FTP/TFTP server, use the following command to copy it to the controller:

```
(host) # copy ftp: <ftphost> <ftpusername> <image filename> system: partition 1
or
(host) # copy tftp: <tftphost> <image filename> system: partition 1
```
2. Set the controller to boot with your pre-upgrade configuration file.

- ```
boot config-file <backup configuration filename>
```
3. Execute the **show image version** command to view the partition on which your previous software image is stored. You cannot load a new image into the active system partition (the default boot).
  4. Set the backup system partition as the new boot partition:

```
boot system partition 0
```
  5. Reboot the controller:

```
reload
```
  6. When the boot process is complete, verify that the controller is using the correct software:

```
show image version
```

## Before You Call Technical Support

Before you place a call to Technical Support, follow these steps:

1. Provide a detailed network topology (including all the devices in the network between the user and the Aruba controller with IP addresses and Interface numbers if possible).
2. Provide the wireless device's make and model number, OS version (including any service packs or patches), wireless NIC make and model number, wireless NIC's driver date and version, and the wireless NIC's configuration.
3. Provide the controller logs and output of the **show tech-support** command via the WebUI Maintenance tab or via the CLI (**tar logs tech-support**).
4. Provide the syslog file of the controller at the time of the problem. Aruba strongly recommends that you consider adding a syslog server if you do not already have one to capture logs from the controller.
5. Let the support person know if this is a new or existing installation. This helps the support team to determine the troubleshooting approach, depending on whether you have an outage in a network that worked in the past, a network configuration that has never worked, or a brand new installation.
6. Let the support person know if there are any recent changes in your network (external to the Aruba controller) or any recent changes to your controller and/or AP configuration. If there was a configuration change, list the exact configuration steps and commands used.
7. Provide the date and time (if possible) when the problem first occurred. If the problem is reproducible, list the exact steps taken to recreate the problem.
8. Provide any wired or wireless sniffer traces taken during the time of the problem.
9. Provide the controller site access information, if possible.

This chapter discusses the steps required to migrate your existing controllers to 7200 Series controllers.



---

For information about migrating to the 7200 Series Controller, visit [www.support.arubanetworks.com](http://www.support.arubanetworks.com).

---

## Migrating to the 7200 Series Controller

You must complete the following tasks to complete the migration process:

- Back up the controller data from your existing controller.
- Upgrade your network to ArubaOS 6.2.x.x. This ensures that the image on your new controllers matches the image of the rest of the controllers in your network.
- Back up the controller data from your upgraded, existing controller.
- Transfer existing licenses to your new controller.
- Install your new controller.
- Install the backed up data on your new controller.
- Apply transferred and new licenses.
- Reload your controller.
- Update port-related configuration.
- Confirm that your new controller operates as expected.

### Important Points to Remember

- The 7200 Series controllers use a different port number scheme than other controllers. Ports on the 7200 Series are numbered **slot/module/port**. Other controller ports are numbered **slot/port**.
- Not all Aruba controller models support ArubaOS 6.2. The following controllers support ArubaOS 6.2:
  - 7200 Series
  - M3
  - 3200XM, 3400, and 3600
  - 600 Series



---

Beginning in ArubaOS 6.2, the 650 controller's internal AP is disabled. Additionally, upon upgrade, the 650 will appear as a 650-1 and the 650-8 will appear as a 650-9 in ArubaOS.

---

- You can complete this migration process on a controller-by-controller basis if your replaced controllers support ArubaOS 6.2. The entire deployment does not need to be completed at the same time.
- When replacing a master controller, replace the backup master first.
- If you are migrating to a 7200 Series controller from a controller not listed above, contact Aruba support.

### Backing Up Your Data Before Upgrading to 6.2

Back up your controller data before upgrading to ArubaOS 6.2. To back up your controller data, complete the steps in the following sections:

## Back Up the Flash File System in the WebUI

1. Click on the **Configuration** tab.
2. Click the **Save Configuration** button at the top of the page.
3. Navigate to the **Maintenance > File > Backup Flash** page.
4. Click **Create Backup** to back up the contents of the compact flash file system to the flashbackup.tar.gz file.
5. Click **Copy Backup** to copy the file to an external server.
6. Copy the backup file from the external server to the compact flash file system using the file utility in the **Maintenance > File > Copy Files** page.

## Back Up the Flash File System in the CLI

1. Enter **enable** mode in the CLI on the controller, and enter the following command:  

```
(host) # write memory
```
2. Use the **backup** command to back up the contents of the Compact Flash file system to the flashbackup.tar.gz file.  

```
(host) # backup flash
wait while we tar relevant files from flash...
wait while we compress the tar file...
Checking for free space on flash...
Copying file to flash...
File flashbackup.tar.gz created successfully on flash.
```
3. Use the **copy** command to transfer the backup flash file to an external server:  

```
(host) copy flash: flashbackup.tar.gz ftp: <ftphost> <ftpusername> <ftpuserpassword>
<remote directory>
```

## Upgrading Your Network

Before attempting upgrade any of your controllers, read the [Upgrade Procedures on page 81](#). If you are migrating from controllers that do not support ArubaOS 6.2, best practices are to upgrade to the latest supported build of your current version of ArubaOS before beginning the migration process.

[Table 154](#) provides a brief overview of the steps required to upgrade to ArubaOS 6.2.1.8.

**Table 154:** ArubaOS 6.2 Upgrade Path Overview

| Version                                                                                                         | Step 1                        | Step 2         |
|-----------------------------------------------------------------------------------------------------------------|-------------------------------|----------------|
| 3.x, earlier than 3.4.4.1                                                                                       | Upgrade to the latest 3.4.5x  | Upgrade to 6.2 |
| RN-3.x                                                                                                          | Upgrade to the latest 5.0.4.x | Upgrade to 6.2 |
| 5.x, earlier than 5.0.3.1                                                                                       | Upgrade to the latest 5.0.4.x | Upgrade to 6.2 |
| 6.0.0.x                                                                                                         | Upgrade to the latest 6.0.2.x | Upgrade to 6.2 |
| 6.2.0.x, 6.1.x.x, 6.0.1.x, 6.0.2.x,<br>5.0.3.1 (or later 5.0.3.x), 5.0.4.x<br>3.4.4.1 (or later 3.4.x), 3.4.5.x | Upgrade to 6.2                | –              |

## Backing Up Your Data After Upgrading to 6.2

After completing the upgrade to ArubaOS 6.2, back up your controller data and configuration once more before continuing. It is recommended that you rename your backup file and transfer to an external storage device.

## Transferring Licenses

To transfer existing licenses from one controller to another:

1. Open a browser, navigate to <https://licensing.arubanetworks.com/>, and log in.
2. Navigate to **Certificate Management > Transfer certificate** and select the licenses you want to transfer.
3. All the certificates active on the controller of the license certificate you have selected will be displayed. Select all the certificates you would like to transfer.
4. Enter the serial number of the new controller and click **Transfer**. When the transfer has been completed successfully, you will receive a new set of activation keys.

The selected certificates must be compatible with your new controller. If not, you will not be able to complete the transfer. You will receive the following error message: **This certificate is not compatible with your system!**

If the destination controller does not exist, you will receive the following error message: **This system does not exist**. If you receive this error, ensure that you entered the serial number correctly. Once you have verified that the serial number you entered was correct, contact Aruba Technical Support.

## Installing Your New Controller

For instructions and additional information about installing your 7200 Series controller, refer to the *Aruba 7200 Series Controller Installation Guide* and *ArubaOS 6.2 Quick Start Guide* included with your device. For the latest version of these documents, visit [support.arubanetworks.com](http://support.arubanetworks.com) and click the **Documentation** tab.

After installing your 7200 Series, verify that it is running the latest version of ArubaOS 6.2. If not, it is recommended that you upgrade your controller.

## Installing Backed Up Controller Data

Follow the instructions below to install backed up controller data. Do not modify your configuration before reloading the controller.



---

7200 Series controllers use a different port numbering scheme than other controllers. Ports on the 7200 Series are numbered **slot/port/module**. Other controller ports are numbered **slot/port**. Once you've loaded your old configuration onto a 7200 Series controller, you will no longer be able to connect to the controller over the network. Additionally, all ports will become untrusted. You must connect to your new controller using a serial connection to reconfigure port settings.

---

To install your existing configuration and controller data onto your new controller, complete the following steps.

### Restore the Flash File System in the WebUI

1. Navigate to the **Maintenance > File > Copy Files** page.
  - a. For **Source Selection**, specify the server to which the `flashbackup.tar.gz` file was previously copied.
  - b. For **Destination Selection**, select **Flash File System**.
  - c. Click **Apply**.
2. Navigate to the **Maintenance > File > Restore Flash** page.
3. Click **Restore** to restore the `flashbackup.tar.gz` file to the flash file system.
4. Install licenses before you reboot your controller. Do not modify your configuration until after the controller reloads.

### Restore the Flash File System in the CLI

1. Enter **enable** mode in the CLI on the controller.

2. Transfer the `flashbackup.tar.gz` file from its external location to the controller's flash using the commands that follow according to your preferred method.

```
copy ftp: <ftphost> <srcfilename> flash: flashbackup.tar.gz
copy tftp: <tftphost> <srcfilename> flash: flashbackup.tar.gz
copy scp: <scphost> <username> <srcfilename> flash: flashbackup.tar.gz
copy usb: partition <partition-number> <srcfilename> flash: flashbackup.tar.gz
```

```
restore flash
```

3. Install licenses before you reboot your controller. Do not modify your configuration until after the controller reloads.

## Applying Licenses

After you have installed your new controller and brought it up, you can apply and back up any new or transferred licenses.

### Applying the Software License Key in the WebUI

1. Log in to your controller's WebUI.
2. Navigate to the **Configuration > Network > Controller** select the **License** tab.
3. Copy the software license key, from your email, and paste it into the **Add New License Key** field. Click **Add**.
4. Reboot your controller to enable the new license feature.

### Applying the Software License Key in the License Wizard

1. Log in to your controller's WebUI.
2. Launch the License Wizard from the **Configuration** tab and click the **New** button.
3. The License Wizard will step you through the activation process. Click on the Help tab within the License Wizard for additional assistance.
4. Reboot your controller to enable the new license feature.

### Backing Up Licenses in the WebUI

1. Log in to your controller's WebUI.
2. Navigate to the **Configuration > Network > Controller** and select the **License** tab.
3. Scroll to the bottom of the page and click **Export Database**.
4. Enter the file name of the file to export and click **OK**.
5. Copy the backup file from the external server or USB storage device to the compact flash file system using the file utility in the **Maintenance > File > Copy Files** page.

### Backing Up Licenses in the CLI

1. Use the license export `<filename>` command to create a license backup.

```
(host) #license export licensebackup.db
Successfully exported 1 licenses from the License Database to licensebackup.db
```

2. Use the `copy` command to transfer the backup flash file to an external server or USB drive:

```
(host) copy flash: licensebackup.db ftp: <ftphost> <ftpusername> <ftpuserpassword> <remote
directory>
(host) #copy flash: licensebackup.db usb: partition <partition-number> licensebackup.db
```

## Reload Your Controller

After restoring flash and transferring licenses, you must reboot your controller before continuing.

## Establishing Network Connectivity

Due to the difference in port numbering schemes between the 7200 Series and older controller platforms, your 7200 Series controller will not have network connectivity and all ports will become untrusted after installing your previous controller's configuration in data. All previous controller models used a **slot/port** number scheme; the 7200 Series uses **slot/module/port**. To establish network connectivity, you must manually reconfigure your controller interfaces.



---

Slot and module will always be 0 and 0 on the 7200 Series controller. The first two ports on the 7200 Series, 0/0/0 and 0/0/1 are combination ports and can be used for management, HA, and data traffic. Ports 0/0/2 through 0/0/5 can only be used for data traffic. Keep this in mind when reconfiguring your ports.

---

### Connecting to the Controller

Since your 7200 Series controller does not have network connectivity, you must directly connect to it using a serial port connection. Once connected, you will receive a login prompt. Login using your configured credentials.

After you restore the flash and rebooting, all inherited port configurations are be lost. This can include, but is not limited to, trusted settings, port channel, and port monitoring settings. The following commands are affected by this new port numbering scheme and must be considered when reconfiguring your ports:

```
interface gigabitethernet <slot/port/module>
 trusted

interface range gigabitethernet <slot/port/module>

interface port-channel gigabitethernet
 add <slot/port/module>
 delete <slot/port/module>

interface gigabitethernet port monitor <slot/port/module>

interface vlan <vlan-id>
 ip igmp proxy gigabitethernet <slot/port/module>
```

### Verifying Controller Operation

Once you have completed the tasks described above, verify that your controller and the expected APs come up and are active.

#### Verifying Migration in the WebUI

1. Log in into the WebUI to verify all your controllers are up after the reboot.
2. Navigate to **Monitoring > Network Summary** to determine if your APs are up and ready to accept clients.
3. Verify that the number of access points and clients are what you would expect.
4. Test a different type of client for each access method that you use, and in different locations when possible.
5. Complete a backup of all critical configuration data and files on the compact flash file system to an external server or mass storage facility.

#### Verifying Migration in the CLI

1. Log in into the CLI to verify all your controllers are up after the reboot.
2. Use the command **show ap active** to determine if your APs are up and ready to accept clients.
3. Issue the command **show ap database** to verify that the number of access points and clients are what you would expect.
4. Test a different type of client for each access method that you use, and in different locations when possible.

5. Backup all critical configuration data and files on the compact flash file system to an external server or mass storage facility. See [Backing Up Your Data Before Upgrading to 6.2 on page 91](#).