ArubaOS 6.2.1.4

Release Notes

www.arubanetworks.com

1344 Crossman Avenue
Sunnyvale, California 94089

Phone: 408.227.4500
Fax 408.227.4550

Contents

Chapter 1

Release Overview

ArubaOS 6.2.1.4 is a software patch release that includes fixes to a number of known issues. 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*.

NOTE

See the Upgrade Procedures on page 61 for instructions on how to upgrade your controller to this release.

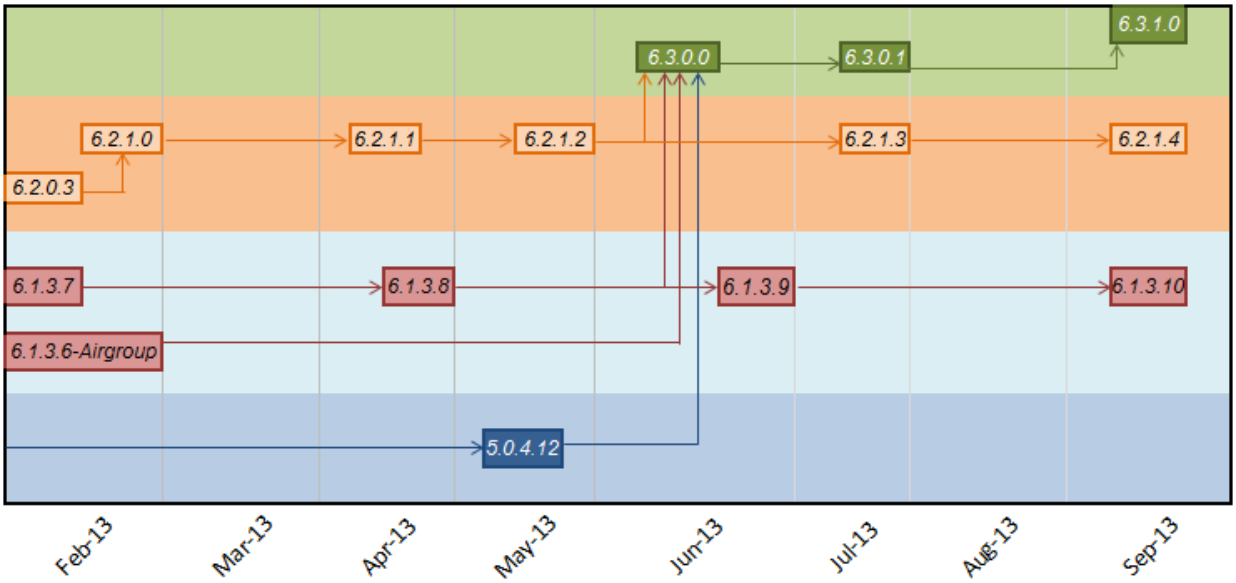
Chapter Overview

- What's New in this Release on page 9 describes the fixes introduced in this release.
- Features Added in Previous Releases on page 19 provides descriptions of features and enhancements added in previous 6.2.0.x releases.
- Issues Fixed in Previous Releases on page 25 lists issues fixed in previous releases of 6.2.
- Known Issues observed in Previous Releases on page 51 provides descriptions and workarounds for outstanding issues in ArubaOS 6.2.1.4.
- Upgrade Procedures on page 61 cover the procedures for upgrading your controller from any release of ArubaOS to ArubaOS 6.2.1.4.
- 7200 Series Migration on page 73 provides instructions for migrating your existing controllers to the new 7200 Series controller. For additional information, see support.arubanetworks.com.

Release Mapping

The following illustration shows which patches and maintenance releases are included in their entirety in ArubaOS 6.2.1.4.

Figure 1 *ArubaOS Releases and Code Stream Integration*



Supported Browsers

Beginning with ArubaOS 6.2, the following browsers are officially supported for use with the ArubaOS WebUI:

- Microsoft Internet Explorer 8.x and 9.x on Windows XP, Windows Vista, Windows 7, and MacOS
- Mozilla Firefox 14, 15, and 16 on Windows XP, Windows Vista, Windows 7, and MacOS
- Apple Safari 5.x on MacOS

Contacting Support

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

This chapter describes regulatory enhancements and issues resolved in ArubaOS 6.2.1.4. In addition, it lists new issues discovered since the prior release, and customer issues currently under investigation.

Regulatory Enhancements

The following table describes regulatory enhancements introduced in ArubaOS 6.2.1.4:

NOTE: Check with your local Aruba sales representative on device availability and support for countries listed in the following table.

Table 1 *Regulatory Domain Updates*

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

Resolved Issues in ArubaOS 6.2.1.4

802.1X Authentication

Table 2 *802.1X Fixed Issues*

Bug ID	Description
71930	**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. **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.
85896	**Symptom**: A controller rebooted after an internal controller module stopped responding. Internal memory improvements resolve this issue. **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.

Table 2 *802.1X Fixed Issues (Continued)*

Bug ID	Description
86162	**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. **Scenario**: This issue was triggered by some 2k server certificates. This issue was observed on 6000 controller platforms with XLR/XLS processors, 3000 Series, and 600 Series controllers running ArubaOS 6.x.

AP-Datapath

Table 3 *AP-Datapath Fixed Issues*

Bug ID	Description
86469	**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 4 *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 5 *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 6 *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.

BaseOS Security

Table 7 *BaseOS Security Fixed Issues*

Bug ID	Description
81390	**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. **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.
80396	**Symptom**: An internal (profmgr) 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. **Scenario**: This issue occurred when a configuration profile referring to an external RADIUS server, for example, the aaa-server-group 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, 6.2.x, and 6.3.x.

Captive Portal

Table 8 *Captive Portal Fixed Issues*

Bug ID	Description
87294	**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. **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.

Controller Datapath

Table 9 *Controller Datapath Fixed Issues*

Bug ID	Description
84071	**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. **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.
83029	**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. **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.

Controller Platform

Table 10 *Controller Platform Fixed Issues*

Bug ID	Description
85398	**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. **Scenario:** This issue occurred on a 3400 controller configured to operate as a DNS server while running ArubaOS 6.1.3.6.
85685	**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. **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 a specific controller or ArubaOS release.
86266	**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. **Scenario**: This issue was triggered by varying sequences of commands issued via the telnet shell, and is not specific to any controller model or release version.
87794 88311 88360 88683 88740 88505 88833	**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. **Scenario**: This issue occurred in 7200 Series controllers running ArubaOS 6.2.1.x.

Intrustion Detection System

Table 11 *IDS Fixed Issues*

Bug ID	Description
86681	**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**. **Scenario:** This issue occurred because legitimate frames sent with a large duration were also treated as an IDS Large Duration attack, triggering false alarms.

Mobility

Table 12 *Mobility Fixed Issues*

Bug ID	Description
88063	**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. **Scenario**: This issue occurrs 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.

PPPoE

Table 13 *PPPoE Fixed Issues*

Bug ID	Description
85398	**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. **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.

Voice

Table 14 *Voice Fixed Issues*

Bug ID	Description
86864	**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 wired voice clients are deleted from the SNMP tree resolve this issue. **Scenario**: This issue occurred on controllers running ArubaOS 6.2.1.0 with voice clients connected to the controller using a wired connection.
86224	**Symptom**: Calls dropped after 30 seconds when performing a blindly transferred SIP call. **Scenario**: This issue was observed on the M3 controller module running ArubaOS version 6.2.1. It occurred when Ascom phones sent a DELTS request upon receiving either an "invite" message from the SIP server or after sending a "180 Ringing" message back to the server.

WebUI

Table 15 *WebUI Fixed Issues*

Bug ID	Description
73459	**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. **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 release.
80233 85375	**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. **Scenario**: This issue occurred on a master/local topology with one 6000 master controller and two local controllers running ArubaOS 6.2.1.0.

Known Issues in ArubaOS 6.2.1.4

The following issues have been identified since the last release. For a list of known issues found in previous versions of ArubaOS, see Chapter 5, “Known Issues observed in Previous Releases” .

AP Platform

Table 16 *AP Platform Known 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. **Scenario**: This issue is triggered by network congestion or breaks in the connection between the controller and AP. **Workaround**: None.
89916	**Symptom**: AP-125 access points unexpectedly reboot. Log files for the event indicate that the APs reboot because they are out of memory. **Scenario**: This issue is observed AP-125 access points associated to a local controller running ArubaOS 6.2.1.x. **Workaround**: None.
89701	**Symptom**: An AP is unable to handle fragmented PAPI packets that arrive at their destination out of order, causing the AP to fail to gets its configuration when it boots up. **Scenario**: This issue is observed in ArubaOS 6.2.1.2 in a network where when the VPN link is heavily loaded, although the error clears when the packets arrive in the correct order. **Workaround**: Enabling control place security will resolve the problem the remote sites.

ARM

Table 17 *ARM Known Issues*

Bug ID	Description
88514	**Symptom**: The Adaptive Radio Management (ARM) feature is not correctly setting power levels on APs. **Scenario**: This issue is observed in ArubaOS 6.2.1.1, when ARM sets APs to use their maximum power levels to overcome high levels of interference, even though the output of the **show ap tech-support** command shows that the APs are not experiencing high levels of interference. **Workaround**: None.

BaseOS Security

Table 18 *BaseOS Security Known Issues*

Bug ID	Description
86867	**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. **Scenario**: This issue was observed on a controller running ArubaOS 6.2.1.2. **Workaround**: Do not create an ACL for the IP access-group that has a name matching that of any user-role in the configuration.

Controller Datapath

Table 19 *Controller Datapath Known Issues*

Bug ID	Description
82402	**Symptom**: A controller unexpectedly rebooted. The controller log files listed the reason for the event as **Nanny rebooted machine - httpd_wrap process died**. **Scenario**: This issue occurs on a controllers running ArubaOS 6.2.x. **Workaround**: None.

Controller Platform

Table 20 *Controller Platform Known Issues*

Bug ID	Description
86903	**Symptom**: An M3 controller module may not consistently respond to ping messages for the first 1-2 minutes after that module reboots. **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. **Workaround**: None.
87410	**Symptom**: A controller unexpectedly stops responding and reboots. The controller log files list the reason for the event as a **Watchdog Timeout**. **Scenario**: This issue occurs when messages are not correctly sent from the module of the controller that manages control plane security and the controller datapath. This triggers a failure process that timed out, causing the watchdog error. **Workaround**: None.

WebUI

Table 21 *WebUI Known Issues*

Bug ID	Description
88398	**Symptom**: The **Dashboard > Security page** of a controller running ArubaOS 6.2.1.3 does not allow network administrators to manually contain or reclassify a group of detected rogue APs. **Scenario**: This issue occurs when multiple rogue APs are selected in the **Dashboard > Security** page. **Workaround**: Reclassify or manually contain rogue APs individually, rather than managing them as a group.

Issues Under Investigation

The following issues have been reported in ArubaOS but not confirmed. The issues have not been reproduced yet, and the root cause has not yet been determined. They are included here because they have been reported to Aruba, and are being investigated. In the tables below, issues have been grouped together by topic and then by the Bug ID number.

802.1X Authentication

Table 22 *802.1X Authentication Observed Issues*

Bug ID	Description
89836	**Symptom**: Some wireless clients running Windows 7 and Windows XP are unable to authenticate on AP-105 access points. The key exchange process halts at wpa2-key3.

AP Platform

Table 23 *AP Platform Observed Issues*

Bug ID	Description
85112	**Symptom**: Changing an AP from AP mode to AM (Air Monitor) mode fails to correctly trigger the trap *wlsxAPModeChange*.
88763 88827 89714 89741	**Symptom**: AP-125 access points associated to a 7200 Series 6000 or 3400 controller running ArubaOS 6.2.1.3 unexpectedly rebooted.

BaseOS Security

Table 24 *BaseOS Security Observed Issues*

Bug ID	Description
88011	**Symptom**: A MAC address ACL created on a master controller was not correctly pushed to the standby controller. However, session ACLs are correctly pushed from the master to the standby controller.

Controller Datapath

Table 25 *Controller Datapath Observed Issues*

Bug ID	Description
88011	**Symptom**: Some clients using captive portal authentication can not access the captive portal login page, and do not correctly receive DNS responses. This issue is triggered when the controller failed to correctly add client MAC addresses to the internal ARP table.

Controller Platform

Table 26 *Controller Platform Observed Issues*

Bug ID	Description
88107	**Symptom**: A controller unexpectedly reboots. The controller log files list the reason for the event as **User Pushed Reset**. This issue occurred on a standalone 3000 Series controller running ArubaOS 6.2.1.2.
88241	**Symptom**: A controller unexpectedly reboots. The controller log files indicated that the internal wireless management (WMS) module triggered the issue. This issue occurred on a M3 controller module running ArubaOS 6.2.1.2.
89924 90029	**Symptom**: A controller unexpectedly reboots. The controller log files indicated that the internal station management (STM) module triggered the issue. This issue occurred on a 7200 Series controller running ArubaOS 6.2.1.3.
89539	**Symptom**: A controller unexpectedly reboots. The controller log files indicated that the internal datapath module triggered the issue. This issue occurred on a 7200 Series controller module running ArubaOS 6.2.1.2.
88494 89817 89829 89436 89839	**Symptom**: A controller unexpectedly reboots. The controller log files list the reason for the event as **Kernel Panic**. This issue occurred on 7200 Series and 3000 Series controllers and M3 controller modules running ArubaOS 6.2.1.x in a master-local topology.
89892	**Symptom**: The syslog daemon on a controller running ArubaOS 6.2.1.3 consumes excessive CPU resources.

Controller Software

Table 27 *Controller Software Observed Issues*

Bug ID	Description
88814	**Symptom**: The output of the **show user-table verbose** command indicates that clients incorrectly receive IPv6 router advertisements and IPv6 IP addresses from VLANs other than those to which the clients are associated.
89460	**Symptom**: During an unlimited throughput UDP test with 128 byte packets, client traffic slowed significantly, and clients were incorrectly disassociated from the network.

Remote AP + Branch Office AP

Table 28 *Remote AP + Branch Office AP Observed Issues*

Bug ID	Description
86650	**Symptom**: A controller is sending continuous RADIUS requests for the clients connected behind the wired port of a remote AP (RAP). The wired AP is in split-tunnel mode and uses both MAC and 802.1X authentication.

SNMP

Table 29 *SNMP Observed Issues*

Bug ID	Description
88618	**Symptom**: A 3000 Series controller running ArubaOS 6.2.1.0 is unable to use an SNMP MIB walk to determine values in the table w*lsxSysXMemoryTable*.

Chapter 3

Features Added in Previous Releases

This chapter describes features introduced in previous releases of ArubaOS 6.2.1.x. For more information about features introduced in ArubaOS 6.2.0.x, refer to the *ArubaOS 6.2.0.3 Release Notes*.

Introduced in ArubaOS 6.2.1.3

Regulatory Enhancements

The following table describes regulatory enhancements introduced in ArubaOS 6.2.1.3.

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

Table 30 *Country Code Regulatory Updates*

Country	Change
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-175P/AP-175AC access points.

Table 30 *Country Code Regulatory Updates (Continued)*

Country	Change
Macau	Added support for AP-134/AP-135 access points.
Macau, Ukraine	Added support for the AP-175P access point.
Canada	Enabled DFS channels for AP-175P/AC/DC 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/RAP-109 access points.

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
```

Introduced in ArubaOS 6.2.1.2

Regulatory Enhancements

The following changes impact new installations of RAP-108, RAP-109, AP-124, AP-125, AP-134, and AP-135 access points running ArubaOS 6.2.1.2:

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

Table 31 *Changes in this Release*

Country Domain	Change
Changes for RAP-108/RAP-109 Access Points	

Table 31 *Changes in this Release (Continued)*

Country Domain	Change
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 and100-140. 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.
Australia, New Zealand	These country domains support all channels allowed by the FCC (including indoor, outdoor and DFS channels).

Table 31 *Changes in this Release (Continued)*

Country Domain	Change
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.

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 4**G 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 32.

Table 32 *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).

Table 32 *Cellular Network Preference Parameters*

Parameter	Description
3g_only	Locks the modem to operate only in 3G
4g_only	Locks the modem to operate only in 4G
advanced	The remote AP (RAP) controls the cellular network service selection based on an Received Signal Strength Indication (RSSI) threshold-based approach. • 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)
```

Chapter 4

Issues Fixed in Previous Releases

This chapter describes issues fixed in a previous ArubaOS 6.2.1.x release. For information on issues resolved in ArubaOS 6.2.0.x, refer to the *ArubaOS 6.2.0.3 Release Notes*.

Resolved Issues in ArubaOS 6.2.1.3

The following issues are resolved in ArubaOS 6.2.1.3:

Air Management - IDS

Table 33 *Air Management - IDS Fixed Issues*

Bug ID	Description
84889	**Symptom:** False alarms for AP spoof detection were observed in ArubaOS 6.3. 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 release version.

AP-Platform

Table 34 *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's Ethernet driver. **Scenario:** This issue occurred when the IP phone was connected to the enet interface of RAP-3WN 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 limited to any specific version of ArubaOS.

AP-Datapath

Table 35 *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 36 *AP-Regulatory Fixed Issues*

Bug ID	Description
76222	**Symptom:** The country code for Algeria was not supportd on AP-105, AP-92, and AP-93 access pointes. 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 37 *AP-Wireless Fixed Issues*

Bug ID	Description
85806	**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. **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.

Base OS Security

Table 38 *Base OS Security Fixed Issues*

Bug ID	Description
72093	**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 resolved this issue. **Scenario:** This issue was not limited to a specific controller model or software version.
80006 85167	**Symptom:** The internal controller module that manages authentication stopped responding. Enhancements to the internal code that provide valid values to the authentication process fixed this issue in ArubaOS 6.2.1.3. **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.

Table 38 *Base OS Security Fixed Issues (Continued)*

Bug ID	Description
80805 81775 85642	**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. **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.
81458	**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. **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.
83776	**Symptom:** Atheros clients did not support multiple relay counters using WPA-TKIPencryption 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. **Scenario:** This issue was observed when Wireless Multimedia Extensions (WMM) was enabled and the atheros clients did not support multiple relay controllers.
84628 86814	**Symptom:** A 6000 controller unexpectedly rebooted. Log files for the event listed the reason for the reboot as **Datapath timeout**. This issue was fixed by validating the bridge entries for VoIP clients. **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.
85519	**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. **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, 6.2.x, and 6.3.x

Controller Platform

Table 39 *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:** Arace 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.

DHCP

Table 40 *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 41 *Local Database Fixed Issues*

Bug ID	Description
84494	**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 was 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. **Scenario:** This issue occurred on a standalone master 7210 controller with one associated AP-135 access point.

OSPF

Table 42 *OSPF Fixed Issues*

Bug ID	Description
82730	**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. **Scenario**: This issue was not limited to a specific controller model and was observed in ArubaOS 6.2.1.0.

RAP+BOAP

Table 43 *RAP+BOAP Fixed Issues*

Bug ID	Description
74024	**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. **Scenario:** This issue was observed in ArubaOS controllers, and RAP-3WN, and RAP-5 access points.
78914	**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 was fixed by removing the split-tunnel mobility that triggered the error. **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.

Table 43 *RAP+BOAP Fixed Issues (Continued)*

Bug ID	Description
84752 84391 84893 85160 85629 86217 86339 86372 86375 86738 86742	**Symptom:** Campus APs (CAPs) and Remote (RAPs) rebooted after upgrading the software to ArubaOS 6.2.1.3. Memory improvements resolve this issue. **Scenario:** This issue was triggered by to insufficient memory and was not specific to any controller or AP model.
85053	**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. **Scenario**: This issue was identified in ArubaOS 6.2.1.1, when a RADIUS server was configured on the controller.

Radius

Table 44 *Radius Fixed Issues*

Bug ID	Description
84060 85623	**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. **Scenario:** This was an intermittent issue and was not limited to a specific controller model or software version.
85277	**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 **Avg RspTm** field to correctly update, and increasing controller stability. **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.

Role/VLAN Derivation

Table 45 *Role/VLAN Derivation Fixed Issues*

Bug ID	Description
77242	**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. **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.

SNMP

Table 46 *SNMP Fixed Issues*

Bug ID	Description
77584 81499	**Symptom**: An SNMP get request to poll *sysExtCardStatus* 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 *sysExtCardStatus* to display the cached information from the previous poll status instead of an error message. **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.

Station Management

Table 47 *Station Management Fixed Issues*

Bug ID	Description
83091 83547	**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. **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.
84718 84719 84725	**Symptom:** The internal controller module that manages station authentication stopped responding and temporarily prevented clients from associating to the network. This issue was fixed by adding validations to prevent this controller module from crashing. **Scenario:** This issue was not limited to a specific controller model or release version.

Switch Datapath

Table 48 *Switch Platform 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.

Switch Platform

Table 49 *Switch Platform Fixed Issues*

Bug ID	Description
84825	**Symptom:** A 651 controller crashed or failed to respond. This issue was fixed by adding checks to deny access to invalid DRAM channels for the 651 controller. **Scenario:** This issue was observed on a 651 controller running ArubaOS 6.3, ArubaOS 6.2, and ArubaOS 6.1.3.7.

UI-Configuration

Table 50 *UI-Configuration Fixed Issues*

Bug ID	Description
77933 85051 85740	**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. **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.
83744 85222 85646	**Symptom**: Changes to the account start and end date fields did not take effect when adding a new guest user. **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.

UI-Monitoring

Table 51 *UI-Monitoring Fixed Issues*

Bug ID	Description
84387	**Symptom:** Clicking on the **Locate** button in the **Security** page for **Valid Clients** displayed the **Internal error while executing query** error. This issue was fixed by generating the correct locate query for the filter related to the client. **Scenario:** This issue was not limited to a specific controller model or release version.
85229	**Symptom**: The **Security Summary** page in the WebUI timed out as the event table in the WMS database became very large. This issue was resolved by enabling periodic clean-up of the WMS event table entries. **Scenario**: This issue was observed when too many APs where terminating on a controller. This issue was not limited to any specific controller model.
85784 76383	**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. **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.

Voice

Table 52 *Voice Fixed Issues*

Bug ID	Description
83517 84723	**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. **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 and 6.3.

Resolved Issues in ArubaOS 6.2.1.2

AP Platform

Table 53 *AP Platform Fixed Issues*

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

AP Wireless

Table 54 *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.

BaseOS Security

Table 55 *BaseOS Fixed Issues*

Bug ID	Description
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 56 *Command Line Interface Fixed Issues*

Bug ID	Description
62292	**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. **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.

Control Plane Security (CPsec)

Table 57 *Control Plane Security Fixed Issues*

Bug ID	Description
66413 67875 68010	**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. **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.

Controller Datapath

Table 58 *Controller Datapath Fixed Issues*

Bug ID	Description
80625	**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. **Scenario:** This issue was observed when tunnels were used on controllers running ArubaOS 6.1.3.x or later.
83216	**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. **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.
83409	**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. **Scenario:** This issue was observed when a huge traffic hit the control plane causing loss of acknowledgements in the communication infrastructure. This is not specific to any controller model.

Controller Platform

Table 59 *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 6.2.1.4. **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**. IThis 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 60 *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 BDPU 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.

Dot1x

Table 61 *Dot1x Fixed Issues*

Bug ID	Description
83375	**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 6.2.1.4. **Scenario**: This issue was observed in controllers running ArubaOS 6.2.1.0 and was not specific to any controller model.

Enhanced Voice-Data Optimized

Table 62 *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 63 *IPv6 Fixed Issues*

Bug ID	Description
76426 78962	**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. **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.
79452 77012	**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. **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.

Mobility

Table 64 *Mobility Fixed Issues*

Bug ID	Description
82673	**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. **Scenario:** This issue was observed when L3 mobility was enabled on controllers running ArubaOS 6.1.x.

Online Certificate Status Protocol (OCSP)

Table 65 *OCSP Fixed Issues*

Bug ID	Description
79704	**Symptom:** The process that handles the OCSP verification requests from the internal user authentication module was not responding. This issue is resolved by making the OCSP server communication asynchronous. **Scenario:** This issue was observed when OCSP server was configured as revocation check point and an incoming certificate was validated against the OCSP, with rapid similar incoming requests. This issue is not specific to any controller model.

RADIUS

Table 66 *RADIUS Fixed Issues*

Bug ID	Description
76484	**Symptom:** RADIUS authentication failed in networks that had different Maximum Transmission Values (MTUs). **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.

Voice SIP

Table 67 *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 68 *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 ArubaOS controllers running 6.1.3.4 and 6.2.x and was not specific to any controller model.
80269	**Symptom:** The GigabitEthernet interface 10 option was missing in the VRRP tracking Interface drop-down under **Advanced Services > Redundancy > Add virtual Router > Tracking Interface table** of the WebUI. ArubaOS 6.2.1.2 now includes the GigabitEthernet 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 6.2.1.4. **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

802.1X

Table 69 *802.1X Fixed Issues*

Bug ID	Description
77154	**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. **Scenario:** This issue occurred in ArubaOS 6.1.2.4, when clients authenticating with a RADIUS server roamed between APs.
80841	**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. **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.

Air Management - IDS

Table 70 *Air Management - IDS Fixed Issues*

Bug ID	Description
81073	**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. **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.

AMON

Table 71 *AMON Fixed Issues*

Bug ID	Description
81759	**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. **Scenario:** This issue was identified on ArubaOS 6.2.0.2 and not limited to any specific controller model.

AP Platform

Table 72 *AP Platform Fixed Issues*

Bug ID	Description
77236	**Symptom**: An AP-125 configured to discover its master controller using DNS failed to connect to the controller after completing 802.1X authentication. Improvements to the master discovery process resolve this issue in ArubaOS 6.2.1.1. **Scenario**: When the AP completed 802.1X authentication, the AP selected an IP address before the master was discovered. This issue occurred on APs running ArubaOS 6.1.3.2 configured to use 802.1X authentication and dynamic master discovery.

AP Regulatory

Table 73 *AP Regulatory Fixed Issues*

Bug ID	Description
79804	**Symptom:** AP-93 APs using the Panama country code operated in air-monitor mode even though the AP's 802.11a and 802.11g radio profiles were configured in AP-mode. This issue is fixed by adding support for Panama and Puerto Rico in the PR country code on an AP-93. **Scenario:** This occurred on AP-93 access points running ArubaOS 6.1.3.x and later.

AP Wireless

Table 74 *AP Wireless Fixed Issues*

Bug ID	Description
79724	**Symptom**: An AP-70 did not deliver buffered data to a Vocera B3000 communication badge when the Vocera device came out of powersave mode, preventing the device from initiating a call. The fix for this issue ensures that the AP sends out buffered data packets when it is notified that the Vocera client has come out of powersave mode. **Scenario**: This issue occurred on AP-70 APs running ArubaOS 6.1.3.6, when the client Vocera badge receiving the call roamed to another AP, and then returned to its original AP.
80334	**Symptom**: Clients intermittently disconnected after successfully connecting to the 2.4 GHz Band of an AP-125. On rare occasions, if an AP deferred scanning, ArubaOS might keep some scan flags turned on and assume the AP to be in a scanning state, preventing the AP from transmitting data frames.Changes to how the scan flags are cleared when the AP defers scanning resolves this issue in ArubaOS 6.2.1.1. **Scenario**: This issue occurred when clients connected to an Open or Secure SSID, in a topology where the client VLAN was a L2 VLAN on the controller and an uplink Cisco switch was the default gateway for the client.

ARM

Table 75 *ARM Fixed Issues*

Bug ID	Description
79204	**Symptom**: In ArubaOS 6.2.0.0-6.2.1.0, APs without clients scan non-home channels for longer periods than APs that do have associated clients. This increase in scan times for APs without clients could prevent VoWLAN phones like the Motorola EWP1000 from considering those APs as roaming candidates. This issue is resolved by changing the default scan time for APs without clients to the same scan time as APs with clients. **Scenario**: This issue occurred in ArubaOS 6.2.0.0-6.2.1.0, and is not specific to any controller model.

BaseOS Security

Table 76 *BaseOS Fixed Issues*

Bug ID	Description
76027	**Symptom**: The configured netservices **svc-papi** and **svc-sec-papi** did not appear in the output of the **show running-config** CLI command. A change to how these services are added to the controller resolves this issue. **Scenario**: This issue appeared in ArubaOS 6.2.0.0, and is not limited to any specific controller model.
79564	**Symptom:** The controller's internal user authentication process crashed when a wireless client used captive portal authentication and the client user role required reauthentication. Improvements to the reauthentication timer fixed this issue in ArubaOS 6.2.1.1. **Scenario:** This issue only occurred if the wireless client had more than one IPv4/IPv6 address. When the first IP address aged out before the reauthentication timer triggered, the process crashed. This issue was observed in controllers running ArubaOS 6.x.

Table 76 *BaseOS Fixed Issues (Continued)*

Bug ID	Description
79805	**Symptom:** An internal controller process stopped responding, causing the controller to reboot and preventing clients from authenticating. Memory buffer improvements resolve this issue in ArubaOS 6.2.1.1. **Scenario:** In rare conditions, the error handling process incorrectly released the Extensible Authentication Protocol (EAP) memory twice, causing memory corruption. This issue occurred in an M3 controller running ArubaOS 6.1.3.7 in a master-local topology where an M3 controller acted as a local controller.
80162	**Symptom:** An error in the internal authentication module on a controller caused it to stop responding. This authentication module crash occurred when another controller process mistakenly told the authentication module that a VPN user was ready before the user had completed the authentication process. A fix is added to ArubaOS 6.2.1.1 prevent this issue. **Scenario:** This issue was first identified in ArubaOS 6.2.0.2 and is not limited to any specific controller model.
80324	**Symptom**: An internal controller module stopped responding when the controller upgraded from ArubaOS 6.1.3.6 to ArubaOS 6.1.3.7, causing the controller to reboot. Improvements to how the controller checks for null Aruba certificates has resolved this issue in ArubaOS 6.2.1.1. **Scenario**: This issue occurred on a 620 controller in a master-local topology.

Control Plane Security (CPsec)

Table 77 *Control Plane Security Fixed Issues*

Bug ID	Description
78301	**Symptom:** A master controller stopped synchronizing its CPsec whitelist with local controllers due to an interruption in the synchronization process. Enhancements to how the synchronization process performs retry attempts fixes this issue in ArubaOS 6.2.1.1. **Scenario:** The CPsec whitelist synchronization failure on the master controller was caused by an interruption that could include any of the following: • loss of network connectivity • loss of minor frames • crash or reboot associated with the controller This issue was observed in ArubaOS 6.1.2.6.

Controller Platform

Table 78 *Controller Platform Fixed Issues*

Bug ID	Description
79553 77810 80328 81489	**Symptom**: An internal controller module failed to respond, causing the controller to reboot, when a Campus AP (CAP) was deployed behind a Remote AP (RAP). Improvements to the encapsulation process fixe this issue in ArubaOS 6.2.1.1. **Scenario**: This issue was triggered by packets that became corrupted after IPSEC encryption. The issue was observed in on M3 controllers running ArubaOS 6.2.0.2.
80360	**Symptom:** The 7200 Series controller experienced an internal process (datapath) crash and reboot when connected to and receiving data from an AMSDU-enabled client device. **Scenario:** AMSDU caused an internal process error that resulted in a crash and reboot of the 7200 Series controller. This issue was identified in ArubaOS 6.2.1.0 and has been fixed in this release.

Table 78 *Controller Platform Fixed Issues (Continued)*

Bug ID	Description
80419 80523	**Symptom**: A feature allowed the ArubaOS DNS server to reveal its version number. This feature has been disabled in ArubaOS 6.2.1.1 as a security precaution. **Scenario**: This issue was identified in ArubaOS 6.2.0.0.
81178	**Symptom**: When a 7220 controller upgraded to 6.2.1.0, an internal controller module stopped responding, causing the controller to reset. This issue was triggered by reserved source descriptor fields that were incorrectly defined in the POE buffer address info and the POE flow info packets. Changes that prevent these reserved fields from getting set resolve this issue in ArubaOS 6.2.1.1. **Scenario**: This issue was identified on a 7200 Series controller running ArubaOS 6.2.1.0.
81865	**Symptom:** When a loopback IP address is configured on a controller but the controller IP is set to the IP address of another VLAN interface, no entry appears for the loopback interface's IP address in the user table. A fix is introduced in ArubaOS 6.2.1.1 to create an entry in the user table if the controller IP address is different from the loopback IP address. **Scenario:** This issue was identified on ArubaOS 6.1.3.5 and is not limited to any specific controller model.

MAC-Based Authentication

Table 79 *MAC-Based Authentication Fixed Issue*

Bug ID	Description
77491	**Symptom:** The **Session-Timeout** attribute returned from the RADIUS Server during MAC authentication was not honored in reauthentications, and the client did not revert to its initial user role when MAC authentication failed. This issue has been fixed on ArubaOS 6.2.1.1 by adding session-timeout support for MAC authentication. **Scenario:** This issue was identified on a controller running ArubaOS 6.1.3.5, and not specific to any controller model.

Mesh

Table 80 *Mesh Fixed Issues*

Bug ID	Description
78805	**Symptom:** The controller process that handles AP management and user association unexpectedly stopped and restarted. This issue is fixed in ArubaOS 6.2.1.1 by blocking certain entries and events that are created when the image on an AP does not match the image on the local controller. **Scenario:** This issue was observed in M3 controllers running ArubaOS 6.1.3.6 with Mesh Portals and Points in the setup. When the image version on the AP was different from the image version stored on the controller, the initialization sequence for these APs was not accurate. This created some incomplete entries that caused a crash.

Mobility

Table 81 *Mobility Fixed Issues*

Bug ID	Description
75093	**Symptom**: The **show ip mobile host** CLI command incorrectly displayed the roaming status of a client as **No state** instead of the expected **Home Switch/Home VLAN**. Changes in the mobile IP process that free the client's host entry fixed this issue in ArubaOS 6.2.1.4. **Scenario**: This issue was observed when L3-mobility was enabled in the controller. This issue was not limited to any controllers model or version of ArubaOS.
78111	**Symptom:** Roaming clients experienced traffic interruption when L3 mobility was enabled on the controller. This issue has been fixed in ArubaOS 6.2.1.1. **Scenario:** This issue occurred because duplicate ARP responses were sent from both the home agent and foreign agent for the roaming client. This issue was observed when the controllers were upgraded from ArubaOS 5.x to 6.1.x.

Remote AP

Table 82 *Remote AP Fixed Issues*

Bug ID	Description
77450	**Symptom:** Wired clients connected to a remote AP in bridge forwarding mode were unable to get an IP address when the remote AP lost connectivity to the controller, or if any of the following fields changed in the Virtual AP or SSID: • WLAN SSID opmode • WLAN SSID profile passphrase • probe type • Physical connection (phy) type • Forwarding mode • Remote AP operation • VLAN • ESSID • Backup Virtual AP in bridge forwarding-mode with PSK enabled ArubaOS 6.2.1.1. resolves this issue with a change that prevents the uplink destination device (bond0) from being removed from the VLAN multicast table when a backup SSID is enabled and there are other wired or wireless devices present in the VLAN multicast table. **Scenario**: This issue was observed when the AP had a backup Virtual AP in the same VLAN as the wired clients, and the AP wired port profile had the **Remote-AP backup** option enabled. This issue was observed in APs running ArubaOS 6.1.x, and was not limited to any specific AP model.
78656	**Symptom**: A remote AP could not operate in L2 mode when connected to a local controller in a master-local topology or a backup controller in a redundant master topology. A change in how the source IP of the GRE tunnel is defined resolves this issue in ArubaOS 6.2.1.1. **Scenario**: This issue occurred on remote APs in L-2 mode connected to a local or backup master controller, and was not limited to any specific AP model. It was triggered because the AP did not use the **controller-ip** IP address as the source IP of the GRE tunnel, which caused the controller to respond with ICMP unreachable messages for packets sent by the AP.

Role/VLAN Derivation

Table 83 *Role/VLAN Derivation Fixed Issue*

Bug ID	Description
78322	**Symptom:** Clients connected to an AP in bridge forwarding mode derived incorrect roles when the AP was connected to a Cisco bridge VLAN. This issue has been resolved in ArubaOS 6.2.1.1, which now checks to see if the source MAC address from the L2 bridge mobility advertisement message is the AP's MAC address, then prevents the AP from deleting L2 and L3 entries if the MAC addresses are the same. **Scenario:** This issue was observed when an AP connected to a Cisco bridge VLAN received its own broadcast message over the uplink and started deleting L2 and L3 database entries. This issue is not specific to a controller model.

Spectrum-Infrastructure

Table 84 *Spectrum-Infrastructure Fixed Issue*

Bug ID	Description
79144	**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 6.3. **Scenario:** This issue occurred when spectrum monitoring was enabled in the AP's 802.11a or 802.11g radio profile.

Voice SIP

Table 85 *Voice SIP Fixed Issue*

Bug ID	Description
79717	**Symptom:** The SIP application-level gateway (ALG) did not prioritize Real-time Transport Protocol (RTP) traffic for the Jabber application. Changes to the SIP parser fix this issue in ArubaOS 6.2.1.1. **Scenario:** SIP ALG was not able to parse SDP (Session Description Protocol), which prevented the the traffic from being correctly prioritized. This issue was observed in ArubaOS 6.1.3.5.

WebUI

Table 86 *WebUI Fixed Issue*

Bug ID	Description
77548	**Symptom**: Accessing any page of the controller's WebUI generated a **Null** error message. Changes to how WebUI sessions are managed fix this issue in ArubaOS 6.2.1.4. **Scenario**: This issue occurred due to an internal error in a process that affects how commands are executed in a WebUI session. This issue is not limited to any controller model or version of ArubaOS.

Resolved Issues in ArubaOS 6.2.1.0

The following issues have been resolved in ArubaOS 6.2.1.0:

3G/4G

Table 87 *3G/4G Fixed Issue*

Bug ID	Description
77928	**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 **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.

Air Management-IDS

Table 88 *Air Management-IDS Fixed Issues*

Bug ID	Description
76936	**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. **Scenario**: This issue was first identified in ArubaOS 6.1.3.5, and was not limited to any specific controller or AP model.
76808	**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. **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.

AP Wireless

Table 89 *AP Wireless Fixed Issue*

Bug ID	Description
77946	**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. **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.

AP Platform

Table 90 *AP Platform Fixed Issues*

Bug ID	Description
76021	**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. **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.
77183	**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. **Scenario:** This issue occurred when the **RX Sensitivity Tuning Based Channel Reuse** setting in the dot11x radio profile was set to **dynamic**.
77645	**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. **Scenario**: This issue occurred on a 7200 Series controller in a master-local topology where the APs failed over between two controllers.

BaseOS Security

Table 91 *BaseOS Fixed Issue*

Bug ID	Description
75754	**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. **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.

Dot1x

Table 92 *Dot1x Fixed Issues*

Bug ID	Description
77705 78658 78559	**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. **Scenario:** This issue occurred on 7200 Series controllers running ArubaOS 6.2.0.2.
79546	**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. **Scenario:** This issue occurred on M3 controllers running ArubaOS 6.1.3.7.

IPsec

Table 93 *IPsec Fixed Issues*

Bug ID	Description
68035	**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. **Scenario:** This occurred when site-to-site VPN was enabled and a static route was added to a remote subnet with an IPsec map.
76301	**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 **Scenario:** This issue occurred on both campus APs (CAPs) and remote APs (RAPs) with IPsec tunnel to the controller.

Management Auth

Table 94 *Management Auth Fixed Issues*

Bug ID	Description
75665 75860	**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. **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.

Mesh

Table 95 *Mesh Fixed Issue*

Bug ID	Description
71371	**Symptom:** An AP-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. **Scenario:** This issue occurred in an AP-85 mesh portal associated to an M3 controller in a master-local topology.

RADIUS

Table 96 *RADIUS Fixed Issue*

Bug ID	Description
71836	**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. **Scenario:** This issue occurred when multiple users with the same MAC address tried to connect to the controller using a wired connection.

Remote AP

Table 97 *Remote AP Fixed Issue*

Bug ID	Description
72454	**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. **Scenario:** This issue was identified on RAPs with a UML290 modem uplink running ArubaOS 6.1.3.3.

Spectrum-Infrastructure

Table 98 *Spectrum-Infrastructure Fixed Issue*

Bug ID	Description
79144	**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. **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.

Station Management

Table 99 *Station Management Fixed Issues*

Bug ID	Description
74455	**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. **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.

Switch-Platform

Table 100 *Switch-Platform Fixed Issues*

Bug ID	Description
62096	**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. **Scenario:** This issue was observed on an M3 controller when there was high traffic between the control plane and the datapath.
75232	**Symptom:** An internal system error occurred in the M3 controller and APs failed to connect to the controller. **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.

Table 100 *Switch-Platform Fixed Issues (Continued)*

Bug ID	Description
75411	**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. **Scenario:** This is an infrequent occurrence on these controllers.
76852	**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. **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.
79385	**Symptom**: A RAP-5WN associated to a 3200 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. **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.

Switch-Datapath

Table 101 *Switch-Datapath Fixed Issues*

Bug ID	Description
75843 72359 73246 73256 74575 75700 75753	**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. **Scenario:** This issue occurred when an M3 controller experienced heavy traffic between the control plane module and the network.
77535 77537 77024	**Symptom:** Android, iOS, and MacOS 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. **Scenario:** The iOS, MacOS, 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.
76307	**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. **Scenario:** When a user added a VLAN ID to the master controller and executed the command `write-mem`, the local controller crashed due to an internal process failure. This issue was not specific to any controller or software version.
77484 78181 78667 78873 79682	**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. **Scenario:** This occurred on 7200 Series controllers running ArubaOS 6.2.0.x.
77814	**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 **Scenario:** This issue occurred on M3 or 3000 Series controllers in a master-local topology running ArubaOS 6.1.x.

Table 101 *Switch-Datapath Fixed Issues (Continued)*

Bug ID	Description
78326	**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. **Scenario**: This issue was triggered when a controller that receives GRE-type PPP packets has a user role that enables source NAT.
78593 79897	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 coredumps resolves this issue. Scenario: This issue was observed in a 7200 Series controller in a master-local topology.

UI Configuration

Table 102 *UI Configuration Fixed Issue*

Bug ID	Description
76348	**Symptom:** When an AP provisioned with a Fully Qualified Domain Name FQLN parameter using the format *<floor>.<bulding>.<campus>* 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. **Scenario:** This issue occurred on APs provisioned with the FQLN parameter, and was not limited to any specific controller or AP model.

WebUI

Table 103 *WebUI Fixed Issues*

Bug ID	Description
74227	**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. **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.
76335	**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. **Scenario:** This issue occurred on controllers running ArubaOS 6.2.0.x, and was not limited to a specific controller model.

This chapter describes the known issues and limitations identified.

Maximum DHCP Lease Per Platform

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

Table 104 *Maximum DHCP Lease Per Platform*

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

Known Issues

802.1X

Table 105 *802.1X 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.)

AP Wireless

Table 106 *AP Wireless Known Issues*

Bug ID	Description
75564	**Symptom**: An internal process in an AP-135 running ArubaOS 6.1.3.3 restarts, causing that AP to unexpectedly reboot. **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. **Workaround**: Set the **Monitored Device Stats Update Interval** in the IDS General profile to 0, its default value.
84329	**Symptom**: AP-175 access points experienced significant ping losses, causing clients to disconnect. **Scenario**: This issue occurred on AP-175 associated to a standalone 6000 controller running ArubaOS 6.2.1.0. **Workaround**: None.

AP Platform

Table 107 *AP Platform Known Issues*

Bug ID	Description
58011 61100 60846 64517 66118 66128 66185 66596 64526 61539 61196 67435 67670 67671 67673 67871 67872 68875 68937 72069 74142 75366 75539 75703 75366	**Symptom**: A 651 controller reboots unexpectedly after enabling the internal AP. **Scenario**: This issue is observed in 651 controllers running ArubaOS 5.0 or later. The internal AP is disabled when a 651 controller upgrades to ArubaOS 6.2.1.x. **Workaround**: None.

Authentication

Table 108 *Authentication Known Issues*

Bug ID	Description
55867	**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). **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. **Workaround:** Remove the VLAN from the 802.1X authenticated role and machine authentication.

Base OS Security

Table 109 *Base OS Security Known Issues*

Bug ID	Description
55419	**Symptom**: An internal ArubaOS process (Certmgr) becomes busy when the OCSP server is unreachable. **Scenario**: Users are unable to authenticate because this process is busy queuing the OCSP requests. (Clients using 802.1X, IKE, and management authentication can be affected). This issue is observed in ArubaOS 6.2. **Workaround**: None
75565	**Symptom**: A wired user is incorrectly assigned to an initial user role instead of a user role derived from DHCP fingerprinting. **Scenario**: This issue is observed in ArubaOS 6.1.3.4, and is not specific to any controller platform. **Workaround**: Delete the user from the user table, and verify that the corresponding bridge entry is removed from the datapath before reconnecting the user.
76291	**Symptom:** An internal controller process (resolvewrap) stops responding at random intervals when a RADIUS authentication server is configured with a host name. **Scenario:** This crash does not have any impact on the ArubaOS operation as the resolvewrap 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. **Workaround:** If this crash is observed continually, use an IP address is used instead of a host name in the server authentication profile.
76424	**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. **Scenario:** This issue occurred on a 7200 Series controller running ArubaOS 6.2. **Workaround:** Delete fewer users at a time.
79467	**Symptom:** User table entries for users that disconnect from the network are not correctly aging out and getting removed from the controller user table. **Scenario**: This issue was observed on a 7240 local controller running ArubaOS 6.2.0.2 in a master/local topology. **Workaround**: None.

Table 109 *Base OS Security Known Issues (Continued)*

Bug ID	Description
81243	**Symptom**: When an AP boots up, the controller log files display the message *AP-Group is not present in the RADIUS server for username=<mac address>; AP will take the ap-group as provisioned in the AP.* **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. **Workaround**: No workaround is needed since this error message does not indicate a functionality issue.
82540	**Symptom**: The internal controller module that manages handles user authentication stopped responding, preventing users from authenticating until the process automatically restarted. **Scenario**: This issue occurred on a M3 controller module running ArubaOS 6.2.0.2 in a master-local topology. **Workaround**: None

Controller-Platform

Table 110 *Controller-Platform Known Issues*

Bug ID	Description
69277	**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. **Scenario:** This issue is seen in ArubaOS 6.1.3.2. **Workaround:** None.
74428	**Symptom:** On the dual-personality RJ45 ports 0/0/0 and 0/0/1, if the port speed is forced from/to 1Gbps to/from 10/100Mbps when traffic is flowing, traffic forwarding on the port can stop in an unintended manner. **Scenario:** This issue has been observed in controller models 7210, 7200 and 7240 running ArubaOS 6.2 in configurations or topologies where traffic is flowing. The trigger is unknown. **Workaround:** Change the speed on the port following these steps: 1. Shut the port. 2. Change the speed on the port. 3. Open the port.
76220	**Symptom:** A controller crashes due to a virtual AP configuration change. **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. **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.
84597	**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. **Scenario**: This issue is not limited to any specific controller model or software version, and can occur in networks. controllers are using VRRP redundancy, there is a firewall between the controllers and the campus AP, and the campus AP terminates at the VRRP IP **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.

IPsec

Table 111 *IPsec Known Issues*

Bug ID	Description
75891	**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. **Scenario:** This occurs on controllers running ArubaOS 6.2 or later, 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. **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.

IPv6

Table 112 *IPv6 Known Issues*

Bug ID	Description
74367	**Symptom**: Clients using temporary IPv6 addresses are not be able to communicate as traffic is getting dropped. **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. **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. • Avoid the usage of temporary IPv6 addresses.

Management Auth

Table 113 *Management Auth Known Issues*

Bug ID	Description
81517	**Symptom**: The controller log files are being flooded with the error *Datapath-UserRem(IPv4/L2) failed: mac=<controller-mac-addr>*. **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. **Workaround**: None

Master-Redundancy

Table 114 *Master-Redundancy Known Issues*

Bug ID	Description
70343	**Symptom**: Custom captive portal pages are not synced between a master and standby controller when set up to do so. **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.

Table 114 *Master-Redundancy Known Issues (Continued)*

Bug ID	Description
75367	**Symptom**: Enabling web-server debug logging using the CLI command l**ogging level debugging system subcat webserver** does not take effect until you restart the HTTPD process. **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. **Workaround**: Restart the HTTPD process in order to enable debug logging.

Mobility

Table 115 *Mobility Known Issues*

Bug ID	Description
58883 60328	**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. **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 6.2.1.4 or earlier. **Workaround:** Do not issue the **router enable** command along with the **ipv6 enable** command in the controller.
63163	**Symptom:** There is an increase in datapath CPU utilization in the controller. **Scenario:** This issue occurs in a Layer-3 IP mobility enabled network, where a wired 802.1X client is connected to an untrusted port and the IP address of the client changes rapidly. The Layer-3 IP mobility edits the bridge table entries for such clients. This results in an increased CPU utilization. This issue is found in controllers running ArubaOS 6.2 or earlier. **Workaround:** Do not change the IP address of the wired client at a rapid rate.

Remote AP

Table 116 *Remote AP Known Issues*

Bug ID	Description
79799	**Symptom**: A remote AP (RAP) failed to come up using a 3G uplink or failover to a 3G uplink when the signal strength of the 4G network was significantly lower than the 3G signal, or when only a 3G signal was available. **Scenario**: This issue was identified on a RAP-5WN AP connected to a 3200 controller and provisioned with both 4G and 3G parameters. **Workaround**: Rebootstrap the RAP to restore the 3G network connection.
81245	**Symptom**: The user table contains stale entries for users that aged out or disassociated from the network. **Scenario**: This issue occurs when users associated to a AP in split-tunnel forwarding mode and using captive portal authentication roam to multiple APs exhibiting the same ESSID. **Workaround**: Periodically delete the stale entries from the user table.
83002	**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. **Scenario**: This issue occurred when the controller upgraded to ArubaOS 6.2. **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.

Table 116 *Remote AP Known Issues (Continued)*

Bug ID	Description
84004	**Symptom**: In some instances calls from IP phones connected to a RAP-3WN AP fail because the AP drops packets. **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. **Workaround**: None.
87105	**Symptom**: Printers connected to the wired port of a remote AP (RAP) in tunnel mode intermittently fall into the wrong VLAN. **Scenario**: This issue occurs on a remote AP running 6.2.1.2, when configuration settings are not properly cleared on a remote AP that resets its connection to the controller. As a result, the RAP's ethernet interface is brought up in bridge mode first, then changed to tunnel mode. This causes a configuration conflict between the controller and the RAP, as the controller manages the RAP as a remote bridge user, and the RAP operates as a user in tunnel mode.

Startup Wizard

Table 117 *Startup Wizard Known Issues*

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

Station Management

Table 118 *Station Management Known Issues*

Bug ID	Description
72194	**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. **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. **Workaround:** Disable VLAN mobility and the preserve VLAN feature.

Table 118 *Station Management Known Issues (Continued)*

Bug ID	Description
82012	**Symptom**: An internal controller process kept restarting, preventing the controller from servicing clients. **Scenario**: This issue was identified when the controller upgraded its image, and was triggered when the controller expected IKEv2 information that was missing from the mysql global AP database. **Workaround**: none.

WebUI

Table 119 *WebUI Known Issues*

Bug ID	Description
55981	**Symptom:** When a user views the Spectrum UI with saved preferences from a newer version of ArubaOS, the UI will display charts incorrectly. **Scenario:** After downgrading from a newer version of ArubaOS, such as from 6.2.x to 6.1.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 and previous versions. **Workaround:** Use the command **ap spectrum clear-webui-view-settings** on the controller to delete the saved preferences.
66521	**Symptom:** Two **Apply** buttons are displayed in the WebUI when adding users to the internal database. **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. **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.
75836	**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**. **Scenario:** This issue occurs on controllers running ArubaOS 6.2 or later. 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. **Workaround:** None.
75857	**Symptom:** An incorrect label is displayed on the **WLAN Details** page when the WLAN hyperlink is selected from the **Client** page. **Scenario:** This issue occurs on controllers running ArubaOS 6.2 or later, when WLAN detail page is navigated from Client page, Client filter gets applied instead of the WLAN filter. **Workaround:** None.
76836	**Symptom:** A Javascript error occurs when trying to view the trend on the **WLAN Summary** page. **Scenario:** This issue occurs on controllers running ArubaOS 6.2 or later, 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. **Workaround:** None.
77274	**Symptom:** An error occurs when creating an access control list using the WebUI when the **invert** option is enabled in **netdestination**. **Scenario:** This issue occurs on controllers running ArubaOS 6.2, where an error occurs while creating the acls with netdestination created with invert option. **Workaround:** None.

Table 119 *WebUI Known Issues (Continued)*

Bug ID	Description
77542	**Symptom:** The 600 Series controller is unable to upgrade from a local file. **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, 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. **Workaround:** None. Use the USB, TFTP, SCP, or CLI option to upgrade instead.
79146	**Symptom:** The SSID does not display properly if the SSID name contains special characters. **Scenario:** This issue occurs on controllers running ArubaOS 6.2 or later, when the cursor is placed on the WLAN. **Workaround:** Do not configure an SSID name with special characters.
80233 82724	**Symptom**: The **Monitoring>Access Points** and **Monitoring>Network>All Access Points** pages of the controller WebUI show APs as down, even they are shown as up in the command-line interface. **Scenario**: This issue occurred on a master/local topology with one 6000 master controller and two local controller running ArubaOS 6.2.1.0. **Workaround**: none
80260	**Symptom:** Users cannot add use the WebUI to add a netdestination to a whitelist or blacklist in the **Captive Portal** profile. **Scenario:** This issue occurs on controllers running ArubaOS 6.2, 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. **Workaround:** None.
82611	**Symptom**: The **Dashboard>Access Points** WebUI page of a controller running ArubaOS 6.2.0.3 does not correctly display AP information. **Scenario**: Accessing the **Dashboard>Access Points** page can trigger the following error in the controller log files: "*An internal system error has occurred at file mon_mgr.c function mon_mgr_proc_trend_query line 4142 error PAPI_Send failed: Cannot allocate memory.*" This issue is not related to a memory allocation error. **Workaround**: None
82502	**Symptom**: A controller does not correctly display the **Monitoring>Network Summary** WebUI page. **Scenario**: This issue was observed on a 3600 standalone master controller running ArubaOS 6.2.1.0. **Workaround**: None.

WMM

Table 120 *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 or lower in Tunnel and D-Tunnel modes. **Workaround**: None.

Issues Under Investigation

The following issues have been reported in ArubaOS but not confirmed. The issues have not been able to be reproduced and the root cause has not been isolated. They are included here because they have been reported to Aruba and are being investigated. In the tables below, similar issues are grouped together.

Controller-Datapath

Table 121 *Controller Datapath Issues Under Investigation*

Bug ID	Description
84105	**Symptom**: A local controller is unable to send packets. The controller log files include a warning message stating that **Configured Session limit reached for client**.

Chapter 6

Upgrade Procedures

This chapter details software upgrade procedures. Aruba best practices recommend 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

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

- Beginning with ArubaOS 6.2, 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, 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. 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 is supported only on the newer MIPS controllers (7200 Series, M3, 3400, 3600, 600 Series, 3200XM, and any 3200 controller with its memory upgraded using 3200-MEM-UG kit).

  Legacy PPC controllers (200, 800, 2400, SC1 and SC2) and 3200 (default memory) are *not* supported. DO NOT upgrade to 6.2.x if your deployments contain a mix of MIPS and PPC controllers in a master-local setup.

  When upgrading the software in a multi-controller network (one that uses two or more Aruba 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 65).
- Upon upgrade to ArubaOS 6.2, the internal AP of the 651 controller will be disabled. The controller will then operate as a 650 controller.
- 3200XM controllers with 1GB of memory can be upgraded to ArubaOS 6.2. The 3200 controller with 512MB of memory is not supported by ArubaOS 6.2.

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 then 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 ArubaOS 6.2.1.4, 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 63 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 63 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 63 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 63.

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 ArubaOS 6.2.1.4:

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

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. For details, see Memory Requirements on page 63

600 Series controllers running ArubaOS 6.2 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 ArubaOS 6.2.1.4.

- 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.

Follow step 2–step 11 of the procedure described in Upgrading From a Recent version of ArubaOS on page 65 to install the interim version of ArubaOS, then repeat step 1–step 11 of the procedure to download and install ArubaOS 6.2.1.4.

Upgrading From a Recent version of ArubaOS

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

- ArubaOS 6.2.0.x
- ArubaOS 6.1.x
- ArubaOS 6.0.1.x

- ArubaOS 6.0.2.x
- ArubaOS 5.0.3.1 or later 5.0.x releases (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 66 before proceeding further.)
- ArubaOS 3.4.4.1 or later 3.4.x releases.

Install the ArubaOS 6.2.1.4 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 ArubaOS 6.2.1.4 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 63 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 66. 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 ArubaOS 6.2.1.4 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. For details, see Memory Requirements on page 63

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.

Follow step 2 –step 7 of the procedure described in Upgrading From a Recent version of ArubaOS on page 67 to install the interim 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 6.2.0.x
- ArubaOS 6.1.x
- ArubaOS 6.0.1.x
- ArubaOS 6.0.2.x
- ArubaOS 5.0.3.1 or later 5.0.x releases (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 66 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 ArubaOS 6.2.1.4 from the customer support site.
2. Open a Secure Shell session (SSH) on your master (and local) controller(s).
   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>
   ```

3. 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
```

4. 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>
```

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

```
(hostname)# show image version


---------------------------------
Partition               : 0:1 (/dev/ha1) **Default boot**
Software Version        : ArubaOS 6.2.1.4 (Digitally Signed - Production Build)
Build number            : 39657
Label                   : 39657
Built on                : Wed Sept 18 00:03:14 PDT 2013
---------------------------------
Partition               : 0:1 (/dev/ha1)
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
```

6. Reboot the controller:

```
(hostname)# reload
```

7. 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 63 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 ArubaOS 6.2.1.4 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 ArubaOS 6.2.1.4 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 63.
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 ArubaOS 6.2.1.4 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 ArubaOS 6.2.1.4, the changes do not appear in RF Plan in the downgraded ArubaOS version.
- If you installed any certificates while running ArubaOS 6.2.1.4, 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).

   In the following example, partition 0, the backup system partition, contains the backup release 6.1.3.2. Partition 1, the default boot partition, contains the ArubaOS 6.2.1.4 image:

   ```
   #show image version
   ```

```
----------------------------------
Partition               : 0:1 (/dev/ha1)
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
----------------------------------
Partition               : 0:1 (/dev/hda2) **Default boot**
Software Version        : ArubaOS 6.2.1.4 (Digitally Signed - Production Build)
Build number            : 39657
Label                   : 39657
Built on                : Wed Sept 18 19 00:03:14 PDT 2013
```

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.

NOTE

For information about migrating to the 7200 Series Controller, visit 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. 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

NOTE

Beginning in ArubaOS 6.2, the 651 controller's internal AP is disabled. Additionally, upon upgrade, the 651 will appear as a 650-1 and the 651-8 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, it is recommended that you read the Upgrade Procedures on page 61.

If you are migrating from controllers that do not support ArubaOS 6.2, it is recommended that you upgrade to the latest supported build of your current version of ArubaOS before beginning the migration process.

Table 122 provides a brief overview of the steps required to upgrade to ArubaOS 6.2. For more detailed information and procedures on upgrading, see Upgrade Procedures on page 61.

Table 122 *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

Table 122 *ArubaOS 6.2 Upgrade Path Overview (Continued)*

Version	Step 1	Step 2
6.0.0.x	Upgrade to the latest 6.0.2.x	Upgrade to 6.2
6.2.0.x 6.1.x 6.0.1.x 6.0.2.x 5.0.3.1 (or later 5.0.3.x) 5.0.4.x 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 login.
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 document, visit 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. See Upgrade Procedures on page 61.

Installing Backed Up Controller Data

CAUTION

The 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.

CAUTION

Do not reboot your controller before installing licenses.

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
```

CAUTION

Do not reboot your controller before installing licenses.

NOTE

Do not modify your configuration before reloading the controller.

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.

The following commands are affected by this new port numbering scheme and must be considered when reconfiguring your ports:

After restoring the flash and rebooting, all inherited port configuration will be lost. This can include, but is not limited to, trusted settings, port channel, port monitoring, and so on.

```
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 expected.
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 74.