

# ArubaOS 6.2



Release Notes

## Copyright

© 2012 Aruba Networks, Inc. Aruba Networks trademarks include  Airwave, Aruba Networks®, Aruba Wireless Networks®, the registered Aruba the Mobile Edge Company logo, Aruba Mobility Management System®, Mobile Edge Architecture®, People Move. Networks Must Follow®, RFProtect®, Green Island®. All rights reserved. All other trademarks are the property of their respective owners.

## Open Source Code

Certain Aruba products include Open Source software code developed by third parties, including software code subject to the GNU General Public License (GPL), GNU Lesser General Public License (LGPL), or other Open Source Licenses. The Open Source code used can be found at this site:

[http://www.arubanetworks.com/open\\_source](http://www.arubanetworks.com/open_source)

## Legal Notice

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

## Warranty

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

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



[www.arubanetworks.com](http://www.arubanetworks.com)

1344 Crossman Avenue  
Sunnyvale, California 94089

Phone: 408.227.4500  
Fax 408.227.4550

<b>Chapter 1</b>	<b>Release Overview .....</b>	<b>7</b>
	Chapter Overview .....	7
	Release Mapping .....	7
	Supported Browsers.....	8
	Contacting Support .....	8
<b>Chapter 1</b>	<b>What's New in this Release .....</b>	<b>9</b>
	Upgrading the New Software Image Scheme .....	9
	Hardware Platforms.....	9
	7200 Series Controller.....	9
	RAP-108 and RAP-109 Remote Access Points.....	10
	RAP-3WN and RAP-3WNP Remote Access Points.....	10
	Remote Nodes Feature .....	10
	LLDP .....	10
	Spectrum Analysis.....	10
	Improved Visibility in the 5 GHz Radio Band .....	10
	Spectrum Analysis RFPlayback Tool .....	11
	Increased AP Support for Spectrum Analysis.....	11
	Platform .....	12
	Controller Capacity Alerts .....	12
	Threshold Descriptions.....	12
	ARM Scanning Enhancements .....	13
	Timestamps in CLI Output .....	13
	Support for New Version of ETSI DFS standard .....	13
	Enabling FCC DFS channels.....	13
	Regulatory adjustments .....	13
	Support for Single-Chain Mode .....	13
	L2/L3 VLAN Scalability Requirements .....	15
	Enhancement to WMM-DSCP Mapping .....	15
	Configurable WMM AC Mapping .....	15
	New Wizard Enhancements .....	16
	Controller Wizard .....	16
	Campus Wizard.....	16
	WebUI Profile Usability Enhancements.....	16
	Policy Enforcement Firewall (PEF) Visibility .....	17
	Security.....	17
	Enabling Bandwidth Contract Support for RAPs.....	17
	Applying Contracts .....	17
	DHCP Exhaustion Prevention .....	18
	RAP Servicability Enhancements.....	18
	Captive Portal Enhancements.....	18
	Inter-Controller IP Mobility Support on L2-GRE Tunnel.....	19
	RAP 3G/4G Backhaul Link Quality Monitoring.....	19
	New MIB Enhancements .....	19
	LLDP MIBs .....	19
	RAP Instrumentation for Airwave Monitoring.....	19

Aruba Products sysObject IDs.....	20
User Idle Timeout Behavior Change.....	20
Changes to Hardware Support.....	21
651 Controller .....	21
3200 Controller .....	21
Upgrade Caveats.....	21
Resolved Issues in ArubaOS 6.2 .....	22
AP Datapath .....	22
AP Platform .....	22
AP Regulatory .....	22
AP Wireless .....	23
Air Management.....	24
Authentication .....	25
Base OS Security .....	25
Captive Portal.....	27
Configuration.....	27
Controller-Platform.....	27
DataPath/Platform.....	28
Dot1x.....	28
DPA .....	28
Dynamic Authorization .....	29
IPsec .....	29
Mesh .....	29
RAP .....	29
Remote Access Point.....	30
Roles/VLAN Derivation.....	30
Station Management.....	30
STP.....	31
UI-Configuration.....	31
UI-Monitoring .....	31
Voice .....	31
WebUI .....	32
WMM.....	32
Known Issues and Limitations in ArubaOS 6.2 .....	32
AP Wireless .....	33
AP Platform .....	33
Air Management.....	34
Authentication .....	34
Base OS Security .....	34
Controller Platform .....	36
Dot1x.....	36
IPSec.....	37
IPv6 .....	37
Local Database .....	38
Management Auth.....	39
MAC-Based Authentication .....	39
Mobility.....	39
RAP .....	40
Roles/VLAN Derivation.....	40
SNMP .....	40
Station Management.....	41
VIA.....	41
WebUI .....	41
WMM.....	42
Issues Under Investigation .....	42
AP .....	42
Base OS Security .....	43

	Controller-Datapath .....	43
	Dot1x.....	44
	Mesh .....	44
<b>Chapter 2</b>	<b>Known Issues.....</b>	<b>45</b>
	Phonehome SMTP.....	45
	Supported Browsers.....	45
	Maximum DHCP Lease Per Platform .....	45
	Known Issues .....	46
	Controller-Datapath .....	46
	Remote Access Point.....	46
	Security .....	46
	Syslog .....	46
<b>Chapter 3</b>	<b>Upgrade Procedures .....</b>	<b>47</b>
	Upgrade Caveats.....	47
	Important Points to Remember and Best Practices.....	47
	Memory Requirements .....	48
	Backing up Critical Data.....	49
	Back Up and Restore Compact Flash in the WebUI .....	50
	Back Up and Restore Compact Flash in the CLI .....	50
	Upgrading in a Multi-Controller Network.....	51
	Upgrading to 6.2.x.....	51
	Install using the WebUI .....	51
	Upgrading From an Older version of ArubaOS .....	51
	Upgrading From a Recent version of ArubaOS.....	51
	Upgrading With RAP-5 and RAP-5WN APs .....	52
	Install using the CLI .....	53
	Upgrading From an Older version of ArubaOS .....	53
	Upgrading From a Recent version of ArubaOS.....	53
	Downgrading .....	55
	Before you Begin.....	55
	Downgrading using the WebUI.....	56
	Downgrading using the CLI .....	56
	Before You Call Technical Support .....	57
<b>Chapter 4</b>	<b>7200 Series Migration.....</b>	<b>59</b>
	Migrating to the 7200 Series Controller.....	59
	Important Points to Remember.....	59
	Backing Up Your Data Before Upgrading to 6.2.....	60
	Back Up the Flash File System in the WebUI.....	60
	Back Up the Flash File System in the CLI .....	60
	Upgrading Your Network .....	60
	Backing Up Your Data After Upgrading to 6.2.....	61
	Transferring Licenses.....	61
	Installing Your New Controller .....	61
	Installing Backed Up Controller Data.....	62
	Restore the Flash File System in the WebUI .....	62
	Restore the Flash File System in the CLI.....	62
	Applying Licenses .....	62
	Applying the Software License Key in the WebUI .....	62
	Applying the Software License Key in the License Wizard .....	63
	Backing Up Licenses in the WebUI .....	63
	Backing Up Licenses in the CLI .....	63

Reload Your Controller.....	63
Establishing Network Connectivity .....	63
Connecting to the Controller .....	64
Verifying Controller Operation.....	64
Verifying Migration in the WebUI .....	64
Verifying Migration in the CLI .....	64

ArubaOS 6.2 is a major software release that introduces new features and fixes to many previously outstanding 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*.



See the “Upgrade Procedures” on page 47 for instructions on how to upgrade your controller to this release.

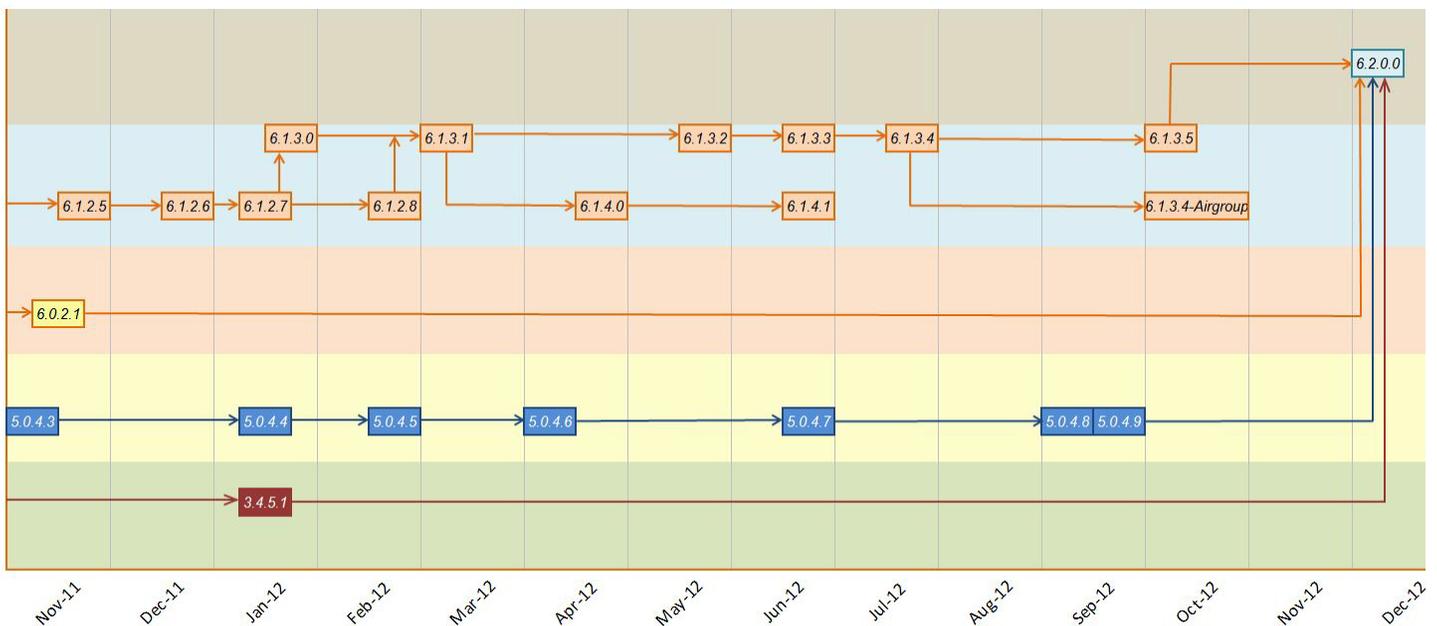
### Chapter Overview

- Chapter 1, “What’s New in this Release” on page 9 describes the new features introduced in this release.
- Chapter 2, “Known Issues” on page 45 provides descriptions and workarounds for outstanding issues in ArubaOS 6.2.
- Chapter 3, “Upgrade Procedures” on page 47 cover the procedures for upgrading your controller from any release of ArubaOS to ArubaOS 6.2.
- Chapter 4, “7200 Series Migration” on page 59 provides instructions for migrating your existing controllers to the new 7200 Series controller. For additional information, see [support.arubanetworks.com](http://support.arubanetworks.com).

### Release Mapping

The following illustration shows which patches and maintenance releases are included in their entirety in ArubaOS 6.2.

**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 above on Windows XP, Windows Vista, Windows 7, and MacOS
- Mozilla Firefox 3.x and above on Windows XP, Windows Vista, Windows 7, and MacOS
- Apple Safari 5.x and above on MacOS

## Contacting Support

**Table 1** *Web Sites and Emails*

Web Site	
• Main Site	<a href="http://www.arubanetworks.com">http://www.arubanetworks.com</a>
• Support Site	<a href="https://support.arubanetworks.com">https://support.arubanetworks.com</a>
• Software Licensing Site	<a href="https://licensing.arubanetworks.com/login.php">https://licensing.arubanetworks.com/login.php</a>
• Wireless Security Incident Response Team (WSIRT)	<a href="http://www.arubanetworks.com/support/wsirt.php">http://www.arubanetworks.com/support/wsirt.php</a>
Support Emails	
Americas and APAC	<a href="mailto:support@arubanetworks.com">support@arubanetworks.com</a>
EMEA	<a href="mailto:emea_support@arubanetworks.com">emea_support@arubanetworks.com</a>
WSIRT Email Please email details of any security problem found in an Aruba product.	<a href="mailto:wsirt@arubanetworks.com">wsirt@arubanetworks.com</a>

**Table 2** *Contact Phone Numbers*

Telephone Numbers	
• Aruba Corporate	+1 (408) 227-4500
• FAX	+1 (408) 227-4550
Support	
United States	800-WI-FI-LAN (800-943-4526)
Universal Free Phone Service Number (UIFN): Australia, Canada, China, France, Germany, Hong Kong, Ireland, Israel, Japan, Korea, Singapore, South Africa, Taiwan, and the UK	+800-4WIFI-LAN (+800-49434-526)
All other countries	+1 (408) 754-1200

The ArubaOS 6.2 release includes the following new features:

## Upgrading the New Software Image Scheme



CAUTION

Upgrading from ArubaOS 3.3.x, 3.4x, 5.0.x or 6.0.x to ArubaOS 6.2 requires an “upgrade hop”. Refer to [Table 4](#) for more information. Carefully follow the upgrade steps in “Upgrade Procedures” on page 47.

[Table 4](#) provides a brief overview of the steps required to upgrade to ArubaOS 6.2.

**Table 4** ArubaOS 6.2 Upgrade Path Overview

Version	Step 1	Step 2
3.4.x	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
5.0.3.x	Upgrade to the latest 5.0.4.x	Upgrade to 6.2
6.0.x	Upgrade to the latest 6.0.2.x	Upgrade to 6.2
6.1.x	Upgrade to 6.1.3.5	Upgrade to 6.2

## Hardware Platforms

### 7200 Series Controller



NOTE

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

The 7200 series controllers deliver a wide range of network services to large campus networks. The 7200 series supports up to 32,000 users and performs stateful firewall policy enforcement at speeds up to 40 Gbps. The 7200 series includes three models that provide varying levels of functionality.

**Table 5** Aruba 7200 Controller

Model	APs Supported	Supported Users
7210	512	16,000
7220	1024	24,000
7240	2048	32,000

## RAP-108 and RAP-109 Remote Access Points

The Aruba RAP-108 and RAP-109 are dual-radio, dual-band remote access points that support the IEEE 802.11n standard for high-performance WLAN.

The RAP-108/RAP-109 ships with Aruba Instant software. Therefore, out of the box, the RAP-108/RAP-109 will operate as a Virtual Controller (VC) or an Instant AP. However, the RAP-108/RAP-109 can be converted to operate as a Remote AP (RAP).

## RAP-3WN and RAP-3WNP Remote Access Points

This release of ArubaOS introduces support for RAP-3WN and RAP-3WNP access points (APs). The Aruba RAP-3WN and RAP-3WNP are single-radio, single-band wireless APs that support the IEEE 802.11n standard for high-performance WLAN.

The RAP-3WN and RAP-3WNP ship with Aruba Instant software. Therefore, out of the box, the RAP-3WN and RAP-3WNP will operate as a Virtual Controller (VC) or an Instant AP. However, the RAP-3WN and RAP-3WNP can be converted to operate as a Remote AP (RAP).

## Remote Nodes Feature

The Remote Nodes feature is not supported in this release.

## LLDP



---

See the “[LLDP MIBs](#)” on [page 19](#) for MIB information specific to LLDP.

---

Link Layer Discovery Protocol (LLDP), is a Layer-2 protocol that allows network devices to advertise their identity and capabilities on a LAN. Wired interfaces on Aruba APs support LLDP by periodically transmitting LLDP Protocol Data Units (PDUs) comprised of selected type-length-value (TLV) elements. For more information on the LLDP feature, refer to the Voice and Video section of the ArubaOS 6.2 User Guide.

## Spectrum Analysis

### Improved Visibility in the 5 GHz Radio Band

Spectrum monitor radios can now monitor the entire 5 GHz radio band at once, allowing you to view spectrum data for the upper, middle, or lower portions of the 5 GHz band using a single radio. In previous releases, a spectrum monitor radio could monitor just one portion of the 5GHz radio band at any time.

The following spectrum analysis charts now include a **Band** configuration option that allows you to change the portion of the 5GHz band you want to display for 5 GHz Spectrum Monitor radio.

- Active Devices
- Channel Metrics
- Device Duty Cycle
- Devices vs. Channel
- FFT Duty Cycle
- Interference Power
- Quality Spectrogram

- Real-Time FFT
- Swept Spectrogram

For more information on Spectrum Analysis, including the instructions to change these charts to display a different portion of the 5GHz radio band, refer to the Spectrum Analysis section of the ArubaOS 6.2 User Guide.

## Spectrum Analysis RFPlayback Tool

Starting with ArubaOS 6.2, there are two ways to play back a spectrum recording. You can use the playback feature in the spectrum dashboard, or view recordings using the new Aruba RFPlayback tool available for download from the Aruba web site. The Aruba RFPlayback tool can play spectrum recordings created in this and earlier versions of ArubaOS. Aruba uses the Adobe AIR application to display spectrum recording information.

Follow the steps below to download and install the free Adobe AIR application and the Aruba spectrum playback tool.

1. Download the Adobe Air application from <http://get.adobe.com/air/> and install it on the client on which you want to play spectrum recordings.
2. Next, download the spectrum playback installation file from the Aruba web site.
3. Open the folder containing the spectrum installation file, and double-click the spectrum.air icon to install the spectrum playback tool. You will also be prompted to select the folder in which you want to install this tool.



If you create a spectrum analysis recordings for a 5 GHz radio using ArubaOS 6.2 or later, you will be able to view data for any lower, middle, or upper portion of the 5 GHz radio band when you play back the recording. Spectrum recordings created using ArubaOS 6.1 or earlier capture data for only part of the 5Ghz band, so these older recordings can only display data for only one portion of the 5 GHz band.

Both the spectrum dashboard and the RFPlayback tool include a playback progress bar that shows what part of the recording is being displayed. If you pause a recording, you can click and drag the red slider on this progress bar to advance to or replay any part of the current record.

## Increased AP Support for Spectrum Analysis

In ArubaOS 6.2, radios on AP-104 and AP-93H devices can be configured as spectrum monitors, and AP-105 radios can be configured as either a spectrum monitor or a hybrid AP. The table below lists the AP models that support the spectrum analysis feature. Note that only radios on the AP-105 and AP-130 Series can be configured as hybrid APs.

**Table 6** Device Support for Spectrum Analysis

Device	Configurable as a Spectrum Monitor?	Configurable as a Hybrid AP?
AP-104	Yes	No
AP-105	Yes	Yes
AP-92	Yes	No
AP-93	Yes	No
AP-93H	Yes	No

**Table 6** Device Support for Spectrum Analysis (Continued)

Device	Configurable as a Spectrum Monitor?	Configurable as a Hybrid AP?
AP-120 Series	Yes	No
AP-130 Series	Yes	Yes
AP-175	Yes	No

## Platform

### Controller Capacity Alerts

The new controller capacity feature allows you to use the **Configuration>Management>Thresholds** page of the WebUI or the **threshold** CLI command to configure controller capacity thresholds which, when exceeded, will trigger alerts. The controller will send a **wlsxThresholdExceeded** SNMP trap and a syslog error message when the controller has exceeded a set percentage of the total capacity for that resource. A **wlsxThresholdCleared** SNMP trap and error message will be triggered if the resource usage drops below the threshold once again. Current threshold values and limits appear in the output of the **show threshold** and **show threshold-limits** commands.

### Threshold Descriptions

Threshold Parameter	Description
controlpath cpu	Set an alert threshold for controlpath CPU capacity. The value of this parameter is the percentage of the total controlpath CPU capacity that must be exceeded before the alert is sent. The default threshold for this parameter is 80%.
controlpath memory	Set an alert threshold for controlpath memory consumption. The value of this parameter is the percentage of the total memory capacity that must be exceeded before the alert is sent. The default threshold for this parameter is 80%.
datapath cpu	Set an alert threshold for datapath CPU capacity. The value of this parameter is the percentage of the total datapath CPU capacity that must be exceeded before the alert is sent. The default threshold for this parameter is 30%.
Total APs	The maximum number of APs that can be connected to a controller is determined by that controller's model type and installed licenses. Use this command to trigger an alert when the number of APs currently connected to the controller exceeds a specific percentage of its total AP capacity. The default threshold for this parameter is 80%.
Total local controllers	Set an alert threshold for the master controller's capacity to support remote nodes and local controllers. A master controller can support a combined total of 256 remote nodes and local controllers. The value of this parameter is the percentage of the total master controller capacity that must be exceeded before the alert is sent. The default threshold for this parameter is 80%.

Threshold Parameter	Description
Total tunnels	Set an alert threshold for the controller's tunnel capacity. The value of this parameter is the percentage of the controller's total tunnel capacity that must be exceeded before the alert is sent. The default threshold for this parameter is 80%
Total Users	Set an alert threshold for the controller's user capacity. The value of this parameter is the percentage of the total resource capacity that must be exceeded before the alert is sent. The default threshold for this parameter is 80%.

## ARM Scanning Enhancements

The default ARM scanning interval is determined by the **scan-interval** parameter in the ARM profile. Starting with ArubaOS 6.2, if the AP does not have any associated clients (or if most of its clients are inactive) the ARM feature will dynamically readjust this default scan interval, allowing the AP obtain better information about its RF neighborhood by scanning non-home channels more frequently. If an AP attempts to scan a non-home channel but is unsuccessful, the AP will make additional attempts to rescan that channel before skipping it and continuing on to other channels.

## Timestamps in CLI Output

The timestamp feature can include a timestamp in the output of each show command issued in the command-line interface, indicating the date and time the command was issued. Note that the output of show clock and show log do not include timestamps, even when this feature is enabled. To enable this feature, access the command-line interface in config mode and issue the command **clock append**.

## Support for New Version of ETSI DFS standard

With the exception of RAP-5WN and the AP-120 Series APs, all supported APs will comply with version 1.6.1 or later of the ETSI DFS standard EN301893 when the system is upgraded to ArubaOS 6.2




---

The RAP-5WN and AP-120 Series APs can be upgraded to ArubaOS 6.2, but will not become compliant with the version 1.6.1 of the standard. RAP-5WN and AP-120 Series APs already installed in a network are allowed to remain compliant with the previous version of the standard, but any new devices added to the network after 12/31/2012 must comply with the version 1.6.1 or later wherever ETSI rules apply.

---

## Enabling FCC DFS channels

ArubaOS 6.2 enables FCC DFS channels in the 5GHz band for the following APs:

- AP-92 and AP-93
- AP-93H
- AP-105
- AP-134 and AP-135

Prior to ArubaOS 6.2, FCC DFS channels were only enabled on the AP-120 Series APs.

## Regulatory adjustments

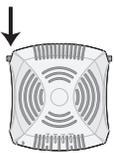
Country support and EIRP transmit power levels have been updated to reflect the latest regulatory status and test results.

## Support for Single-Chain Mode

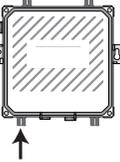
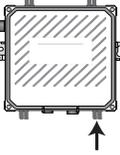
Radios on all 802.11n MIMO APs can now be configured to operate in single-chain mode, allowing those APs to transmit and receive data using only legacy rates and single-stream (SISO) HT rates up to MCS 7. This feature is disabled by default.

Table 7 below shows the antenna ports used by an AP operating in single-chain mode.

**Table 7** Antenna Interfaces for Single-Chain Mode

AP Model	Frequency Band	Antenna Port
AP-92	2.4GHz or 5GHz	ANT0 
AP-104	2.4GHz	R1/A0 
	5GHz	R0/A0 
AP-120 and AP-124	2.4Ghz	Upper Left 
	5GHz	Upper Right 
AP-134	2.4GHz or 5GHz	ANT0 

**Table 7** Antenna Interfaces for Single-Chain Mode (Continued)

AP Model	Frequency Band	Antenna Port
AP-175	2.4GHz	R1-1 
	5GHz	R0-1 

## L2/L3 VLAN Scalability Requirements

The following table displays the supported numbers of L2 VLANs, L3 VLANs and Static Routes on each of the listed controller types.

**Table 8** L2/L3 VLAN Scalability Requirements

Platform	L2 VLANs	L3 VLANs	Static Routes
620	128	128	128
650	128	128	128
3200XM	1024	512	256
3400	2048	1024	512
3600	4096	2048	1024
M3	4096	2048	2048
7200	4096	4096	2048

## Enhancement to WMM-DSCP Mapping

After you customize a WMM Access Class mapping and apply it to the SSID, the controller overwrites the default mapping values and uses the configured values. If a controller is upgraded to 6.2 from an older version, the default as well as the user configured WMM-DSCP mappings in the existing SSID profiles are retained. There are no default mappings for a newly created SSID profile and for a factory default running 6.2 image. The maximum number of values that can be configured for WMM-DSCP is 8.

## Configurable WMM AC Mapping

The IEEE 802.11e standard defines the mapping between WMM ACs and Differentiated Services Codepoint (DSCP) tags. The WMM AC mapping commands allow you to customize the mapping between WMM ACs and DSCP tags to prioritize various traffic types. You apply and configure WMM AC mappings to a WMM-enabled SSID profile

DSCP classifies packets based on network policies and rules, not priority. The configured DSCP value defines per hop behaviors (PHBs). The PHB is a 6-bit value added to the 8-bit Differentiated Services (DS) field of the IP packet header. The PHB defines the policy and service applied to a packet when traversing the network. You configure these services in accordance with your network policies. The table below shows the default WMM AC to DSCP decimal mappings and the recommended WMM AC to DSCP Hex mappings.

**Figure 2** WMM Access Category to DSCP Mappings

DSCP Decimal Value	WMM Access Category
8	Background
10	
0	Best Effort
24	
32	Video
40	
48	Voice
56	

## New Wizard Enhancements

Several new wizard enhancements were added to this release. These include:

### Controller Wizard

You can now create a VLAN by name. After creating a new VLAN name, you can configure it for VLAN IDs, IP address, enable for NAT, add port members and configure DHCP settings.

An Uplink step has been added that allows you to enable the uplink manager.

### Campus Wizard

An Uplink step has been added that allows you to enable the uplink manager.

## WebUI Profile Usability Enhancements

Starting with ArubaOS 6.2, several configuration profiles are divided into two tabs, **Basic** and **Advanced**. The **Basic** tab displays only those configuration settings that often need to be adjusted to suit a specific network. The **Advanced** tab shows all configuration settings, including settings that do not need frequent adjustment or should be kept at their default values.

The following profiles now appear in the WebUI with **Basic Settings** and **Advanced Settings** tabs.

<ul style="list-style-type: none"><li>• ap system profile</li><li>• wired ap profile</li><li>• rf 802.11a profile</li><li>• rf 802.11g profile</li><li>• rf arm profile</li><li>• high-throughput radio profile</li><li>• rf event thresholds</li><li>• rf am scanning profile</li><li>• rf ssid profile</li><li>• high-throughput SSID profile</li></ul>	<ul style="list-style-type: none"><li>• Virtual AP profile</li><li>• LLDP profile</li><li>• LLDP-MED profile</li><li>• rf 802.1x auth profile</li><li>• VIA connection profile</li><li>• voip call admission control profile</li><li>• ids unauthorized device profile</li><li>• ids impersonation profile</li><li>• mesh-ht-ssid profile</li><li>• mesh radio profile</li></ul>
---	--

## Policy Enforcement Firewall (PEF) Visibility

The Policy Enforcement Firewall (PEF) Visibility is a new PEF feature on the ArubaOS controller. It enables network administrators to monitor the applications running and the users using them in a given network.

The **Dashboard** page of the WebUI now has a new **Firewall** page. This page displays the PEF summary of all the sessions in the controller aggregated by users, devices, destinations, applications, WLANs, and roles.



---

PEF Visibility is a beta feature in ArubaOS 6.2. For troubleshooting, contact the Aruba technical support team.

---

## Security

### Enabling Bandwidth Contract Support for RAPs

This release of ArubaOS provides Bandwidth Contract support on remote APs. This is achieved by extending the Bandwidth Contract support on split-tunnel and bridge modes.

You can apply Bandwidth Contract for a RAP on a per-user or per-role basis. By default, Bandwidth Contract is applied on a per-role basis. This implies that all the users belonging to the same role will share the bandwidth pool. When Bandwidth Contract configured on the controller is attached to a user-role, it automatically gets pushed to the RAPs terminating on it.

The following show commands have been enhanced in this release to retrieve the Bandwidth Contract information from the RAP:

```
show datapath user ap-name <ap-name>
show datapath bwm ap-name <ap-name>
```

### Applying Contracts

You can apply the contract on a per-role or per-user basis. Use the following commands to apply the contracts on a per-role basis for upstream and downstream:

For upstream contract of 512 Kbps:

```
(host) (config) #user-role authenticated bw-contract 512k upstream
```

For downstream contract of 256 Kbps:

```
(host) (config) #user-role authenticated bw-contract 256k downstream
```

Use the following commands to apply the contracts on a per-user basis for upstream and downstream:

For upstream contract of 512 Kbps:

```
(host) (config) #user-role authenticated bw-contract 512k per-user upstream
```

For downstream contract of 256 Kbps:

```
(host) (config) #user-role authenticated bw-contract 256k per-user downstream
```

## DHCP Exhaustion Prevention

A new **Prevent DHCP Exhaustion** parameter in the Global Firewall settings checks DHCP client hardware address against the packet source MAC address. This feature checks the frame's source-MAC against the DHCPv4 client hardware address and drops the packet if it does not match. Enabling this feature prevents a client from submitting multiple DHCP requests with different hardware addresses, thereby preventing DHCP pool depletion.

## RAP Servicability Enhancements

- When RAP or CPSEC CAP fails to receive an IP address using DHCP from its ENET0 link, it keeps trying every 35 seconds. After 10 such retries, the RAP will reboot and start the whole process all over.
- Users with RAPs configured in either bridge mode or split-tunnel mode can use the RAP Console screen in the WebUI to troubleshoot connectivity issues. Access the RAP console using the URL: <http://rapconsole.arubanetworks.com>. This page also has a link to generate support file (Generate and save support file link). These logs contains the ap-related information to troubleshoot. As part of this, firewall commands and process/mem usage commands are added as follows:
  - Firewall commands - A snapshot of the Bridge table, acl table, session table, user table and arp table in RAP.
  - ps - reports the snapshot of the current processes.
  - dmesg - Displays the kernel debug logs.
  - ifconfig - Gives the state of the interface information.
  - meminfo - Gets the current Total Memory, Free and the Swap space of the Device.
  - SlabInfo - Kernel Slab Allocator Statistics.

## Captive Portal Enhancements

This release of ArubaOS introduces the following captive portal enhancements in tunnel and split-tunnel forwarding modes.

- When a client using captive portal authentication gets redirected to the captive portal server, the controller will send information about the AP group and name of the AP to which the client is trying to connect in the redirect URL. If the AP name is not configured, the redirect URL will contain the AP MAC address.
- A new option **redirect-url** is introduced in the Captive Portal Authentication profile which allows you to redirect the users to a specific URL after the authentication is complete.
- Captive Portal Login URL length has been increased from 256 characters to 2048 characters.
- Support for “?” (question mark) inside the Captive Portal login URL has been added.
- A new field, description has been introduced in the netdestination and netdestination6 commands to provide a description about the netdestination up to 128 characters long.
- Support for configuring Whitelist in Captive Portal has been introduced.

## Inter-Controller IP Mobility Support on L2-GRE Tunnel

In the earlier implementation of IP Mobility, visitor traffic to/from the foreign agent (FA) is tunneled back to the home agent (HA) over an IPIP tunnel. The IPIP tunnel did not carry the original L2 headers from the visitor.

This release of ArubaOS replaces the IPIP tunnel with L2 GRE tunnel for the IP mobility functionality. This preserves the L2 headers in the packets from the visitor at FA to HA. The HA then bridges the traffic from the L2 GRE tunnel to the appropriate home VLAN, provided the HA knows the home VLAN of the visitor.



---

• The L2-GRE Tunnel implementation of the IP mobility functionality is supported only on ArubaOS versions 6.2 or later and is not backward compatible with the earlier implementation.

• This release of ArubaOS supports only v4 mobility and does not support IPv6 L3 mobility.

---

## RAP 3G/4G Backhaul Link Quality Monitoring

The RAP is enhanced to support link monitoring on 2G, 3G, and 4G modems to provide information about the state of USB modem and cellular network.

The USB modem has the following four states:

- Active - The USB modem is used as the primary path for connecting VPN to the controller
- Standby or Backup - The network is available but the USB modem is not used for connecting VPN to the controller
- Error - The USB modem is available but the modem is faulty
- Not Plugged - The USB modem is unavailable

## New MIB Enhancements

### LLDP MIBs

Two new tables have been added to the **wlsxRSMIB (aruba-rs.my)**. These include:

- **wlsxLldpNeighborTable**: This table enumerates the LLDP neighbors discovered by the access point.
- **wlsxLldpNeighborManAddrTable**: This table enumerates the LLDP neighbor management addresses discovered by the access point.
- **wlsxRemoteWiredPortTable**: The interface name object, **remotePortName**, has been added to this table. This object specifies the name of the port.

### RAP Instrumentation for Airwave Monitoring

The following objects have been added to the **wlsxWlanAPTable**:

- **wlanAPOuterIpAddress**: The outer IP address of the access point
- **wlanAPRemoteLanIpAddress**: The LAN IP address of the Remote Access Point (RAP)
- **wlanAPActiveUplink**: The uplink of the RAP (Ethernet or USB)

The following objects have been added to the **wlsxRemoteUSBTable**:



---

USB modem statistics are applicable only for the USB-based modems AP type Aruba RAP-5WN.

---

- **usbRSSI:** The USB Received Signal Strength Indicator (RSSI)
- **usbStatus:** The device status
- **usbNetworkServiceLevel:** The USB network service level and type
- **usbEsnNumber:** The USB electronic serial number (ESB)
- **usbifOperStatus:** The operational status of the USB interface
- **usbifInUcastOctets:** The received bytes
- **usbifOutUcastOctets:** The transmitted bytes
- **usbifInUcastPkts:** Received unicast packets
- **usbifOutUcastPkts:** Transmitted unicast packets
- **usbifInErrors:** The errors in the incoming interface
- **usbifOutErrors:** The errors in the outgoing interface.

## Aruba Products sysObject IDs

Table 9 defines the sysObjectIds for Aruba products added to this release:

**Table 9** SNMP OIDs returned as sysObjectID for Aruba products

SNMP MIB	OID
ap93h	.1.3.6.1.4.1.14823.1.2.50
rap3wn	.1.3.6.1.4.1.14823.1.2.51
rap3wnp	.1.3.6.1.4.1.14823.1.2.52
ap104	.1.3.6.1.4.1.14823.1.2.53
rap108	.1.3.6.1.4.1.14823.1.2.56
rap109	.1.3.6.1.4.1.14823.1.2.57

## User Idle Timeout Behavior Change

The user idle timeout behavior for the way wireless users are aged out of the system has changed in ArubaOS 6.2.

In ArubaOS pre-6.2 versions, users were idled out if there was no IP traffic for five minutes (the default setting for **configure terminal aaa timers idle-timeout**). Now, users are idled out if there is no wireless traffic.

In ArubaOS 6.2, if the client signals that the AP it has left the BSSID, the client is aged out in the time specified by **aaa user idle-timeout**. Otherwise the client is aged out with the wireless timeout, whose default period is 1000 sec (**configure terminal wlan ssid-profile <profile name> ageout**).

Due to a change in user idle detection internal functionality, there is a possibility that VIA clients may get disconnected prematurely. This change affects non-Windows based VIA users deployed in split-tunnel mode only.

If you notice that the “Idle users due to SOS: other” counter is higher than usual, Aruba suggests that you consider changing **aaa user idle timeout** to a higher value.

```
(host) #show aaa state debug-statistics
user miss: ARP=0, 8021Q=413438, non-IP=0, zero-IP=0, loopback=0
user miss: mac mismatch=308733, spoof=0 (0), drop=379355, ncfg=0 enforce_dhcp=0
```

```
user miss: non-auth opcode=0, no-l2-user=18337, l2tp=0, vrrp=0, special mac=0, iap 13
user=0
Idled users = 26718
Idled users due to MAC mismatch = 0
Idled users due to SOS: wireless tunnel=0 wireless dtunnel=0
Idled users due to SOS: wired tunnel=16460 wired dtunnel=0
Idled users due to SOS: other=0
Idled users due STM deauth: tunnel=9883 dtunnel=0
Idled users from STM timeout: tunnel=345 dtunnel=0
Idled users from STM: other=0
Current users with STM idle flag = 6144
Idle messages: SOS=16460 STM deauth=51952 STM timeout=1
Logon lifetime iterations = 255, entries deleted = 0
SIP authentication messages received 0, dropped 0
Missing auth user deletes: 0
Captive-portal forced user deletes: 0
```

## Changes to Hardware Support

### 651 Controller

Beginning in ArubaOS 6.2, the internal AP of the 651 controller will be disabled. For more information, see [“AP Platform Known Issues” on page 33](#). Additionally, upon upgrade, the 651 will appear as 650-1 and the 651-8 will appear as 650-9 in ArubaOS.

### 3200 Controller

The 3200 controller is not supported on ArubaOS 6.2. However, ArubaOS 6.2 does support the 3200XM controller.

## Upgrade Caveats

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

- If you have mesh APs in your deployment, and Airwave is configured, remove **mgmt-server** configuration before upgrade. Execute the following commands to remove the configuration:

```
no mgmt-server type amp primary-server <mgmt_server_ip>
write memory
```

There is a mesh related stability issue in this release. By disabling **mgmt-server** configuration, you will not be able to use Airwave to manage your network

- Before upgrading to ArubaOS 6.2, you must remove any **phonehome smtp** configuration. Execute the following commands to remove the configuration:

```
no phonehome smtp
write memory
```

Once your upgrade is complete, add **phonehome smtp** back to your configuration.

- ArubaOS 6.2.x is supported only on the newer MIPS controllers (7200 Series, M3, 3200XM, 3400, 3600, and 600 Series).

Legacy PPC controllers (200, 800, 2400, SC1 and SC2) and 3200 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 51](#).)

- User Idle Timeout behavior has changed in ArubaOS 6.2. For more information, see “[User Idle Timeout Behavior Change](#)” on page 20.
- 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.

## Resolved Issues in ArubaOS 6.2

The following issues have been resolved in ArubaOS 6.2.

### AP Datapath

**Table 10** *AP Datapath Fixed*

Bug ID	Description
63782	<p><b>Symptom:</b> An AP would crash and reboot randomly for unknown reasons. This issue has been fixed in ArubaOS 6.2.</p> <p><b>Scenario:</b> This issue was observed only on legacy APs such as AP 60/61 running ArubaOS 6.1.2.x.</p>
67214	<p><b>Symptom:</b> An AP would unexpectedly reboot. This issue was resolved by a change that allows the AP to handle an error by dropping a frame rather than rebooting.</p> <p><b>Scenario:</b> Some occurrences of this issue impacted AP-120 Series access points configured with a 10Mb/s uplink.</p>

### AP Platform

**Table 11** *AP Platform Fixed Issues*

Bug ID	Description
61604	<p><b>Symptom:</b> The option to sort the output of the <b>show ap monitoring</b> command did not work. Sorting can now be done by individual column name. Additionally, the user can now set the order (ascending or descending) of the output.</p> <p><b>Scenario:</b> This issue could occur on all controller models.</p>
69426, 75265	<p><b>Symptom:</b> When a certain internal AP process (SAPD) crashed, configured Virtual APs (VAPs) were not deleted from the AP. When the process restarted, the AP saw that the VAPs already existed. As a result, the following error message was triggered:</p> <p><b>sapd  An internal system error has occurred at file sapd_wlanconfig.c function sapd_wlanconfig_create line 86 error Error creating VAP 0:0</b></p> <p>The AP can now recognize that the undeleted VAPs are already there, avoiding this issue.</p> <p><b>Scenario:</b> This issue was not limited to any specific controller model. When the SAPD process on AP crashes and restarts, it returns this error when it tries to bring up VAPs since the VAPs are already existing. It is a harmless error log and, therefore, the log level was lowered from error to debug.</p>

### AP Regulatory

**Table 12** *AP Regulatory Fixed*

Bug ID	Description
72390	<p><b>Symptom:</b> AP-175 access points would not come up in AP-mode in the Turkey domain. Support for the Turkey domain on AP-175 APs was introduced in ArubaOS 6.2.</p> <p><b>Scenario:</b> This issue was identified on an AP-175 running ArubaOS 6.1.2.7.</p>

**Table 12** AP Regulatory Fixed

Bug ID	Description
73076	<p><b>Symptom:</b> When the RF 802.11g profile was set to channel 13 in European countries, the <b>Invalid channel for 802.11G</b> error message was displayed.</p> <p><b>Scenario:</b> This issue occurred because support for the 8-12 and 9-13 High Throughput (HT) 40MHz channels for all European countries was not available. Due to this issue, the channel pairs 8-12 and 9-13 were not available in the regulatory domain profile for Germany and APs were not initialized in AP mode in the Turkey domain. This issue was found in 3600 controllers running ArubaOS 6.1.3.4 and later.</p>
68431	<p><b>Symptom:</b> AP-135 access points did not support the Chile (CL) Country Domain.</p> <p><b>Scenario:</b> This issue occurred on AP-135 APs running ArubaOS 6.1.3.5 and earlier, and now works properly.</p>

## AP Wireless

**Table 13** AP Wireless Fixed

Bug ID	Description
57624	<p><b>Symptom:</b> An AP-105 sometimes used excessive transmit power on the first transmit packet after the device reset. This issue prevented an AP-105 connected to a Cisco POE switch from getting power. This issue was resolved by a software change that defers transmission power or channel changes if any frames are pending.</p> <p><b>Scenario:</b> This issue occurred on APs that scan outside home channels aggressively.</p>
58361	<p><b>Symptom:</b> The noise floor reported right after an 802.11n AP reset was much higher than normal noise floor values, which sometimes resulted in client connectivity issues. This issue has been resolved.</p> <p><b>Scenario:</b> This issue occurred when ARM scanning was enabled.</p>
61669	<p><b>Symptom:</b> A local controller crashed due to an internal process (SAPD) error.</p> <p><b>Scenario:</b> This issue occurred on a 651 controller running an ArubaOS version where the internal AP is enabled. The internal AP is now disabled so this issue no longer occurs.</p>
65947	<p><b>Symptom:</b> AP-125 performance in 5GHz dropped significantly as RSSI dropped below -65 on ETSI DFS channels. The AP-125 performance in 5GHz now works properly in ArubaOS 6.2.</p> <p><b>Scenario:</b> This issue was observed on an AP-125 running on ArubaOS 6.1.3.2.</p>
65984	<p><b>Symptom:</b> Random AP rebootstrapping was observed along with poor WLAN performance and ping issue. This issue has been resolved in ArubaOS 6.2.</p> <p><b>Scenario:</b> When a controller configured as default gateway in L2 network was responding to a large number of ARP requests, AP rebootstrapping was observed due to high CPU utilization. This issue was observed on controllers running ArubaOS 6.1.3.1 or earlier.</p>
66780	<p><b>Symptom:</b> Some APs in the Turkey country code continuously rebooted when they were configured to use channels 100-140. This has been fixed by adding the missing channel definitions.</p> <p><b>Scenario:</b> This occurred on the AP-60, AP-61, AP-65, AP-70, and AP-85 running on ArubaOS versions pre-6.2 Missing channel definitions in the driver caused the AP to crash.</p>
68347	<p><b>Symptom:</b> Clients were unable to send packets on a virtual AP (VAP) if it had derived more than 32 unique VLANs. The maximum number of supported VLANs per VAP has been raised from 32 to 64.</p> <p><b>Scenario:</b> This issue was not limited to any specific controller model. Clients were unable to send any packets on a VAP if that VAP had more than 32 unique VLANs. The higher limit alleviates this issue.</p>

**Table 13** AP Wireless Fixed (Continued)

Bug ID	Description
69034	<p><b>Symptom:</b> An issue was fixed where a TCP connection between a Panasonic tablet device and an Aruba 802.11n AP timed out frequently in the middle of data transmission.</p> <p><b>Scenario:</b> This issue occurred when the tablet device went into power-save mode very often during data transmission.</p>
69063, 72123	<p><b>Symptom:</b> An unexpected AP reboot occurred. This issue was caused by an internal reference to an empty entry in a data table, and was resolved by adding a check to prevent the access of this data when the entry is not present.</p> <p><b>Scenario:</b> This issue was identified on an AP terminating on a local 3600 controller running ArubaOS 6.1.3.2 in a master-local topology.</p>
71332	<p><b>Symptom:</b> The handoff-assist feature sometimes failed to force a client off an AP when the RSSI dropped below the defined minimum threshold. Clients that exceed the maximum transmission fail threshold defined in the AP's WLAN SSID profile are now moved to a different access point by the handoff assist feature, regardless of whether they are roaming away from the AP.</p> <p><b>Scenario:</b> This issue was identified in ArubaOS 6.1.3.4, and could impact any AP model.</p>
72382	<p><b>Symptom:</b> Ping loss (~5%) was observed in clients (laptops) with Intel pre-15.1 chip sets causing poor voice quality in the voice application running on laptops. This issue has been resolved in ArubaOS 6.2.</p> <p><b>Scenario:</b> This issue occurred on 801.11n APs running on ArubaOS 6.1.3.2.</p>

## Air Management

Bug ID	Description
63116	<p><b>Symptom:</b> The AP did not select the correct primary channel in a 40MHz channel for the Rogue-Aware assignment, and rogue containment was not effective for 40MHz rogue APs on certain channels. AP containment is now working properly on a band when a rogue AP is on a different channel than a valid AP.</p> <p><b>Scenario:</b> This occurred on controllers running ArubaOS 6.1.x. AP-Mode APs are used to contain Rogue APs in other channels (rogue-aware ARM).</p>
66653	<p><b>Symptom:</b> Master and local controllers were not maintaining the same suspect rogue confidence level between them. Suspect rogue confidence level is now sent from the AP to the WLAN Management System (WMS). If WMS is on the master, the local controller will use this to update its own state.</p> <p><b>Scenario:</b> This issue could occur on controllers in a master-local topology, and was not limited to any specific controller model.</p>
67823	<p><b>Symptom:</b> An issue was observed where a large number of BlockACK false positives appeared with the destination MAC address FF::FF::FF::FF::FF::FF. The AP channel scanning mechanism has been improved to prevent this.</p> <p><b>Scenario:</b> This issue could occur on any controller with BlockACK detection enabled (this is enabled by default). A BlockACK attack is detected when a data frame is received outside the range of expected sequence numbers maintained in APs that detect ADDBA frames. Therefore, when a new ADDBA frame was not detected or if the AP did not detect data frames in its expected range, a BlockACK false positive was triggered.</p>
68550	<p><b>Symptom:</b> When A WMS module crash caused by a corrupt ProbePollResponsePacket resulted in slow response of the WebUI and CLI. The controller now checks for message corruption in the ProbePollResponse packet sent from the AP to avoid this issue.</p> <p><b>Scenario:</b> This issue was not limited to any specific controller or AP model and was caused by packet corruption on the network between the AP and controller.</p>

Bug ID	Description
68669	<p><b>Symptom:</b> When there were a large number of devices the database backup operation did not operate properly. As a result, issuing WMS CLI commands such as <b>show wms general</b> and <b>show wms ge</b> would trigger the error “Module WMS is busy. Please try later.”</p> <p><b>Scenario:</b> This occurred on an M3 running ArubaOS 5.0.3.3. Database synchronization took a long time when there were a large number of entries that need updating.</p>

## Authentication

**Table 14** *Authentication Fixed*

Bug ID	Description
61935, 66647, 67620, 50192	<p><b>Symptom:</b> A user did not derive a VLAN from a user derived rule based on DHCP fingerprinting due to errors in the internal key exchange process. This issue has been resolved.</p> <p><b>Scenario:</b> This issue occurred in controllers running ArubaOS 6.1 or later when the SSID used 802.1X authentication.</p>
68412, 74269	<p><b>Symptom:</b> The controller incorrectly used MSCHAPv2 instead of Password Authentication Protocol (PAP) during management authentication. Changes in the internal management authentication process fixed this issue.</p> <p><b>Scenario:</b> This issue occurred when a controller running ArubaOS 6.1.3.0 or later rebooted.</p>
72449	<p><b>Symptom:</b> The AAA RADIUS attributes in the default configuration file were garbled and corrupted. This issue has been resolved in ArubaOS 6.2.</p> <p><b>Scenario:</b> When custom RADIUS attributes were added and deleted multiple times with different attribute ID or vendor ID, incorrect attributes were seen in the configuration file. This issue was not limited to any specific controller model.</p>
72587, 55202	<p><b>Symptom:</b> When a client using MAC authentication roamed, the it was incorrectly assigned the default VLAN instead of a MAC authentication derived VLAN. The fix for this issue properly updates the MAC-authentication VLAN so it does not get overwritten.</p> <p><b>Scenario:</b> This issue occurred when MAC authentication was configured to derive a VLAN from a server followed by the 802.1X authentication.</p>
74831	<p><b>Symptom:</b> When some clients were connecting in EAP-GTC mode, they experienced a token issue and failed authentication. This issue was fixed by sending EAP-Failure message along with the extended EAP-Failure message to the clients.</p> <p><b>Scenario:</b> When RSA Token server sent a failure message, the controller forwarded the extended EAP-Failure message to the client. Some client application was unable to process the extended EAP-Failure message as it was expecting an EAP-Failure message. This issue was observed on controllers running AOS 6.1.x or later.</p>

## Base OS Security

**Table 15** *Base OS Security Fixed*

Bug ID	Description
55301	<p><b>Symptom:</b> The starting and ending IP addresses in the default NAT pool <b>dynamic-srcnat</b> could not be modified on a 600-series controller, although this setting could be modified on other controller models. The fix for this issue prevents users from changing this NAT pool on any controller type, as this value is dynamically created by the controller and shouldn't be modified.</p> <p><b>Scenario:</b> This issue was identified on a 600 Series controller running ArubaOS 5.0.3.3.</p>

**Table 15** Base OS Security Fixed

Bug ID	Description
68425	<p><b>Symptom:</b> Editing an existing user role in the WebUI or issuing the show rights command in the CLI on a controller that has ethernet or MAC-based ACLs with more than 100 configured rules caused the controller to fail to respond properly. This issue has been resolved by a change that also divides the output of the show rights CLI command into sections that display up to 100 rules each.</p> <p><b>Scenario:</b> This issue was first identified in ArubaOS 5.0.3.0, and occurred on a controller with an ACL configured with 100 rules or more.</p>
68467	<p><b>Symptom:</b> The correct VLAN was assigned to a wireless client when the initial dot1x authentication assigned a user a role with a role-based VLAN. However, when the same client reauthenticated using a different credential which assigned a role without a role-based VLAN, the role-based VLAN from the first authentication was incorrectly assigned. Changes in ArubaOS 6.2 resolved this issue and now provides <b>default_role</b> and <b>userderived_vlan</b> information in log messages.</p> <p><b>Scenario:</b> This issue that was noticed in controllers running ArubaOS 6.1.3.2.</p>
69859	<p><b>Symptom:</b> A client was required to reauthenticate using captive portal authentication when roaming to a new AP. This issue was resolved in ArubaOS 6.2.</p> <p><b>Scenario:</b> This issue occurred when a captive portal profile had configured both machine authentication and 802.1X authentication. When a client was momentarily assigned the machine authentication role during roaming, it was forced the user to authenticate using captive portal again.</p>
70307	<p><b>Symptom:</b> A wired client behind an L-3 router could bypass the authentication process on successive connection attempts. This issue was fixed by a change that ensures that these wired clients must reauthenticate to reconnect back to the network after they have aged out.</p> <p><b>Scenario:</b> This issue occurred when multiple wired clients were behind an L3-router. All the wired clients appeared to the controller to have the same mac-address, so after one wired client aged out, a second wired client bypassed the authentication and took over the role which associated to the first, aged-out wired client.</p>
70800	<p><b>Symptom:</b> In the <b>show user</b> CLI command detailed output, the DHCP server IP address was not shown in certain conditions. This issue was fixed by changes to this command. Note that the DHCP server IP address no longer displays in the output.</p> <p><b>Scenario:</b> The DHCP server did not send its own IP address in the siaddr field. This issue was observed in controllers running ArubaOS 6.1.x and later.</p>
73454	<p><b>Symptom:</b> The internal controller model that manages authorization temporarily stopped responding, which impacted client authentication on the network. This issue was resolved with a change that ensures that when a Virtual AP (VAP) is disabled or removed, ACLs that are no longer used are not being referenced.</p> <p><b>Scenario:</b> This issue occurred when a network administrator issued the write mem CLI command on controllers that are running ArubaOS 6.1.3.2 and earlier, and are configured with ap-group ACLs.</p>
73751	<p><b>Symptom:</b> An Internal controller module stopped responding, affecting the ability of management users on the controller to authenticate using a RADIUS server. This issue was caused by internal management user data that did not get properly deleted from the data tree, and has been fixed in ArubaOS 6.2.</p> <p><b>Scenario:</b> This issue was identified on controllers in a master-standby topology, and occurred when a user was configuring authentication settings on the master controller, and issued the <b>write mem</b> command to save the configuration changes.</p>
74353, 75343	<p><b>Symptom:</b> The Universal Database (UDB) module failed on master controller, causing that controller to temporarily lose connectivity to the local controllers. Changes in memory allocation fixed this issue.</p> <p><b>Scenario:</b> This issue occurred on master controller running ArubaOS 6.1.3.4 with more than 255 local controllers.</p>

**Table 15** *Base OS Security Fixed*

Bug ID	Description
74537	<p><b>Symptom:</b> The internal controller model that manages authorization temporarily stopped responding, which could impact client authentication on the network. This issue was resolved with a change to an internal statistics table that now bases the columns of the table on server statistics instead of server names.</p> <p><b>Scenario:</b> This issue was identified in ArubaOS 6.1.3.4, and is not limited to any specific controller model.</p>

## Captive Portal

**Table 16** *Captive Portal Fixed*

Bug ID	Description
53357, 54900, 74688	<p><b>Symptom:</b> An issue was fixed where clicking <b>Accept</b> in the captive portal's user agreement policy page did not redirect users to the requested website. This issue was fixed by the addition of an internal check to verify if client had accepted the acceptable user policy on the login page.</p> <p><b>Scenario:</b> This issue occurred when a custom captive portal login page was configured to use an Acceptable User Policy with no user or guest logon role. This issue was found in controllers running ArubaOS 6.1.3.2 or earlier.</p>

## Configuration

**Table 17** *Configuration Fixed*

Bug ID	Description
68197	<p><b>Symptom:</b> The output of the <b>show ip route</b> command did not display the subnet mask information. This issue has been fixed in ArubaOS 6.2.</p> <p><b>Scenario:</b> This issue occurred on controllers running ArubaOS 6.1.2.5.</p>

## Controller-Platform

**Table 18** *Controller-Platform Fixed*

Bug ID	Description
52685, 52915, 61925, 64196, 64511, 65485, 65541, 65690, 75594	<p><b>Symptom:</b> Errors in the internal datapath or control plane modules caused a M3 or 3000 Series controllers to unexpectedly reboot. Improvements to the internal datapath now prevent this error.</p> <p><b>Scenario:</b> This issue occurred on M3 or 3000 Series controllers in a master-local topology</p>
69595	<p><b>Symptom:</b> The Monitoring section of the WebUI reported an incorrect number of controllers as up when a new controller when a new controller had the same IP address as the controller it replaced. This issue was resolved by improvements to how controller serial numbers are handled after a duplicate controller IP entry is removed.</p> <p><b>Scenario:</b> This issue occurred on 3600 controllers running ArubaOS 6.1.2.3.</p>

**Table 18** *Controller-Platform Fixed*

Bug ID	Description
70075	<p><b>Symptom:</b> Multiple VLANs could not be added into a port channel using the WebUI. The WebUI is now working properly and supports port channel configurations.</p> <p><b>Scenario:</b> This issue in ArubaOS versions earlier than ArubaOS 6.2, and was not limited to any specific controller model.</p>

## DataPath/Platform

**Table 19** *DataPath/Platform Fixed*

Bug ID	Description
60854, 64569	<p><b>Symptom:</b> A controller experienced high CPU utilization when there was large amounts of IPv6 neighbor discovery traffic. This issue was fixed by changes to how ArubaOS manages IPv6 Router Advertisements (RAs).</p> <p><b>Scenario:</b> This issue was found in M3 controllers running ArubaOS 6.1.3.2 or earlier.</p>
66798, 69102, 68829	<p><b>Symptom:</b> Users experienced low throughput after enabling a bandwidth contract. This issue was resolved by an increase in the queue size for lower contract rates.</p> <p><b>Scenario:</b> This issue occurred when contract rates less than 1 Mbps were applied to bandwidth contracts on controllers running ArubaOS 6.1.3.0.</p>

## Dot1x

**Table 20** *Dot1x Fixed*

Bug ID	Description
71930	<p><b>Symptom:</b> Client 802.1x authentication failed after a new security certificate was uploaded on a controller. This issue was the result of a rare condition where some values in a RSA private key were less than 128 bytes in length, and has been resolved by changes to how the controller manages RSA keys.</p> <p><b>Scenario:</b> This issue occurred on controllers running 6.1.3.2 in a master-local topology and updated with new certificates.</p>
75545	<p><b>Symptom:</b> If a Change of Authorization (CoA) request is used to assign a role to a client, the PMK cache is not updated with the CoA information. In scenarios like roaming where the PMK cache is used to bypass full authentication, CoA information is lost. This issue was resolved with a fix that ensures that the cache is updated with the correct CoA role.</p> <p><b>Scenario:</b> This issue was not limited to a specific controller model, and was first identified in ArubaOS 6.1.3.5.</p>

## DPA

**Table 21** *DPA Fixed*

Bug ID	Description
69226	<p><b>Symptom:</b> A controller upgrade from ArubaOS 3.4.4.2 to ArubaOS 6.1.3.1 triggered the configuration error message <b>Configuration Error: Unknown authentication SecureID</b>. Changes to how the controller manages SecureID authentication has resolved this issue.</p> <p><b>Scenario:</b> This issue occurred on a controller where clients used SecureID authentication and a point-to-point protocol (PPP) to log in to the network.</p>

## Dynamic Authorization

**Table 22** *Dynamic Authorization Fixed*

Bug ID	Description
31834	<p><b>Symptom:</b> A client's user rights didn't change correctly when the user roamed to an AP with an ACL based upon an AP-Group. The fix for this issue removed the unnecessary ap-group option from the CLI command <b>user-role &lt;name&gt; access list</b>.</p> <p><b>Scenario:</b> This issue occurred on a controller running ArubaOS 3.3 that used captive portal authentication and had two configured AP groups with different access roles.</p>

## IPsec

**Table 23** *IPsec Fixed*

Bug ID	Description
70903	<p><b>Symptom:</b> The internal controller module that handles IPsec consumes an unusually high amount of CPU resources, and the output of the <b>show crypto isakmp stats</b> CLI command showed an unusually large number of transport reinit. This issue has been resolved in ArubaOS 6.2</p> <p><b>Scenario:</b> This issue was observed in ArubaOS 5.0.2.0, but is not associated with a specific controller type.</p>
72356	<p><b>Symptom:</b> Site to Site VPN between two controller only works when it is initiated from a single side. The fix for this issue allows either controller to act as the initiator.</p> <p><b>Scenario:</b> This issue occurred on local controllers (a 620 and M3) configured to use a site-to-site VPN with the force-natt and pre-connect VPN features enabled. It was first identified in ArubaOS 6.1.3.3</p>
72681	<p><b>Symptom:</b> Remote APs failed to establish an IPsec tunnel with the master controller. This issue was a result of high CPU utilization by the internal controller module that handles IPsec, which caused the process be busy and fail to respond. Changes to how the controller managed stale entries in an internal hash table has resolved this issue.</p> <p><b>Scenario:</b> This issue occurred on a M3 controller in a master-local topology, where the M3 master controller was running ArubaOS 6.1.3.2.</p>

## Mesh

**Table 24** *Mesh Fixed*

Bug ID	Description
70498	<p><b>Symptom:</b> On an AP-93H mesh point, ports ENET1-4 did not work unless ENET0 was used as well. ENET1-4 now work correctly before ENET0 becomes active.</p> <p><b>Scenario:</b> This issue occurred on an AP-93H configured as a mesh point in which ENET0 is not connected.</p>

## RAP

**Table 25** *RAP Fixed*

Bug ID	Description
67191	<p><b>Symptom:</b> A remote AP rebooted with following error message: <b>Module SAPM client is busy. Please try later.</b> This issue has been resolved.</p> <p><b>Scenario:</b> When more than 8 Virtual APs were configured with Remote-AP operation set to "Always", the AP would reboot. This issue was observed on an AP-135 running AOS 6.1.2.8.</p>

## Remote Access Point

**Table 26** *Remote Access Point Fixed*

Bug ID	Description
49070	<p><b>Symptom:</b> A Remote AP (RAP) failed to register in the controller. The fix for this issue checks if the RAP DHCP subnet is the same as the LMS or Tunnel-IP, and changes the RAP DHCP if it matches either value.</p> <p><b>Scenario:</b> When the controller IP address was the same as that of the RAP's DHCP server, the packets were not exchanged between the RAP and the controller. Due to this, the RAP could not download any configuration from the controller. This issue was found in ArubaOS 5.0.2 and later.</p>
75141	<p><b>Symptom:</b> Bridge mode clients do not receive an IP address from the external DHCP server.</p> <p><b>Scenario:</b> This issue occurs due to the restart of an internal AP process (STM module) which causes disruptions to client connectivity and packet forwarding.</p>

## Roles/VLAN Derivation

**Table 27** *Roles/VLAN Derivation Fixed*

Bug ID	Description
51691, 56746	<p><b>Symptom:</b> A client was assigned an incorrect role when using DHCP user derivation rules and captive portal authentication. The fix for this issue allows these clients to receive their correct role.</p> <p><b>Scenario:</b> This issue occurred when a client was incorrectly assigned a derived role during DHCP-renew, and when in Captive Portal authentication mode. This issue was seen in ArubaOS 6.1.0.0.</p>
54037, 56411, 57168, 60866, 61411, 62342, 62808, 62244, 62403, 55898	<p><b>Symptom:</b> The controller assigned VLAN 1 to wired and wireless users that connected over a GRE tunnel. This issue was fixed by improvements to the user authentication process.</p> <p><b>Scenario:</b> This issue occurred when the users connected to a controller over a GRE tunnel, and was found in controllers running ArubaOS 6.1 or earlier.</p>

## Station Management

**Table 28** *Station Management*

Bug ID	Description
64452	<p><b>Symptom:</b> The warning message “number of VLANs limit exceeded 32” appeared when over 32 VLANs were configured on a Virtual AP (VAP). The controller now recognizes that the limit has been reached, but not exceeded, and no longer incorrectly returns this message.</p> <p><b>Scenario:</b> This issue occurred on any situation in which 32 VLANs are configured per VAP.</p>

## STP

**Table 29** *STP Fixed*

Bug ID	Description
64164	<b>Symptom:</b> The Spanning Tree port cost calculation was incorrect. The fix allows the output of the <b>show spanning-tree interface</b> CLI command to display the correct path cost. <b>Scenario:</b> This issue was observed on a controller with Spanning Tree enabled.

## UI-Configuration

**Table 30** *UI Configuration Fixed*

Bug ID	Description
52624	<b>Symptom:</b> The WebUI did not allow users to add a new policy with a destination netmask in standard format (255.255.255.0). This issue has been resolved in ArubaOS 6.2. <b>Scenario:</b> While adding a new policy in the <b>Configuration&gt;Security&gt;Access Control&gt;User Roles&gt;Add Role&gt;Add new policy</b> page in the WebUI, the destination mask was not accepted in dotted decimal format. This issue was not limited to any specific controller model.

## UI-Monitoring

**Table 31** *UI Monitoring Fixed*

Bug ID	Description
65323	<b>Symptom:</b> User IDs did not display properly in the WebUI. This issue was solved by a change that allows the user table to display only 50 rows of output at once. <b>Scenario:</b> The <b>Dashboard &gt; Clients</b> page in the WebUI did not display the user IDs properly when special characters such as “ ” were used in the user ID. This issue was not limited to a specific controller model.
66887, 62519	<b>Symptom:</b> The WebUI displays a javascript error. This issue was fixed by changes to how javascript is loaded on the WebUI page. <b>Scenario:</b> When a user selected the <b>status</b> button on the <b>Monitoring &gt; Access Points</b> page, the WebUI displayed a blank page with a javascript error. This issue was observed on controllers running 6.1.2 or earlier and was not limited to a specific controller model.

## Voice

**Table 32** *Voice Fixed*

Bug ID	Description
65978	<b>Symptom:</b> The voice quality of VoIP softphone call was poor. <b>Scenario:</b> This issue occurred when a Session Initiation Protocol (SIP) call was initiated with the an update instead of an invite, so the call was not placed into the voice queue. This resulted in poor voice quality. This issue was found in controllers running ArubaOS 6.1.3.0.

## WebUI

**Table 33** *WebUI Fixed*

Bug ID	Description
62907	<p><b>Symptom:</b> The Access Control List (ACL) rules associated with host entries could not be deleted from the WebUI. Changes to the internal command syntax fixed this issue.</p> <p><b>Scenario:</b> This issue occurred when a user tried to delete the ACL rules associated with <code>netdestination</code> host entries from the WebUI. This issue occurred because the <code>netmask</code> keyword was added to the command generated for the ACL instead of the <code>host</code> keyword. This issue was found in controllers running ArubaOS 6.1.2.6.</p>
66388	<p><b>Symptom:</b> The WebUI displayed AAA test authentication messages in red text. WebUI updates have changed the authentication messages, so that a successful AAA test authentication on the <b>Diagnostics&gt;Network&gt; AAA Test Server</b> page of the WebUI is now displayed in green text.</p> <p><b>Scenario:</b> This issue was found in controllers running ArubaOS 6.1.3.2 or earlier.</p>
66516	<p><b>Symptom:</b> APs were not sorting properly by name in the <b>Configuration &gt; Wireless &gt; AP Installation &gt; Provisioning</b> page of the WebUI and the UI sorted only the APs in the current page instead of the entire list.</p> <p><b>Scenario:</b> When a user was sorting the APs in the <b>Provisioning</b> page, only the APs in the current page were sorted instead of the entire list of APs distributed in multiple pages. This issue was found in the controllers running ArubaOS 6.1.3.6 or earlier.</p>
67304	<p><b>Symptom:</b> A user was unable to provision an AP-61 as a RAP from the WebUI of a master controller. Improvements to how the controller handles FQLN campus names with special characters fixed this issue.</p> <p><b>Scenario:</b> This issue occurred when a user tried to provision an AP-61 as a RAP from the WebUI of a master controller running ArubaOS 6.1.3.0, and included special characters in the Fully Qualified Location Name (FQLN) campus name.</p>
70844	<p><b>Symptom:</b> Firewall policies could not be deleted from the <b>Configuration&gt;Security&gt;Access Control&gt;User Roles</b> tab in the WebUI. Changes to the internal command syntax fixed this issue.</p> <p><b>Scenario:</b> When a user edited a firewall policy from the <b>User Roles</b> tab in the WebUI, some ACL rules that contained the <code>host</code> keyword could not be deleted. This issue occurred because ArubaOS considered single IP addresses in the source and destination to be a <code>network</code> value instead of a <code>host</code> value. This issue was found in controllers running ArubaOS 6.1.3.2 or later.</p>
73656	<p><b>Symptom:</b> Creating a user role in the WebUI during a session that timed out caused a loop of <b>User not logged on</b> error messages. This issue was fixed by improvements to the internal session timeout settings.</p> <p><b>Scenario:</b> This issue occurred when an administrator used Internet Explorer to add a user role and the WebUI timed out. It was observed on a 3200 controller running ArubaOS 6.1.3.1.</p>

## WMM

**Table 34** *WebUI Fixed*

Bug ID	Description
65159	<p><b>Symptom:</b> The “Tx WMM [xx] Dropped” counter in the output of the <b>show ap debug client-stats</b> CLI command did not accurately display dropped frames. This issue was resolved by a change that ensured the counter for dropped WMM frames incremented every time a frame is dropped.</p> <p><b>Scenario:</b> This issue occurred on ArubaOS 6.1.2.7 for AP-135 and AP-105 access points.</p>

## Known Issues and Limitations in ArubaOS 6.2

The following are known issues and limitations found in this release of ArubaOS. Applicable Bug IDs and workarounds are included.

## AP Wireless

**Table 35** AP Known Issues

Bug ID	Description
74811	<p><b>Symptom:</b> A wireless patient monitor which continuously sends multicast traffic to a wired monitor in is not working properly. Packets are not received at the AP when multicast traffic from the wireless monitoring system is sent to wired and wireless clients.</p> <p><b>Scenario:</b> This occurs on AP-65 and ArubaOS 6.1.3.4.</p> <p><b>Workaround:</b> None</p>
74984	<p><b>Symptom:</b> Blackberry devices are experiencing severe ping losses when connected to a high throughput SSID.</p> <p><b>Scenario:</b> This issue occurs on AP-135 running on ArubaOS 6.1.3.4 when setting the HT-SSID.</p> <p><b>Workaround:</b> None</p>
75599	<p><b>Symptom:</b> When the diversity-spreading-workaround feature is disabled, the signal strength on the AP goes down depending upon the position from which you are monitoring the AP.</p> <p><b>Scenario:</b> This issue occurs on any deployment with an 802.11n AP running on ArubaOS 6.1.3.2 and later. When this diversity-spreading-workaround feature is enabled, all legacy transmissions will be sent using a single antenna. This enables interoperability for legacy or high-throughput stations that cannot decode 802.11n cyclic shift diversity (CSD) data. The diversity-spreading-workaround behavior changes when the default value changes and this feature is turned off.</p> <p><b>Workaround:</b> Enable diversity-spreading-workaround by disabling the diversity-spreading-workaround parameter in the HT-radio-profile.</p>

## AP Platform

**Table 36** AP Platform Known Issues

Bug ID	Description
58011, 61100, 57925, 60846, 60722, 64517, 66118, 66128, 66185, 66659, 66596, 64526, 61539, 61196, 67435, 67670, 67671, 67673, 67871, 67872, 67977, 68875, 68937, 72069, 74142, 75366, 75539, 75703, 75366	<p><b>Symptom:</b> An Aruba 651 controller reboots unexpectedly after enabling the internal AP.</p> <p><b>Scenario:</b> This issue is observed in Aruba 651 controllers running ArubaOS 5.0 or above.</p> <p><b>Workaround:</b> Effective ArubaOS 6.2, internal AP is disabled in this controller.</p>

## Air Management

**Table 37** *Air Management Known Issues*

Bug ID	Description
74285	<p><b>Symptom:</b> “WMS module busy” message may appear when executing the <b>show run</b> command on a standby-master controller.</p> <p><b>Scenario:</b> This issue was first identified on a controller running ArubaOS 6.1.2.0 and is not specific to any controller platform. It occurs in a master-local topology but the trigger is not yet known.</p> <p><b>Workaround:</b> None</p>
74324	<p><b>Symptom:</b> A WMS module crash has been observed on an M3 controller running ArubaOS 6.1.3.1. When this occurs, you will not be able to execute any WMS-related CLI commands or a <b>write mem</b>.</p> <p><b>Scenario:</b> This issue occurs on master controllers running ArubaOS 6.1.3.1 or later possibly caused by an internal process malfunction.</p> <p><b>Workaround:</b> None.</p>

## Authentication

**Table 38** *Authentication Known Issues*

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

## Base OS Security

**Table 39** *Base OS Security Known Issues*

Bug ID	Description
55419	<p><b>Symptom:</b> An internal ArubaOS process (Certmgr) becomes busy when the OCSP server is unreachable.</p> <p><b>Scenario:</b> Users are unable to authenticate because certmgr is busy queuing the OCSP requests. (All users doing dot1x, IKE, mgmt-auth are affected). This issue is observed on all controllers running ArubaOS 6.2.</p> <p><b>Workaround:</b> None</p>
73130	<p><b>Symptom:</b> When a client reconnects, the 802.1X role is assigned instead of the defined Aruba External Services Interface (ESI) syslog parser role.</p> <p><b>Scenario:</b> This issue occurs because the 802.1X role is cached and the role assigned by the ESI server is overwritten when the client reconnects.</p> <p><b>Workaround:</b> Delete the cache entry of the client: aaa authentication dot1x key-cache clear [station-mac] or delete user entry before the 802.1X role is triggered again: aaa user delete mac &lt;a:b:c:d:e:f &gt;</p>

**Table 39** Base OS Security Known Issues (Continued)

Bug ID	Description
74837	<p><b>Symptom:</b> The controller reboots when the user authentication process fails.</p> <p><b>Scenario:</b> This issue occurs when the Novell eDirectory service sends the <code>equivalentToMe</code> and <code>SecurityEquals</code> optional parameters to the Aruba controller. This issue is not limited to any specific controller model.</p> <p><b>Workaround:</b> Disable the optional parameters in Novell eDirectory service before sending the response to the Aruba controller.</p>
76233	<p><b>Symptom:</b> In ArubaOS 6.2, the Access Control List (ACL) limit is reduced by the number of roles defined.</p> <p><b>Scenario:</b> This limitation can occur on any controller running ArubaOS 6.2. This limitation exists because 2 ACLs are created for every user role that is added. Of these two ACLs, only one is actively used for assigning user roles (stateful ACL) and the other is not used for any operation (stateless ACL). The following commands can be used to identify which ACL is actively being used: <b>show right &lt;role-name&gt;</b>, <b>show acl acl-table</b>, and <b>show ap global acl-table</b>.</p> <p><b>Workaround:</b> None.</p>
76291	<p><b>Symptom:</b> An internal controller process (<code>resolvewrap</code>) crashes at random interval when a RADIUS authentication server is configured with host-name.</p> <p><b>Scenario:</b> This crash does not have any impact on the ArubaOS operation as the <code>resolvewrap</code> process is used only for resolving the host-name configured for authentication server periodically. If resolving the host-name fails due to crash then subsequent attempt to resolve the host name would be a success.</p> <p><b>Workaround:</b> If this crash is observed continuously then it is recommended that an IP address is used instead of host-name in the server authentication profile.</p>
74777	<p><b>Symptom:</b> Clients were incorrectly assigned the default gateway IP address. If the <code>validuser</code> ACL on the controller did not contain the gateway IP address, those clients experienced traffic loss and network connectivity issues.</p> <p><b>Scenario:</b> This issue was observed on controllers running ArubaOS 6.1.3.2 and Windows 7 clients.</p> <p><b>Workaround:</b> Add the gateway IP address to the <code>validuser</code> ACL.</p>
75754	<p><b>Symptom:</b> The user table shows that some 802.1x authenticated clients managed by an external XML-API server are using Web authentication, even though there is no captive portal authentication configured for those clients.</p> <p><b>Scenario:</b> This issue occurred on a controller configured with a 802.1x default role with an ACL that sends traffic through the GRE tunnel to a SafeConnect appliance. In this scenario, L3 authentication is managed by the SafeConnect XML API, which updates the user role to an L3-authenticated role.</p> <p><b>Workaround:</b> None</p>
75565	<p><b>Symptom:</b> A wired user is incorrectly assigned the initial user role instead of a user role derived from DHCP fingerprinting.</p> <p><b>Scenario:</b> This issue has been observed in ArubaOS 6.1.3.4, and is not specific to any controller platform.</p> <p><b>Workaround:</b> Delete the user and verify that the corresponding bridge entry is removed from the datapath before reconnecting the user.</p>

## Controller Platform

**Table 40** *Controller-Platform Known Issues*

Bug ID	Description
52685, 52915, 61925, 64196, 64511, 65485, 65541, 65690, 75594	<p><b>Symptom:</b> Errors in the datapath or control plane modules can cause a M3 or 3000 Series controller to unexpectedly reboot.</p> <p><b>Scenario:</b> This issue occurs on M3 or 3000 Series controllers in a master-local topology</p> <p><b>Workaround:</b> None</p>
72185	<p><b>Symptom:</b> Campus APs are not coming up when control plane security is enabled.</p> <p><b>Scenario:</b> This issue occurs when the whitelist database is not synchronized between the master and local controllers, and is observed on controllers running ArubaOS 6.1.3.1.</p> <p><b>Workaround:</b> Clear the whitelist database on all local controllers and synchronize from the master controller before enabling control plane security.</p>
72485, 72859, 74297, 74857, 75400, 75428	<p><b>Symptom:</b> The 3600, 6000, and M3 controllers reboot unexpectedly due to <b>User-Pressed Reset</b> and <b>Control Plane Kernel Panic</b> causes.</p> <p><b>Scenario:</b> This issue is found in 3600, 6000, and M3 controllers running ArubaOS 6.1.2.4 or later versions. The 6000 and M3 controllers reboot stating <b>User Pressed Reset</b> as the cause, while the 3600 controllers fail due to <b>Control Plane Kernel panic</b> issue.</p> <p><b>Workaround:</b> None</p>
74048, 75107	<p><b>Symptom:</b> 72x0 controllers crash due to AMSDU traffic.</p> <p><b>Scenario:</b> This issue occurs when a client makes a wireless connection to the AP-125. Upon receiving the AMSDU traffic, the Aruba 72x0 controller crashes. The issue is seen in ArubaOS 6.2.0.0.</p> <p><b>Workaround:</b> By default, AMSDU negotiation is disabled on 72x0 controllers. However if a client does not accept the AMSDU negotiation, disable AMSDU processing on the controller by setting the AMSDU parameter to <b>no firewall amsdu</b>.</p>
75411	<p><b>Symptom:</b> 10GE ports on Aruba 7200 Series controllers are reporting sporadic packets being dropped with CRC errors.</p> <p><b>Scenario:</b> This is an infrequent occurrence on these controllers.</p> <p><b>Workaround:</b> Reboot the controller. Use the <code>show port status</code> command to see if the CRC counter is incrementing properly.</p>
76220	<p><b>Symptom:</b> Controller crashes due to a virtual AP configuration change.</p> <p><b>Scenario:</b> In a high traffic deployment, when a virtual AP with active client associations is removed from an AP group, a race condition may trigger a controller crash.</p> <p><b>Workaround:</b> Before removing a virtual AP profile from an AP group, wait for all active associated clients to disassociate or time out. Use the <code>show ap association</code> command to verify the virtual AP client association status.</p>

## Dot1x

**Table 41** *Dot1x Known Issues*

Bug ID	Description
50785	<p><b>Symptom:</b> Multicast key rotation is not working with 802.1x clients in bridge mode.</p> <p><b>Scenario:</b> This occurs only with bridge mode clients running 6.x versions of the software.</p> <p><b>Workaround:</b> Disable multicast key rotation using the <code>configure terminal aaa authentication dot1x default no multicast key rotation</code> command.</p>

**Table 41** *Dot1x Known Issues*

Bug ID	Description
71363	<p><b>Symptom:</b> A client configured to use both machine and user authentication cannot authenticate on the network.</p> <p><b>Scenario:</b> This issue was observed on clients using a Dell 1520 wireless with the 1/7/2011 driver in a wireless network managed by a controller running ArubaOS 6.1.3.2.</p> <p><b>Workaround:</b> Configure a client to use machine or user authentication, but not both.</p>
74663	<p><b>Symptom:</b> Clients are not able to reauthenticate after rebooting or logging off the networks.</p> <p><b>Scenario:</b> This issue was 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 radio profile.</p> <p><b>Workaround:</b> Disable the eapol logoff setting in the 802.11Xradio profile. (This setting is disabled by default.)</p>

## IPSec

**Table 42** *IPv6 Known Issues*

Bug ID	Description
75891	<p><b>Symptom:</b> Upon idle timeout, the controller will not send the ping request before aging out the user. The user will be aged out immediately. This applies for VPN, VIA-VPN users as well. When the users ageout, VPN tunnel will also go down.</p> <p><b>Scenario:</b> On all controller platforms running ArubaOS 6.2 or later, this occurs when there is no data for the user during the ageout time period. In case of VPN and VIA-VPN, if the IPSEC tunnel does not have any data for the configured user ageout time, user will be aged out and the tunnel will be deleted.</p> <p><b>Workaround:</b> Increase the value of user ageout time. The default value is 5 minutes. Additionally, if you can ensure that there is always some data sent from the user, this issue can be avoided.</p>

## IPv6

**Table 43** *IPv6 Known Issues*

Bug ID	Description
47868	<p><b>Symptom:</b> The IPv6 alias cannot be created, because there is no <b>Name</b> option for netdestination6.</p> <p><b>Scenario:</b> The <b>Name</b> option is currently not available for netdestination6. Due to this limitation, the IPv6 alias cannot be created for DNS Name queries. This issue is found in ArubaOS 6.1.0.0 or later, and is not limited to any specific controller model.</p> <p><b>Workaround:</b> Provide the host or network IP address of the required destination to set the URL.</p>
47882	<p><b>Symptom:</b> The IPv6 whitelist does not bypass the Captive Portal login and connect to the desired URL.</p> <p><b>Scenario:</b> This issue occurred because the IPv6 netdestination is not supported inside whitelist in the current release. This issue is found in controllers running ArubaOS 6.1.0.0 or later versions.</p> <p><b>Workaround:</b> None</p>

**Table 43** IPv6 Known Issues

Bug ID	Description
57059	<p><b>Symptom:</b> The IPv6 routing fails when maximum IPv6 VLAN interfaces are configured in the controller.</p> <p><b>Scenario:</b> When more than 300 IPv6 VLAN interfaces are configured with three global addresses each on an 3600 controller, the IPv6 routing fails. Currently the following IPv6 interface addresses are supported:</p> <ul style="list-style-type: none"> <li>Aruba 600 Series, 3200 controllers: 32 IPv6 VLAN interfaces * 3 IPv6 addresses per interface = 96 IPv6 addresses</li> <li>3400, 3600 controllers: 64 IPv6 VLAN interfaces * 3 IPv6 addresses per interface = 192 IPv6 addresses</li> <li>Aruba M3, Aruba 7200 Series controllers: 128 IPv6 VLAN interfaces * 3 IPv6 addresses per interface = 384 IPv6 addresses</li> </ul> <p>This issue is in ArubaOS 6.2 or earlier, and is not limited to any specific controller model.</p> <p><b>Workaround:</b> Limit the number of IPv6 VLAN interfaces to the supported limit.</p>
74367	<p><b>Symptom:</b> Clients using temporary IPv6 addresses are not be able to communicate as traffic is getting dropped.</p> <p><b>Scenario:</b> A client can support up to four IPv6 addresses. The usage of temporary IPv6 addresses on the clients generates additional IPv6 addresses and sends traffic using all these IPv6 addresses, which exceeds the limitation of four IPv6 entries for the client in the user-table. The issue occurs on the controllers that support IPv6 clients.</p> <p><b>Workaround:</b></p> <ul style="list-style-type: none"> <li>Delete unused IPv6 addresses from the user-table with the command <code>aaa ipv6 user delete &lt;ip address&gt;</code>.</li> <li>Increase the time that a client keeps the temporary IPv6 address before changing to a new address.</li> <li>Avoid the usage of temporary IPv6 addresses.</li> </ul>
76426	<p><b>Symptom:</b> There is an increase in CPU utilization by user authentication process in the controller.</p> <p><b>Scenario:</b> This issue occurs when HTC One X smartphone running Android version 4.1.1 generates a link-local IPv6 address fe80::/128; sends ICMPv6 Neighbor Solicitation packet to the controller but the controller drops this packet. The smartphone sends these packets in a loop expecting an acknowledgement. This increases the CPU utilization in the controller. This issue is found in controllers running any version of ArubaOS.</p> <p><b>Workaround:</b> Create a rule in the <code>validuser</code> ACL to deny packets from host fe80::/128, before permitting any IPv6 traffic:</p> <pre>ip access-list session validuser   network 169.254.0.0 255.255.0.0 any any deny   any any any permit   ipv6 host fe80:: any any deny   ipv6 any any any permit !</pre>

## Local Database

**Table 44** Local Database Known Issues

Bug ID	Description
75662, 75659	<p><b>Symptom:</b> An incomplete or incorrect upgrade procedure occurs when an 3600 controller crashes after upgrading.</p> <p><b>Scenario:</b> This issue occurs on controllers upgrading from ArubaOS 6.1.2.2 to ArubaOS 6.1.3.5.</p> <p><b>Workaround:</b> None</p>

**Table 44** *Local Database Known Issues*

Bug ID	Description
75701	<p><b>Symptom:</b> An incomplete or incorrect upgrade procedure occurs. The internal controller process (UDB Server module) fails after upgrading from ArubaOS 6.1.2.3 to ArubaOS 6.1.3.4.</p> <p><b>Scenario:</b> This issue occurs on M3 controllers upgrading from ArubaOS 6.1.2.3 to ArubaOS 6.1.3.4.</p> <p><b>Workaround:</b> None</p>

## Management Auth

**Table 45** *Management Auth Known Issues*

Bug ID	Description
74274	<p><b>Symptom:</b> A user was not deleted from a user table after the user was idle for a period that exceeded the AAA user idle timeout.</p> <p><b>Scenario:</b> This issue was observed on a local controller in a master-local topology with multiple local controllers, and may be associated with an idle timeout value that is out-of-sync between the datapath and the controller's authentication settings.</p> <p><b>Workaround:</b> None</p>
75665	<p><b>Symptom:</b> A 3rd generation iPad running iOS 6.0.1 is incorrectly assigned to the default VLAN.</p> <p><b>Scenario:</b> This issue occurs in ArubaOS 6.1.3.5, when a Virtual AP is configured with both MAC authentication and 802.1X authentication, a VLAN derivation rule is configured on the MAC authentication server, and the derived VLAN is different from the VAP's default VLAN.</p> <p><b>Workaround:</b> None</p>

## MAC-Based Authentication

**Table 46** *MAC-Based Authentication Known Issues*

Bug ID	Description
56130	<p><b>Symptom:</b> A client receives a logon user role instead of a mac-authentication user role.</p> <p><b>Scenario:</b> This issue occurs when a client associates to an AP that is connected to one controller, but terminates on another controller. It was first observed in controllers running ArubaOS 6.1.2.0</p> <p><b>Workaround:</b> None</p>

## Mobility

**Table 47** *Mobility Known Issues*

Bug ID	Description
58883, 60328	<p><b>Symptom:</b> In a Layer-3 IP mobility enabled network, when the client moves from a Home Agent network to a Foreign Agent network, the IPv4 address of the client changes. This prevents the client from sending traffic.</p> <p><b>Scenario:</b> 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 or earlier.</p> <p><b>Workaround:</b> Do not issue the <b>router enable</b> command along with the <b>ipv6 enable</b> command in the controller.</p>

**Table 47** *Mobility Known Issues (Continued)*

Bug ID	Description
63163	<p><b>Symptom:</b> There is an increase in datapath CPU utilization in the controller.</p> <p><b>Scenario:</b> 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.</p> <p><b>Workaround:</b> Do not change the IP address of the wired client at a rapid rate.</p>
63164, 63144	<p><b>Symptom:</b> The Layer-3 IP Mobility process fails in the controller.</p> <p><b>Scenario:</b> This issue occurs when a network administrator enables and disables the <b>router mobile</b> command, and leads to the incomplete cleanup of client states or controller malfunction. This issue is not limited to any specific controller model or version of ArubaOS.</p> <p><b>Workaround:</b> Reboot the controller when the status of the <b>router mobile</b> command changes.</p>

## RAP

**Table 48** *RAP Known Issues*

Bug ID	Description
51546	<p><b>Symptom:</b> RAP5 drops off from the network randomly.</p> <p><b>Scenario:</b> This is a hardware issue with Sierra 312 USB modem causing the RAP5 to drop off from the network. This issue is observed when Sierra 312 USB modem is used on 3600 controllers running ArubaOS 6.1 or earlier.</p> <p><b>Workaround:</b> Upgrade the firmware of Sierra 312 USB modem from <a href="http://sierrawireless.com">sierrawireless.com</a> or use a different modem.</p>

## Roles/VLAN Derivation

**Table 49** *Roles/VLAN Derivation Known Issues*

Bug ID	Description
66261	<p><b>Symptom:</b> When the <b>Even VLAN</b> and <b>Preserve VLAN</b> features are enabled in the Virtual APs (VAPs) and a client moves from one VAP to another, it is placed in a VLAN of the current VAP instead of the new VAP.</p> <p><b>Scenario:</b> This issue occurs when the client moves from one VAP to another with <b>Even VLAN</b> and <b>Preserve VLAN</b> features enabled. As the client is placed in the VLAN of the current VAP and if the client VLAN does not exist in the new VAP, the client connection fails.</p> <p><b>Workaround:</b> Check with the Aruba Support team before you enable the <b>Even VLAN</b> and <b>Preserve VLAN</b> features.</p>

## SNMP

**Table 50** *SNMP Known Issues*

Bug ID	Description
75570	<p><b>Symptom:</b> An SNMP query from Airwave timed out when the query was directed to the master controller out at peak hours.</p> <p><b>Scenario:</b> This issue occurs on a master controller running ArubaOS 6.1.3.2 or later.</p> <p><b>Workaround:</b> None.</p>

## Station Management

**Table 51** *Station Management Known Issues*

Bug ID	Description
72194	<p><b>Symptom:</b> When VLAN pooling is used with the assignment type EVEN, the user VLAN changes when the client roams from AP to AP, but the IP address remains the same until a release/renew is executed on the client device.</p> <p><b>Scenario:</b> This issue can occur on any controller model with the VLAN mobility and preserve VLAN features enabled. When these features are enabled, the controller's bridge table keeps user entries for 12 hours. This issue occurs when the controller's STM module (an internal process) does not find the entry in the bridge lookup result.</p> <p><b>Workaround:</b> Disable VLAN mobility and preserve VLAN.</p>

## VIA

**Table 52** *VIA Known Issues*

Bug ID	Description
76377	<p><b>Symptom:</b> When a Windows XP client restarts VIA, VIA returns a message stating that the IPSec process could not be enabled.</p> <p><b>Scenario:</b> This occurs on Windows XP clients running VIA. Clients running other operating systems are not affected.</p> <p><b>Workaround:</b> None.</p>

## WebUI

**Table 53** *WebUI Known Issues*

Bug ID	Description
66521	<p><b>Symptom:</b> Two <b>Apply</b> buttons are displayed in the WebUI when adding users to the internal database.</p> <p><b>Scenario:</b> While creating a new user in the WebUI, two <b>Apply</b> buttons appear in the <b>Configuration &gt; Security &gt; Authentication &gt; Internal DB</b> page due to incorrect labeling of the buttons. This issue is not limited to a specific controller model.</p> <p><b>Workaround:</b> Use the <b>Apply</b> button at the top to add a new user. Use the <b>Apply</b> button at the bottom to apply any user list changes.</p>
73170	<p><b>Symptom:</b> Numerous error messages appear in the error.log file where internal processes (such as STM and WMS) are not able to get data from the database.</p> <p><b>Scenario:</b> This issue occurs on a M3 master controller after upgrading from ArubaOS 6.1.3.0 to ArubaOS 6.1.3.4. This issue is caused by a MySQL index file that is inconsistent with its data file. This causes the MySQL server to restart continuously thus preventing other processes that are using the database from inserting or modifying database entries.</p> <p><b>Workaround:</b> Contact Aruba Tech Support at <a href="http://support.arubanetworks.com/">http://support.arubanetworks.com/</a>.</p>
74227	<p><b>Symptom:</b> The Monitoring tab of the WebUI and the output from the <b>show ap active</b> command do not match. The WebUI shows more APs than are actually up and the output of <b>show ap active</b> displays the correct number.</p> <p><b>Scenario:</b> This can occur on any controller model acting as a master and running ArubaOS 6.1.3.2 or later if the bootstrap threshold in the ap system profile is set to more than 40 minutes. In this instance, these APs were powered off when the controller attempted to send a configuration update. The APs failed to receive the update, and the controller marked the APs as down but did not update the AP database as well.</p> <p><b>Workaround:</b> None.</p>

## WMM

**Table 54** *WMM Known Issues*

Bug ID	Description
68503	<p><b>Symptom:</b> The controller chooses 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.</p> <p><b>Scenario:</b> This issue is observed on controllers running AOS 6.2 or lower in Tunnel and D-Tunnel modes.</p> <p><b>Workaround:</b> None.</p>

## 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 have been grouped together.

### AP

**Table 55** *AP Issues Under Investigation*

Bug ID	Description
69424	<p><b>Symptom:</b> When upgrading to ArubaOS 6.2, the AP-125 may crash when rebooted after the upgrade but recovers on subsequent boots. This causes a longer upgrade cycle to occur.</p> <p><b>Scenario:</b> This occurs when upgrading to ArubaOS 6.2 from ArubaOS 6.1.3.2 and later in any deployment with an AP-125.</p> <p><b>Workaround:</b> None</p>
72203	<p><b>Symptom:</b> APs are not coming up and are unable to establish an IPsec tunnel with the controller. This issue is observed on ArubaOS controller running AOS 6.1.3.4. The cause has not been identified.</p>
72618	<p><b>Symptom:</b> An unexpected reboot of an AP-125 terminating on controller running ArubaOS 6.1.3.3 has been observed.</p>
74074	<p><b>Symptom:</b> APs that are up and running on a local controller are listed as DOWN in the master's AP database.</p>
75513	<p><b>Symptom:</b> Clients connected to an AP-135 in a network running ArubaOS 6.1.3.4 take more than 30 seconds to complete the 802.1x authentication, while they are roaming in the network.</p>
75373	<p><b>Symptom:</b> AP-135s in a network running ArubaOS 6.1.3.2 and terminated on the 3600 controller crash due to IPsec encryption failures.</p>
75564	<p><b>Symptom:</b> An unexpected reboot of an AP-135 terminating on controller running ArubaOS 6.1.3.3 has been observed.</p>

## Authentication

**Table 56** *Authentication Observed Issues*

Bug ID	Description
75832	<b>Symptom:</b> EAP-TLS authentication fails for the MAC clients connected to a Remote AP in split-tunnel mode. This issue is observed on controller running ArubaOS 6.1.2.6.

## Base OS Security

**Table 57** *Base OS Security Observed Issues*

Bug ID	Description
67287	<b>Symptom:</b> When L3 mobility is enabled and the <b>auth-sta-roam</b> option is disabled in a network, the alternate home agent for a client does not work and the client is not able to roam.
73373	<b>Symptom:</b> Captive portal authentication for wireless users does not work in some cases as the users are not able to access the Captive Portal login page. The same issue is seen in wired users when they try to access the Web configuration login page.
74631	<b>Symptom:</b> Wired users in tunnel mode, connected to a RAP-5, show up as wired (remote) users when the forward mode of the wired port is changed from split to tunnel. This issue is seen in ArubaOS 6.1.3.4.
75082	<b>Symptom:</b> A controller failed to properly detect or report a MAC/IP spoofing event.
75022	<b>Symptom:</b> A standalone 3200 controller running ArubaOS 6.1.3.2 experiences unusually high CPU utilization.

## Controller-Datapath

**Table 58** *Controller-Datapath Observed Issues*

Bug ID	Description
68211	<b>Symptom:</b> An unexpected controller reboot occurs. The cause has not been identified.
72359, 73246, 73256, 74575, 75700, 75753	<b>Symptom:</b> An unexpected timeout in an internal datapath process caused a controller to unexpectedly reboot.
73350	<b>Symptom:</b> A high number of IPsec encryption failures caused an AP-135 remote AP to reboot.
74942	<b>Symptom:</b> Wireless clients experienced degraded network throughput when the user count on a controller reached 2500 users. This issue has also been associated with a high number of buffer allocation failures.
75137	<b>Symptom:</b> Wireless clients are unable to communicate with a multicast router using a VLAN that does not have a configured IP address.

## Dot1x

**Table 59** *Dot1x Observed Issues*

Bug ID	Description
75082	<b>Symptom:</b> Starting with ArubaOS 6.2, the <b>validate-pmk</b> parameter in a dot1x authentication profile is enabled by default. If a controller has multiple dot1x authentication profiles, and at least one has the validate-pmk feature enabled, other dot1x authentication profiles that previously didn't have validate-pmk enabled may have the validate-pmk enabled after the upgrade to 6.2.
75860	<b>Symptom:</b> A 3rd generation iPad cannot roam between APs in bridge mode. This issue is associated with a PMK caching failure in bridge mode.

## Mesh

**Table 60** *Mesh Observed Issues*

Bug ID	Description
75705	<b>Symptom:</b> An AP-175P used as a mesh point fails to connect to an AP-175P mesh portal after an upgrade to ArubaOS 6.1.3.5.

This chapter describes the known issues and limitations identified in this version of ArubaOS.

## Phonehome SMTP

Before upgrading to ArubaOS 6.2, you must remove any phonehome smtp configuration. To do this, execute **no phonehome smtp** followed by a **write memory** from the configuration terminal mode in the CLI. Once your upgrade is complete, add phonehome smtp back to your configuration.

## Supported Browsers

Beginning with ArubaOS 6.0, the following browsers are officially supported for use with the ArubaOS WebUI:

- Microsoft Internet Explorer 8.x on Windows XP, Windows Vista, Windows 7, and MacOS
- Mozilla Firefox 3.x on Windows XP, Windows Vista, Windows 7, and MacOS
- Apple Safari 5.x on MacOS

## Maximum DHCP Lease Per Platform

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

**Table 1** *Maximum DHCP Lease Per Platform*

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

## Known Issues

### Controller-Datapath

**Table 2** Platform/Datapath Known Issues

Bug ID	Description
69277	<p><b>Symptom:</b> The Point-to-Point Tunneling Protocol (PPTP) VPN connection is lost when the user tries to connect to the PPTP server using Windows 7 client as the VPN client and switches to split-tunnel forwarding mode.</p> <p><b>Scenario:</b> This issue is seen in ArubaOS 6.1.3.2.</p> <p><b>Workaround:</b> None.</p>

### Remote Access Point

**Table 3** Remote Access Point Known Issues and Limitations

Bug ID	Description
63073	<p><b>Symptom:</b> Saving a backup of a virtual AP on a remote AP to flash memory may fail if the virtual AP has large ACLs with 500 ACE entries.</p> <p><b>Scenario:</b> This issue was observed on ArubaOS 6.1.3.0.</p> <p><b>Workaround:</b> Reduce the number of ACE entries on the ACLs before saving the backup.</p>

### Security

**Table 4** Security Known Issues and Limitations

Bug ID	Description
62099	<p><b>Symptom:</b> When connecting a client to an untrusted wired port, user entries appear in the <code>show user-table</code> output and are not aged out.</p> <p><b>Scenario:</b> This issue occurs when a client is connected to an untrusted wired port and this wired port is changed from untrusted to trusted.</p> <p><b>Workaround:</b> To avoid stale user entries from consuming user licenses on the controller, use the <code>aaa user delete</code> command to delete unwanted user names.</p>

### Syslog

**Table 5** Syslog Known Issue and Limitation

Bug ID	Description
62916	<p><b>Symptom:</b> Access points configured as air monitors (AM) may send debug log messages to the Syslog server, even if debug log messages are disabled.</p> <p><b>Scenario:</b> This can occur on any controller running ArubaOS 6.1.3.0 or later.</p> <p><b>Workaround:</b> None.</p>

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” on page 47
- “Important Points to Remember and Best Practices” on page 48
- “Memory Requirements” on page 48
- “Backing up Critical Data” on page 49
- “Upgrading in a Multi-Controller Network” on page 51
- “Upgrading to 6.2.x” on page 51
- “Downgrading” on page 55
- “Before You Call Technical Support” on page 57

## Upgrade Caveats

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

- If you have mesh APs in your deployment, and Airwave is configured, remove **mgmt-server** configuration before upgrade. Use the following commands to remove the configuration:

```
no mgmt-server type amp primary-server <mgmt_server_ip>
write memory
```

There is a mesh related stability issue in this release. By disabling **mgmt-server** configuration, you will not be able to use Airwave to manage your network

- Before upgrading to ArubaOS 6.2, you must remove any **phonehome smtp** configuration. Use the following commands to remove the configuration:

```
no phonehome smtp
write memory
```

Once your upgrade is complete, add **phonehome smtp** back to your configuration.

- ArubaOS 6.2.x is supported only on the newer MIPS controllers (7200 Series, M3, 3200XM, 3400, 3600, and 600 Series).

Legacy PPC controllers (200, 800, 2400, SC1 and SC2) and 3200 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 51.)

- User Idle Timeout behavior has changed in ArubaOS 6.2. For more information, see “User Idle Timeout Behavior Change” on page 20.

- 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.

## 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. Please verify the state of your network by answering the following questions.
  - How many APs are assigned to each controller? Verify this information by navigating to the **Monitoring > Network All Access Points** section of the WebUI, or by issuing the **show ap active** and **show ap database** CLI commands.
  - How are those APs discovering the controller (DNS, DHCP Option, Broadcast)?
  - What version of ArubaOS is currently on the controller?
  - Are all controllers in a master-local cluster running the same version of software?
  - Which services are used on the controllers (employee wireless, guest access, remote AP, wireless voice)?
- Resolve any existing issues (consistent or intermittent) before you upgrade.
- If possible, use FTP to load software images to the controller. FTP is faster than TFTP and offers more resilience over slow links. If you must use TFTP, ensure the TFTP server can send over 30 MB of data.
- Always upgrade the non-boot partition first. If problems occur during the upgrade, you can restore the flash, and switch back to the boot partition. Upgrading the non-boot partition gives you a smoother downgrade path should it be required.
- Before you upgrade to ArubaOS 6.2, 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.



CAUTION

---

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 49 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 49 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 49 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
```

```
Please wait while we tar relevant files from flash...  
Please 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 49](#).



---

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. 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 48](#)

---

### 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.

- 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 versions 6.0.0.0 or 6.0.0.1, download the latest version of ArubaOS 6.0.1.x.

Follow [step 2–step 11](#) of the procedure described in [“Upgrading From a Recent version of ArubaOS” on page 51](#) to install the interim version of ArubaOS, then repeat [step 1–step 11](#) of the procedure to download and install ArubaOS 6.2.

### Upgrading From a Recent version of ArubaOS

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

- 6.0.1.x or later
- 5.0.3.1 or later (If you are running ArubaOS 5.0.3.1 or the latest 5.0.x.x, review [“Upgrading With RAP-5 and RAP-5WN APs” on page 52](#) before proceeding further.)
- 3.4.4.1 or later

Install the ArubaOS 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 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 49](#) 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 52](#). 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 *m*, 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 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 48](#)

---

## 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.

- 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 versions 6.0.0.0 or 6.0.0.1, download the latest version of ArubaOS 6.0.1.x.

Follow [step 2–step 7](#) of the procedure described in [“Upgrading From a Recent version of ArubaOS” on page 53](#) to install the interim version of ArubaOS, then repeat [step 1–step 7](#) of the procedure to download and install ArubaOS 6.2.

## Upgrading From a Recent version of ArubaOS

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

- 6.0.1.x or later
- 5.0.3.1 or later. (If you are running ArubaOS 5.0.3.1 or the latest 5.0.x.x, review [“Upgrading With RAP-5 and RAP-5WN APs” on page 52](#) before proceeding further.)
- 3.4.4.1 or later

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 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/hal)  
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/hal)**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>
```



---

The USB option is only available on the 7200 Series controllers.

---

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

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

```
-----  
Partition           : 0:1 (/dev/hal) **Default boot**  
Software Version    : ArubaOS 6.2 (Digitally Signed - Production Build)  
Build number        : 29381  
Label               : 29381  
Built on            : Fri Sept 28 00:03:14 PDT 2012  
-----
```

```
Partition           : 0:1 (/dev/hal)  
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 49](#) 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 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 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 49](#).
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 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, the changes do not appear in RF Plan in the downgraded ArubaOS version.
- If you installed any certificates while running ArubaOS 6.2, 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 image:

```
#show image version
-----
Partition           : 0:1 (/dev/hal)
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 (Digitally Signed - Production Build)
Build number        : 28864
Built on            : 2012-12-04 2:11:59 PST 2012
```

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, please follow these steps:

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



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



---

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



---

Beginning in ArubaOS 6.2, the 651 controller's internal AP is disabled. Additionally, upon upgrade, the 651 will appear as 650-1 and the 651-8 will appear as 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, please 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
```

```
Please wait while we tar relevant files from flash...
```

```
Please 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



CAUTION

---

Before attempting upgrade any of your controllers, it is recommended that you read the “[Upgrade Procedures](#)” on [page 47](#).

---



NOTE

---

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 1** provides a brief overview of the steps required to upgrade to ArubaOS 6.1. For more detailed information and procedures on upgrading, see “[Upgrade Procedures](#)” on [page 47](#).

**Table 1** ArubaOS 6.2 Upgrade Path Overview

Version	Step 1	Step 2
3.4.x	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
5.0.3.x	Upgrade to the latest 5.0.4.x	Upgrade to 6.2

**Table 1** ArubaOS 6.2 Upgrade Path Overview (Continued)

Version	Step 1	Step 2
6.0.x	Upgrade to the latest 6.0.2.x	Upgrade to 6.2
6.1.x	Upgrade to 6.1.3.5	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**.



---

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.

---

5. When the transfer has been completed successfully, you will receive a new set of activation keys.

## Installing Your New Controller

For instructions and additional information about installing your 7200 Series controller, please 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 this document, visit [support.arubanetworks.com](http://support.arubanetworks.com) and click the **Documentation** tab.



---

After installing your 7200 Series, verify that it is running the latest version of ArubaOS 6.2. If not, it is recommended that you upgrade your controller. See “[Upgrade Procedures](#)” on page 47.

---

## Installing Backed Up Controller Data



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 your 7200 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.



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
```



Do not reboot your controller before installing licenses.



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 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 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 60](#).