

# ArubaOS 6.4.4.3



Release Notes

## **Copyright Information**

© Copyright 2016 Hewlett Packard Enterprise Development LP.

## **Open Source Code**

This product includes code licensed under the GNU General Public License, the GNU Lesser General Public License, and/or certain other open source licenses. A complete machine-readable copy of the source code corresponding to such code is available upon request. This offer is valid to anyone in receipt of this information and shall expire three years following the date of the final distribution of this product version by Hewlett-Packard Company. To obtain such source code, send a check or money order in the amount of US \$10.00 to:

Hewlett-Packard Company

Attn: General Counsel

3000 Hanover Street

Palo Alto, CA 94304

USA

Please specify the product and version for which you are requesting source code. You may also request a copy of this source code free of charge at [dl-gplquery@arubanetworks.com](mailto:dl-gplquery@arubanetworks.com).

---

<b>Contents</b> .....	<b>3</b>
<b>Release Overview</b> .....	<b>4</b>
Chapter Overview .....	4
Important Points to Remember .....	4
Supported Browsers .....	5
Contacting Support .....	6
<b>New Features</b> .....	<b>7</b>
<b>Regulatory Updates</b> .....	<b>10</b>
<b>Resolved Issues</b> .....	<b>11</b>
<b>Known Issues and Limitations</b> .....	<b>16</b>
<b>Upgrade Procedure</b> .....	<b>23</b>
Upgrade Caveats .....	23
GRE Tunnel-Type Requirements .....	24
Important Points to Remember and Best Practices .....	24
Memory Requirements .....	25
Backing up Critical Data .....	25
Upgrading in a Multicontroller Network .....	27
Installing the FIPS Version of ArubaOS 6.4.4.3 .....	27
Upgrading to ArubaOS 6.4.4.3 .....	27
Downgrading .....	31
Before You Call Technical Support .....	33

ArubaOS 6.4.4.3 is a software patch release that includes new features and enhancements along with fixes to issues identified in previous releases.

### Chapter Overview

- [New Features on page 7](#) provides a description of features and enhancements introduced in this release.
- [Regulatory Updates on page 10](#) lists the regulatory updates introduced in this release.
- [Resolved Issues on page 11](#) lists and describes the issues resolved in this release.
- [Known Issues and Limitations on page 16](#) lists and describes the known and outstanding issues identified in this release.
- [Upgrade Procedure on page 23](#) describes the procedures for upgrading a controller to this release.

### Important Points to Remember

If you modify the configuration of an AP, those changes take effect immediately; you do not need to reboot the controller or the AP for the changes to affect the current running configuration. Certain commands, however, automatically force the AP radio to restart.

#### AirGroup

##### Support for Wired Users

Starting from ArubaOS 6.4.3.0, AirGroup does not support wired users.

##### AP Settings Triggering a Radio Restart

Changing the following settings triggers the radio to restart on the AP-200 Series, AP-205H, AP-210 Series, AP-220 Series, AP-270 Series, and AP-320 Series access points. When the radio restarts, wireless services will be briefly interrupted. Clients will automatically reconnect to the network when the radio is again up and running.

**Table 1: Profile Settings in ArubaOS 6.4.x**

Profile	Settings
802.11a/802.11g Radio Profile	<ul style="list-style-type: none"> <li>• Channel</li> <li>• Enable Channel Switch Announcement (CSA)</li> <li>• CSA Count</li> <li>• High throughput enable (radio)</li> <li>• Very high throughput enable (radio)</li> <li>• TurboQAM enable</li> <li>• Maximum distance (outdoor mesh setting)</li> <li>• Transmit EIRP</li> <li>• Advertise 802.11h Capabilities</li> <li>• Beacon Period/Beacon Regulate</li> <li>• Advertise 802.11d Capabilities</li> </ul>
Virtual AP Profile	<ul style="list-style-type: none"> <li>• Virtual AP enable</li> <li>• Forward Mode</li> <li>• Remote-AP operation</li> </ul>
SSID Profile	<ul style="list-style-type: none"> <li>• ESSID</li> <li>• Encryption</li> <li>• Enable Management Frame Protection</li> <li>• Require Management Frame Protection</li> <li>• Multiple Tx Replay Counters</li> <li>• Strict Spectralink Voice Protocol (SVP)</li> <li>• Wireless Multimedia (WMM) settings <ul style="list-style-type: none"> <li>■ Wireless Multimedia (WMM)</li> <li>■ Wireless Multimedia U-APSD (WMM-UAPSD) Powersave</li> <li>■ WMM TSPEC Min Inactivity Interval</li> <li>■ Override DSCP mappings for WMM clients</li> <li>■ DSCP mapping for WMM voice AC</li> <li>■ DSCP mapping for WMM video AC</li> <li>■ DSCP mapping for WMM best-effort AC</li> <li>■ DSCP mapping for WMM background AC</li> </ul> </li> </ul>
High-throughput SSID Profile	<ul style="list-style-type: none"> <li>• High throughput enable (SSID)</li> <li>• 40 MHz channel usage</li> <li>• Very High throughput enable (SSID)</li> <li>• 80 MHz channel usage (VHT)</li> </ul>
802.11r Profile	<ul style="list-style-type: none"> <li>• Advertise 802.11r Capability</li> <li>• 802.11r Mobility Domain ID</li> <li>• 802.11r R1 Key Duration</li> <li>• key-assignment (CLI only)</li> </ul>
Hotspot 2.0 Profile	<ul style="list-style-type: none"> <li>• Advertise Hotspot 2.0 Capability</li> <li>• RADIUS Chargeable User Identity (RFC4372)</li> <li>• RADIUS Location Data (RFC5580)</li> </ul>

## Supported Browsers

The following browsers are officially supported for use with ArubaOS 6.4.4.3 Web User Interface (WebUI):

- Microsoft Internet Explorer 10.x and 11 on Windows 7 and Windows 8
- Mozilla Firefox 23 or later on Windows Vista, Windows 7, Windows 8, and Mac OS
- Apple Safari 5.1.7 or later on Mac OS

## Contacting Support

**Table 2:** *Contact Information*

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>
Airheads Social Forums and Knowledge Base	<a href="http://community.arubanetworks.com/">http://community.arubanetworks.com/</a>
North American Telephone	1-800-943-4526 (Toll Free) 1-408-754-1200
International Telephone	<a href="http://www.arubanetworks.com/support-services/contact-support/">http://www.arubanetworks.com/support-services/contact-support/</a>
Software Licensing Site	<a href="https://licensing.arubanetworks.com/">https://licensing.arubanetworks.com/</a>
End-of-life Information	<a href="http://www.arubanetworks.com/support-services/end-of-life/">http://www.arubanetworks.com/support-services/end-of-life/</a>
Security Incident Response Team (SIRT)	<a href="http://www.arubanetworks.com/support-services/security-bulletins/">http://www.arubanetworks.com/support-services/security-bulletins/</a>
<b>Support Email Addresses</b>	
Security Incident Response Team (SIRT)	<a href="mailto:sirt@arubanetworks.com">sirt@arubanetworks.com</a>

This chapter describes the new features and/or enhancements introduced in this release. For more information about these features, refer to the *ArubaOS 6.4.4.x User Guide*.

### AP-Wireless

#### VHT Bandwidth Signaling

Starting from ArubaOS 6.4.4.3, the Very High Throughput (VHT) bandwidth signaling can be enabled or disabled. This parameter is supported only on AP-320 Series access points. This setting appears in the controller CLI only.

#### In the CLI

A new **VHT Bandwidth Signaling** parameter is introduced in the **rf ht-radio-profile** command. By default, the **VHT Bandwidth Signaling** parameter is disabled for better interoperability with older 802.11ac chipsets which do not respond to Ready To Send (RTS) with bandwidth signaling.

#### rf ht-radio-profile

The following new parameter is introduced in the **rf ht-radio-profile** command:

**Table 3:** VHT Bandwidth Signaling

Parameter	Description	Range	Default
VHT Bandwidth Signaling	Enable or Disable VHT bandwidth signaling (802.11ac) RTS for better interoperability.  This parameter is supported on AP-320 Series access points only	Enabled/Disabled	Disabled

To enable VHT bandwidth signaling, execute the following commands in the config mode:

```
(host) (config) #rf ht-radio-profile <profile>
(host) (High-throughput radio profile <profile>) #vht-bw-signaling
```

To disable VHT bandwidth signaling, execute the following commands in the config mode:

```
(host) (config) #rf ht-radio-profile <profile>
(host) (High-throughput radio profile <profile>) #no vht-bw-signaling
```

To verify the status of VHT bandwidth signaling, execute the **show rf ht-radio-profile** command.

#### show rf dot11a-radio-profile

The following new parameter is introduced as part of the **show rf dot11a-radio-profile** command:

**Table 4:** Status of VHT Bandwidth Signaling

Parameter	Description
VHT Bandwidth Signaling	Displays the status of VHT bandwidth signaling

## Base OS Security

### OCSP Client Support for RAP

Starting from ArubaOS 6.4.4.3, Remote Access Points (RAPs) read the Authority Information Access (AIA) field of a server certificate. If the RAPs are configured to check revocation, the RAPs use the AIA field to query an Online Certificate Status Protocol (OCSP) responder. This allows a RAP that is provisioned with custom certificate to determine if the server-side certificate is revoked.



---

This change is applicable only to FIPS images.

---

To support OCSP client for RAP, two parameters **ocsp\_default** and **cert\_dn** are introduced.

#### OCSP Default

The OCSP default is used during connection failure/response timeout with OCSP responder. Configure the parameter **ocsp\_default** through the controller AP provisioning CLI, RAP console page, or AP serial console.

If the parameter **ocsp\_default** is set to 0 (default accept) and the certificate status is unknown, the server certificate is considered valid and the RAP comes up. If the parameter **ocsp\_default** is set to 1 (default deny) and the certificate status is unknown, the server certificate is considered revoked and the RAP does not come up.

By default, OCSP default is set to 0 (default accept)

#### In the CLI

```
(host) (config) #provision-ap
(host) (AP provisioning) #ocsp-default ?
<ocsp-default>          ocspp_default is [0:OCSP_ACCEPT 1:OCSP_DENY]
```

#### In the RAP Console

1. Navigate to **Certificates > OCSP Default**.
2. Select the desired OCSP default.
3. Click **Save OCSP**.

#### In the AP Serial Console

Execute either of the following commands to choose between the desired OCSP default:

```
setenv ocsp_default 0
setenv ocsp_default 1
```

#### Certificate Domain Name

RAP is allowed to validate the identity of the controller by provisioning the certificate domain name. Only common name string value or wildcard of the server certificate is allowed.

The RAP refuses to connect with any controller if the parameter **cert\_DN** is provisioned in AP environment and does not have a matching identity payload.

Certificate domain name supports wildcard (only \* and . characters) when provisioning the parameter **cert\_DN** to match with the common name string in ID payload. For example, provision "all certs that match the pattern of \*.rap.arubanetworks.com are trusted".

Common name matching is applied only if the parameter **cert\_DN** is configured for RAP. Otherwise, the RAPs come up without validating the controller using a common name.

By default, if the parameter **cert\_DN** is not configured, the common name matching is skipped.

#### In the CLI



```
(host) (AP provisioning) #cert-?
cert-DN          The Server Certificate Common Name for Identity
```

### In the RAP Console

1. Navigate to **Certificates > Cert DN**.
2. Enter the desired certificate domain name.
3. Click **Save ServerCert CN**.

### In the AP Serial Console

Execute the following command to select a certificate domain name:

```
setenv cert_DN CN=AK0010160::00:0b:86:6d:21:f4
```

Other example: \*.rap.arubanetworks.com;controller.abc.com;

## Captive Portal

### Web Portal Authentication

The **exclude-http-security-headers** parameter is introduced in the **web-server profile** command to exclude security headers from HTTP response.



---

On enabling this parameter, the **X-Frame-Options: SAMEORIGIN** is excluded from the HTTP response header. This configuration is generally not recommended, as the client browser may be vulnerable to a [clickjacking](#) attack. This option should be enabled only when an externally hosted Captive Portal is running within an iframe.

---

This chapter describes the regulatory update in this release.



---

Contact your local Aruba sales representative about device availability and support for your country.

---

Periodic regulatory changes may require modifications to the list of channels supported by an AP. For a complete list of channels supported by an AP using a specific country domain, access the controller Command Line Interface (CLI) and execute the **show ap allowed-channels country-code <country-code> ap-type <ap-model>** command.

The following Downloadable Regulatory Table (DRT) file versions are supported in ArubaOS 6.4.4.3:

- DRT-1.0\_52699

For a complete list of countries certified with different AP models, refer to the respective DRT release notes at [support.arubanetworks.com](http://support.arubanetworks.com).

This chapter describes the issues resolved in this release.



This release of ArubaOS resolved specific Network Time Protocol (NTP) vulnerabilities. For details, refer to issue 127194.

### AP-Platform

**Table 5:** *AP-Platform Resolved Issues*

Bug ID	Description
126145 128293 128294 128295 128343 128369	<p><b>Symptom:</b> 802.11ac-capable access points broadcasted the maximum Equivalent Isotropically Radiated Power (EIRP) values instead of the ARM-configured values after each failover. This issue is resolved by implementing changes that allow the access points to broadcast the ARM-configured values after each failover.</p> <p><b>Scenario:</b> This issue occurred during VRRP, master-to-local and local-to-master failover except High Availability (HA) failover. This issue was observed in AP-200 Series, AP-210 Series, and AP-220 Series access points. This issue was observed after a controller was upgraded to ArubaOS 6.4.2.11 or later versions of ArubaOS.</p> <p><b>Platform:</b> AP-200 Series, AP-210 Series, and AP-220 Series access points.</p> <p><b>Reported Version:</b> ArubaOS 6.4.2.12.</p>
128461	<p><b>Symptom:</b> AP-103H access points crashed with the error message <b>athr_gmac_rcv_packets:1744: assertion failed</b>. This issue is resolved by emptying a pending received tasklet before clearing an internal flag.</p> <p><b>Scenario:</b> This issue occurred when a pending received tasklet was not emptied before clearing an internal flag. This issue was observed in AP-103H access points connected to controllers running ArubaOS 6.4.2.5.</p> <p><b>Platform:</b> AP-103H access points.</p> <p><b>Reported Version:</b> ArubaOS 6.4.2.5.</p>

## AP-Wireless

**Table 6:** AP-Wireless Resolved Issues

Bug ID	Description
124323	<p><b>Symptom:</b> The 802.11k neighbor table did not show any access points. This issue is resolved by enhancing the access point search to not have any dependency on the Virtual Access Point (VAP) order and by not checking if the neighbors of an access point are enabled or disabled.</p> <p><b>Scenario:</b> This issue occurred when multi-VAP was configured in controllers running ArubaOS 6.3.1.5.</p> <p><b>Platform:</b> All platforms.</p> <p><b>Reported Version:</b> ArubaOS 6.3.1.5.</p>
124572	<p><b>Symptom:</b> Intel 7260 802.11ac clients that were connected to AP-135 access points reached the default threshold limit of transmission retries. This increased the jitter when voice calls were made. This issue is resolved by maintaining the jitter average value within an acceptable threshold of 20 ms.</p> <p><b>Scenario:</b> This issue occurred when sending data to Intel 7260 802.11ac clients downstream. This issue was observed in AP-135 access points connected to controllers running ArubaOS 6.4.2.6.</p> <p><b>Platform:</b> AP-135 access points.</p> <p><b>Reported Version:</b> ArubaOS 6.4.2.6.</p>
127450	<p><b>Symptom:</b> AP-325 access points displayed the error message <b>Unable to handle kernel NULL pointer dereference at virtual address</b>. This issue is resolved by avoiding data NULL invalidation in the cache.</p> <p><b>Scenario:</b> This issue was observed in AP-325 access points connected to controllers running ArubaOS 6.4.4.1.</p> <p><b>Platform:</b> AP-325 access points.</p> <p><b>Reported Version:</b> ArubaOS 6.4.4.1.</p>
127460	<p><b>Symptom:</b> Multiple RADAR detections were observed on 80 MHz Dynamic Frequency Selection (DFS) channels in JP3 CC. This issue is resolved by improving the detection algorithm for specific type of RADAR pulse.</p> <p><b>Scenario:</b> This issue was observed in controllers running ArubaOS 6.4.3.3.</p> <p><b>Platform:</b> All platforms.</p> <p><b>Reported Version:</b> ArubaOS 6.4.3.3.</p>
127946	<p><b>Symptom:</b> AP-325 access points rebooted with the reason <b>Reboot caused by kernel panic: Rebooting the AP because of FW ASSERT reason</b>. This issue is resolved by adding checks on the host side before sending WMI events.</p> <p><b>Scenario:</b> This issue occurred when clients associated with access points and the host sent WMI event with incorrect Network Switching Subsystem (NSS) number. This issue was observed in AP-325 access points connected to controllers running ArubaOS 6.4.4.1.</p> <p><b>Platform:</b> AP-325 access points.</p> <p><b>Reported Version:</b> ArubaOS 6.4.4.1.</p>

## AirGroup

**Table 7:** *AirGroup Resolved Issues*

Bug ID	Description
123561	<p><b>Symptom:</b> AP-135 access points displayed the country code for MacOS users in Nigeria as <b>NA</b> instead of <b>NG</b>. This issue is resolved by implementing changes that display the correct country code.</p> <p><b>Scenario:</b> This issue occurred when 802.11d and 802.11h were enabled in AP-135 access points and AP-135 access points were provisioned with a regulatory domain code.</p> <p><b>Platform:</b> All platforms.</p> <p><b>Reported Version:</b> ArubaOS 6.4.2.6.</p>
126433	<p><b>Symptom:</b> The multicast Domain Name System (mDNS) process crashed in the controller. This issue is resolved by correcting the timer ID immediately after a user is deleted.</p> <p><b>Scenario:</b> This issue occurred when a shared user-list of an AirGroup policy was modified in ClearPass Policy Manager (CPPM) from one user to another and the earlier user was deleted within 5 seconds after changing the policy. This issue was observed in controllers running ArubaOS 6.4.2.10.</p> <p><b>Platform:</b> All platforms.</p> <p><b>Reported Version:</b> ArubaOS 6.4.2.10.</p>
126926	<p><b>Symptom:</b> Chromecast applications did not work when AirGroup was enabled in a controller. This issue is resolved by sending the wildcard query for unique service IDs that are not part of the allowall service.</p> <p><b>Scenario:</b> This issue occurred because of a change in the Google cast support to application queries for Chromecast. This issue was observed in controllers running ArubaOS 6.4.x or later versions of ArubaOS.</p> <p><b>Platform:</b> All platforms.</p> <p><b>Reported Version:</b> ArubaOS 6.4.2.10.</p>

## Base OS Security

**Table 8:** *Base OS Security Resolved Issues*

Bug ID	Description
128460	<p><b>Symptom:</b> Users were not assigned the correct role-based VLAN after a full 802.1X authentication when the role was changed by Change of Authorization (CoA). This issue is resolved by allowing free role transitions to or from CoA or ESI roles without looking for priorities.</p> <p><b>Scenario:</b> This issue occurred because of adherence to priorities when changing roles. This issue was observed in controllers running ArubaOS 6.4.3.4.</p> <p><b>Platform:</b> All platforms.</p> <p><b>Reported Version:</b> ArubaOS 6.4.3.4.</p>

## Captive Portal

**Table 9:** *Captive Portal Resolved Issues*

Bug ID	Description
115095	<p><b>Symptom:</b> The slash character was added at the end of a redirection URL after external Captive Portal (CP) authentication. This issue is resolved by removing the extra slash character at the end of the redirected URL.</p> <p><b>Scenario:</b> This issue was observed in controllers running ArubaOS 6.4.2.5 when clients performed external CP authentication.</p> <p><b>Platform:</b> All platforms.</p> <p><b>Reported Version:</b> ArubaOS 6.4.2.5.</p>

## Controller-Datapath

**Table 10:** *Controller-Datapath Resolved Issues*

Bug ID	Description
122939	<p><b>Symptom:</b> AP-200 Series access points experienced amplified packet loss during voice calls. This issue is resolved by changing the hybrid-mode spectrum monitoring to be voice-aware.</p> <p><b>Scenario:</b> This issue was observed when spectrum monitoring was enabled in AP-200 Series access points connected to controllers running ArubaOS 6.4.2.x or ArubaOS 6.4.3.x.</p> <p><b>Platform:</b> AP-200 Series access points.</p> <p><b>Reported Version:</b> ArubaOS 6.4.2.5.</p>
126736	<p><b>Symptom:</b> Home Agent/Foreign Agent (HA/FA) configuration did not work with anchor table and clients that sent Dynamic Host Configuration Protocol (DHCP) discover with unicast flag. This issue is resolved by making an exception for Address Resolution Protocol/Dynamic Host Configuration Protocol (ARP/DHCP) flood optimization when the mobility feature is enabled.</p> <p><b>Scenario:</b> This issue was observed when the mobility feature was used with static IP and DHCP clients. This issue was observed in controllers running ArubaOS 6.4.3.4.</p> <p><b>Platform:</b> All platforms.</p> <p><b>Reported Version:</b> ArubaOS 6.4.3.4.</p>
126749	<p><b>Symptom:</b> Although <b>no firewall prohibit-ip-spoofing</b> was configured, IP spoofing packets from untrusted ports were dropped. This issue is resolved by adding checks that do not drop IP spoofing packets.</p> <p><b>Scenario:</b> This issue was observed in controllers running ArubaOS 6.4.3.2.</p> <p><b>Platform:</b> All platforms.</p> <p><b>Reported Version:</b> ArubaOS 6.4.3.2.</p>
127937	<p><b>Symptom:</b> A controller crashed because of datapath timeout after upgrading the controller to ArubaOS 6.4.2.13. This issue is resolved by optimizing the inactive-user timeout logic.</p> <p><b>Scenario:</b> This issue occurred because of fragmented untrusted traffic coming from a client for an active session when the client user entry was not created in the controller. This issue was observed after controllers were upgraded to ArubaOS 6.4.2.13.</p> <p><b>Platform:</b> All platforms.</p> <p><b>Reported Version:</b> ArubaOS 6.4.2.13.</p>

## Controller-Platform

**Table 11:** *Controller-Platform Resolved Issues*

Bug ID	Description
127194	<p><b>Symptom:</b> A newer version of the Network Time Protocol (NTP) program was not available with ArubaOS. This issue is resolved by upgrading the version of the NTP program to 4.2.8.p.4 which includes fixes to CVE-2015-7704, CVE-2015-7705, and CVE-2015-7871.</p> <p><b>Scenario:</b> This issue was observed in controllers running ArubaOS 6.4.4.2.</p> <p><b>Platform:</b> All platforms.</p> <p><b>Reported Version:</b> ArubaOS 6.4.4.2.</p>

## Distributed Data Store

**Table 12:** *Distributed Data Store Resolved Issues*

Bug ID	Description
125225 127492	<p><b>Symptom:</b> The CPU utilization was high for the Distributed Data Store (DDS) module. This issue is resolved by optimizing the DDS module.</p> <p><b>Scenario:</b> This issue was observed in controllers running ArubaOS 6.4.2.4.</p> <p><b>Platform:</b> All platforms.</p> <p><b>Reported Version:</b> ArubaOS 6.4.2.4.</p>

## IPv6

**Table 13:** *IPv6 Resolved Issues*

Bug ID	Description
125261	<p><b>Symptom:</b> High datapath utilization was observed in a controller. This issue is resolved by implementing changes to restrict the flooding of unsolicited Neighbor Advertisement (NA) to Wi-Fi tunnels if the ingress is a Wi-Fi tunnel or the source is not a router.</p> <p><b>Scenario:</b> This issue occurred when a network was flooded with unsolicited NA packets. This issue was observed in controllers running ArubaOS 6.4.3.3.</p> <p><b>Platform:</b> All platforms.</p> <p><b>Reported Version:</b> ArubaOS 6.4.3.3.</p>

## Mesh

**Table 14:** *Mesh Resolved Issues*

Bug ID	Description
124682 126989	<p><b>Symptom:</b> Broadcast traffic from a switch to the Ethernet 0 port of a mesh point was sent back. This issue is resolved by removing eth0 from bond0 interface.</p> <p><b>Scenario:</b> This issue was observed when a client or switch connected to the Ethernet 0 port of a mesh point relayed broadcast traffic.</p> <p><b>Platform:</b> All platforms.</p> <p><b>Reported Version:</b> ArubaOS 6.4.3.2.</p>

This chapter describes the known issues and limitations identified in this release.



---

If there is any specific bug that is not documented in this section, contact Aruba Technical Support with your case number.

---

### Support for AP-320 Series Access Points

The following features are not supported in AP-320 Series access points:

- Enterprise Mesh
- 802.11k
- Turbo QAM
- Modem Support
- Radio Frequency Test (RFT)

### AP-Datapath

**Table 15:** *AP-Datapath Known Issues*

Bug ID	Description
126237	<p><b>Symptom:</b> Clients fail to get IP address from random APs, resulting in traffic failure.</p> <p><b>Scenario:</b> This issue occurs when a split-tunnel Virtual Access Point (VAP) is added with the BS flag, which indicates that the VAP is in both bridge and split-tunnel forwarding modes. This results in client failing to get an IP address. This issue is observed in controllers running ArubaOS 6.4.2.11 or later versions of ArubaOS.</p> <p><b>Platform:</b> All platforms.</p> <p><b>Reported Version:</b> ArubaOS 6.4.2.12.</p> <p><b>Workaround:</b> None.</p>



## AP-Platform

**Table 16:** AP-Platform Known Issues

Bug ID	Description
121629 124058	<p><b>Symptom:</b> AP-125 access points stop responding and reboot. The log files for the event list the reason as <b>NMI watchdog interrupt</b>.</p> <p><b>Scenario:</b> This issue is observed in AP-125 access points connected to controllers running ArubaOS 6.4.2.6.</p> <p><b>Platform:</b> AP-125 access points.</p> <p><b>Reported Version:</b> ArubaOS 6.4.2.6.</p> <p><b>Workaround:</b> None.</p>
123458	<p><b>Symptom:</b> Access points do not send network capabilities in Link Layer Discovery Protocol-Media Endpoint Discovery (LLDP-MED) information.</p> <p><b>Scenario:</b> When receiving LLDP-MED packet, access points add an entry to the neighbor list and update the LLDP-LED flag of the port. The access points send LLDP-LED information based on this flag. When the port is brought down, all port status including LLDP-MED flag are cleared and when the port is brought up, AP does not recover the LLDP-MED flag because the neighbor list exists. Hence, after shutdown/no shutdown of the port, the access point does not send network capabilities in LLDP-MED information. This issue is observed in AP-225 access points connected to controllers running ArubaOS 6.4.3.3.</p> <p><b>Platform:</b> AP-225 access points.</p> <p><b>Reported Version:</b> ArubaOS 6.4.3.3.</p> <p><b>Workaround:</b> None.</p>
124917 129757	<p><b>Symptom:</b> AP-205H access points crash and reboot.</p> <p><b>Scenario:</b> This issue is observed in AP-205H access points connected to controllers running ArubaOS 6.4.3.3.</p> <p><b>Platform:</b> AP-205H access points.</p> <p><b>Reported Version:</b> ArubaOS 6.4.3.3.</p> <p><b>Workaround:</b> None.</p>

## AP-Wireless

**Table 17:** AP-Wireless Known Issues

Bug ID	Description
126690	<p><b>Symptom:</b> Certain Dell Latitude laptops with Dell Wireless 1501 wireless adapter fail to obtain an IP address when associating with AP-220 Series access points.</p> <p><b>Scenario:</b> This issue occurs because of a wrong access point (AP) beacon. When High Throughput (HT) is disabled in <b>rf dot11g-radio-profile</b> and enabled in <b>rf ht-ssid-profile</b>, the AP beacon advertises HT IE and the Dell wireless 1501 wireless adapter fails to obtain an IP address. This issue is observed in AP-220 Series access points connected to controllers running ArubaOS 6.4.2.12.</p> <p><b>Platform:</b> AP-220 Series access points.</p> <p><b>Reported Version:</b> ArubaOS 6.4.2.14.</p> <p><b>Workaround:</b> None.</p>
127051	<p><b>Symptom:</b> AP-324 and AP-325 access points crash with the error message <b>Target ASSERT - 0x009AF80C - _HTC_PipeSendMsg (htc.c:1063)</b>.</p> <p><b>Scenario:</b> This issue is observed in AP-324 and AP-325 access points connected to controllers running ArubaOS 6.4.4.0.</p> <p><b>Platform:</b> AP-324 and AP-325 access points.</p> <p><b>Reported Version:</b> ArubaOS 6.4.4.0.</p> <p><b>Workaround:</b> None.</p>
127053 127111 127441 127967	<p><b>Symptom:</b> AP-325 access points crash with the error message <b>FW assert - wlan_scan_autochan_event_handler</b>.</p> <p><b>Scenario:</b> This issue is observed in AP-325 access points connected to controllers running ArubaOS 6.4.4.1.</p> <p><b>Platform:</b> AP-325 access points.</p> <p><b>Reported Version:</b> ArubaOS 6.4.4.1.</p> <p><b>Workaround:</b> None.</p>

## AirGroup

**Table 18:** *AirGroup Known Issues*

Bug ID	Description
129223	<p><b>Symptom:</b> Clients fail to discover Amazon Fire TV even when AirGroup service is enabled in the controller.</p> <p><b>Scenario:</b> This issue occurs because the service ID is not listed under the AirGroup service in the controller. This issue is observed with Amazon Fire TV and controllers running ArubaOS 6.4.x.</p> <p><b>Platform:</b> All platforms.</p> <p><b>Reported Version:</b> ArubaOS 6.4.3.2.</p> <p><b>Workaround:</b> Execute the following commands to add the Amazon AirGroup service:</p> <pre>(host) (config) #airgroupservice AmazonTV (host) (config-airgroupservice) #id _amzn-wplay._tcp (host) (config-airgroupservice) #write memory</pre>
129646	<p><b>Symptom:</b> Unsolicited mDNS response is not sent correctly across controllers when the shared user list on the AirGroup server is modified in ClearPass Policy Manager (CPPM) policy.</p> <p><b>Scenario:</b> This issue is observed in controllers running ArubaOS 6.4.4.1.</p> <p><b>Platform:</b> All platforms.</p> <p><b>Reported Version:</b> ArubaOS 6.4.4.1.</p> <p><b>Workaround:</b> None.</p>
129649	<p><b>Symptom:</b> When AirGroup is enabled, the wildcard query is sent for subservices that are learned by allowall service.</p> <p><b>Scenario:</b> This issue is observed in controllers running ArubaOS 6.4.3.x and ArubaOS 6.4.4.x.</p> <p><b>Platform:</b> All platforms.</p> <p><b>Reported Version:</b> ArubaOS 6.4.4.3.</p> <p><b>Workaround:</b> Disable the AirGroup allowall service.</p>
129652	<p><b>Symptom:</b> Duplicate subrecords are added under the allowall service for subrecord response packet.</p> <p><b>Scenario:</b> This issue is observed in controllers running ArubaOS 6.4.3.x and ArubaOS 6.4.4.x.</p> <p><b>Platform:</b> All platforms.</p> <p><b>Reported Version:</b> ArubaOS 6.4.4.3.</p> <p><b>Workaround:</b> Disable the AirGroup allowall service.</p>

## Base OS Security

**Table 19:** Base OS Security Known Issues

Bug ID	Description
125232	<p><b>Symptom:</b> User-role and Access Control List (ACL)-related configurations are lost when a controller reboots.</p> <p><b>Scenario:</b> This issue occurs when controllers with large time-range configurations reboot and user-role and ACL configurations are not saved. This issue is observed in controllers running ArubaOS 6.4.2.8.</p> <p><b>Platform:</b> All platforms.</p> <p><b>Reported Version:</b> ArubaOS 6.4.2.8.</p> <p><b>Workaround:</b> Reduce the range of the time-range command in the CLI.</p>
126713	<p><b>Symptom:</b> A controller continues to forward authentication requests to a server that is out of service.</p> <p><b>Scenario:</b> This issue occurs when an authentication server goes out of service after authenticating a user and the same server is reused for authentication in the next instance. The authentication server stored in user context is reused even if the server is out of service. This issue is observed in controllers running ArubaOS 6.4.2.5.</p> <p><b>Platform:</b> All platforms.</p> <p><b>Reported Version:</b> ArubaOS 6.4.2.5.</p> <p><b>Workaround:</b> None.</p>
127421	<p><b>Symptom:</b> The authentication module crashes in a master controller.</p> <p><b>Scenario:</b> This issue is observed in master controllers running ArubaOS 6.4.3.1.</p> <p><b>Platform:</b> All platforms.</p> <p><b>Reported Version:</b> ArubaOS 6.4.3.1.</p> <p><b>Workaround:</b> None.</p>
127971	<p><b>Symptom:</b> When user authentication fails, the controller does not update the syslog entry with the authentication method used.</p> <p><b>Scenario:</b> This issue occurs when replacing the old log entry 522042 with 522275. However, the new log entry does not include the authentication method. This issue is observed in controllers running ArubaOS 6.4.x.</p> <p><b>Platform:</b> All platforms.</p> <p><b>Reported Version:</b> ArubaOS 6.4.2.12.</p> <p><b>Workaround:</b> None.</p>
128466	<p><b>Symptom:</b> A controller displays the error message <b>Invalid TLS version in authentication trace buffer</b> after uploading a new certificate for Extensible Authentication Protocol-Protected Extensible Authentication Protocol (EAP-PEAP) authentication. This results in user authentication failure.</p> <p><b>Scenario:</b> This issue occurs when a client finishes Transport Layer Security (TLS) for 802.1X authentication. The issue occurs when decrypting the pre-master secret due to a bug in parsing the private key. This issue is observed in controllers running ArubaOS 6.4.2.x.</p> <p><b>Platform:</b> All platforms.</p> <p><b>Reported Version:</b> ArubaOS 6.4.2.12.</p> <p><b>Workaround:</b> None.</p>
128800	<p><b>Symptom:</b> User idle timeout from the Captive Portal (CP) profile does not override the default user idle timeout. Default values take effect to idle timeout an idle user.</p> <p><b>Scenario:</b> This issue is observed in controllers running ArubaOS 6.4.3.4.</p> <p><b>Platform:</b> All platforms.</p> <p><b>Reported Version:</b> ArubaOS 6.4.3.4.</p> <p><b>Workaround:</b> None.</p>

## Controller-Datapath

**Table 20:** *Controller-Datapath Known Issues*

Bug ID	Description
124286 129845	<b>Symptom:</b> The datapath module crashes in a controller. <b>Scenario:</b> This issue is observed in controllers running ArubaOS 6.4.3.1. <b>Platform:</b> All platforms. <b>Reported Version:</b> ArubaOS 6.4.3.1. <b>Workaround:</b> None.

## Controller-Platform

**Table 21:** *Controller-Platform Known Issues*

Bug ID	Description
123577	<b>Symptom:</b> After upgrading a controller to ArubaOS 6.4.2.9, the Virtual Router Redundancy Protocol (VRRP) link is unstable at random times. The log files indicate a delay of few seconds in receiving the Link Aggregation Control Protocol (LACP) keepalives. <b>Scenario:</b> This issue occurs when a controller is configured with 1 second of master advertisement interval. This issue is observed in controllers running ArubaOS 6.4.2.9 in a master-local topology. <b>Platform:</b> All platforms. <b>Reported Version:</b> ArubaOS 6.4.2.9. <b>Workaround:</b> Set the master advertisement interval to a longer duration using the <code>vrrp &lt;id&gt; advertise &lt;interval&gt;</code> command in the CLI.

## Remote AP

**Table 22:** *Remote AP Known Issues*

Bug ID	Description
127848	<b>Symptom:</b> Access points do not reconnect their Point-to-Point Protocol over Ethernet (PPPoE) to the backup-LMS when the LMS is not available. <b>Scenario:</b> This issue is observed in AP-205 and AP-274 access points connected to controllers running ArubaOS 6.4.4.0. <b>Platform:</b> AP-205 and AP-274 access points. <b>Reported Version:</b> ArubaOS 6.4.4.0. <b>Workaround:</b> None.

## Station Management

**Table 23:** *Station Management Known Issues*

Bug ID	Description
124275	<p><b>Symptom:</b> All clients continue to obtain IP addresses from the same VLAN even though a RADIUS server Vendor Specific Attribute (VSA) specifies a Virtual Local Area Network (VLAN) pool with multiple VLANs.</p> <p><b>Scenario:</b> This issue occurs when a RADIUS server VSA overrides the Virtual AP VLAN(s) with a different VLAN pool that is configured with the <b>even</b> assignment type. This issue is observed in controllers running ArubaOS 6.4.2.6.</p> <p><b>Platform:</b> All platforms.</p> <p><b>Reported Version:</b> ArubaOS 6.4.2.6.</p> <p><b>Workaround:</b> Change the VLAN assignment type from <b>even</b> to <b>hash</b> using the following CLI command:</p> <pre>(host) (config) #vlan-name &lt;name&gt; assignment hash</pre>

## WebUI

**Table 24:** *WebUI Known Issues*

Bug ID	Description
125862	<p><b>Symptom:</b> An administrator is unable to add a Virtual Local Area Network (VLAN) to the port channel using the controller WebUI.</p> <p><b>Scenario:</b> This issue is observed in both master and local controllers in a master-standby-local topology running ArubaOS 6.4.x.</p> <p><b>Platform:</b> All platforms.</p> <p><b>Reported Version:</b> ArubaOS 6.4.2.5.</p> <p><b>Workaround:</b> Add the VLAN to the port channel using the CLI.</p>

## Maximum Number of NAT Pools

A controller supports a maximum of 60 NAT pools.

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 23](#)
- [GRE Tunnel-Type Requirements on page 24](#)
- [Important Points to Remember and Best Practices on page 24](#)
- [Memory Requirements on page 25](#)
- [Backing up Critical Data on page 25](#)
- [Upgrading in a Multicontroller Network on page 27](#)
- [Installing the FIPS Version of ArubaOS 6.4.4.3 on page 27](#)
- [Upgrading to ArubaOS 6.4.4.3 on page 27](#)
- [Downgrading on page 31](#)
- [Before You Call Technical Support on page 33](#)

## Upgrade Caveats

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

- AP LLDP profile is not supported on AP-120 Series access points in ArubaOS 6.4.x.
- Starting from ArubaOS 6.3.1.0, the local file upgrade option in the 620 and 650 controller WebUIs have been disabled.
- ArubaOS 6.4.x does not allow you to create redundant firewall rules in a single ACL. ArubaOS will consider a rule redundant if the primary keys are the same. The primary key is made up of the following variables:
  - source IP/alias
  - destination IP/alias
  - proto-port/service

If you are upgrading from ArubaOS 6.1 or earlier and your configuration contains an ACL with redundant firewall rules, upon upgrading, only the last rule will remain.

For example, in the below ACL, both ACE entries could not be configured in ArubaOS 6.4.x. When the second ACE is added, it overwrites the first.

```

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

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

```

- ArubaOS 6.4.x supports only the newer MIPS controllers (7200 Series, 7000 Series, M3, 3200XM, 3400, 3600, and 600 Series). Legacy PPC controllers (200, 800, 2400, SC1/SC2) and 3200 controllers are not supported. Do not upgrade to ArubaOS 6.4.x if your deployment contains a mix of MIPS and PPC controllers in a master-local setup.
- When upgrading the software in a multicontroller 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 Multicontroller Network on page 27.](#))

## GRE Tunnel-Type Requirements

This section describes the important points to remember when configuring an L2 GRE tunnel with respect to tunnel-type:

- ArubaOS 6.4.4.0 continues to support L2 GRE tunnel type zero, but it is recommended to use a non-zero tunnel type.
- If both L2 and L3 tunnels are configured between end point devices, you must use a non-zero tunnel type for L2 GRE tunnels.

## Important Points to Remember and Best Practices

Ensure a successful upgrade and optimize your upgrade procedure by taking the recommended actions provided in the following list. 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, such as configuration changes, hardware upgrades, or changes to the rest of the network during the upgrade. This simplifies troubleshooting.
- Know your network and 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 executing 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 this version of ArubaOS, assess your software license requirements and load any new or expanded licenses you may require. For a detailed description of these new license modules, refer to the “Software Licenses” chapter in the *ArubaOS 6.4.x 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, the following compact memory best practices are recommended:

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



---

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 execute the **halt** command before power cycling.

---

If the output of the **show storage** command indicates that there is insufficient flash memory space, you must free up some used memory. Any controller logs, crash data, or 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 up some memory before upgrading:

- **Crash Data:** Execute 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 25](#) to copy the **crash.tar** file to an external server, and then execute the **tar clean crash** command to delete the file from the controller.
- **Flash Backups:** Use the procedures described in [Backing up Critical Data on page 25](#) to back up the flash directory to a file named **flash.tar.gz**, and then execute the **tar clean flash** command to delete the file from the controller.
- **Log files:** Execute 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 25](#) to copy the **logs.tar** file to an external server, and then execute the **tar clean logs** command 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

## Backing up and Restoring 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 the **Configuration** tab.
2. Click **Save Configuration** 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 and click **Restore**.

## Backing up and Restoring Compact Flash in the CLI

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

1. Make sure you are in the **enable** mode in the controller CLI, and execute the following command:

```
(host) # write memory
```

2. Execute 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. Execute 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 by executing the **copy** command.

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

4. Execute the **restore** command to untar and extract the **flashbackup.tar.gz** file to the compact flash file system.

```
(host) # restore flash
```

## Upgrading in a Multicontroller Network

In a multicontroller 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 25](#).



---

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 of the same model.

---

To upgrade an existing multicontroller system to this version of ArubaOS:

1. Load the software image onto all controllers (including redundant master controllers).
2. If all the controllers cannot be upgraded with the same software image and rebooted simultaneously, use the following guidelines:
  - a. Upgrade the software image on all the controllers. Reboot the master controller. After the master controller completes rebooting, you can reboot the local controllers simultaneously.
  - b. Verify that the master and all local controllers are upgraded properly.

## Installing the FIPS Version of ArubaOS 6.4.4.3

Download the FIPS version of the software from <https://support.arubanetworks.com>.

### Instructions on Installing FIPS Software

Follow these steps to install the FIPS software that is currently running a non-FIPS version of the software:

1. Install the FIPS version of the software on the controller.
2. Execute the **write erase** command to reset the configuration to the factory default; otherwise, you cannot log in to the controller using the CLI or WebUI.
3. Reboot the controller by executing the **reload** command.

This is the only supported method of moving from non-FIPS software to FIPS software.

## Upgrading to ArubaOS 6.4.4.3

The following sections provide the procedures for upgrading the controller to ArubaOS 6.4.4.3 by using the WebUI or CLI.

### Install Using the WebUI



---

Confirm that there is at least 60 MB of free memory and at least 75 MB of flash space available for an upgrade using the WebUI. For details, see [Memory Requirements on page 25](#).

---



---

When you navigate to the **Configuration** tab of the controller's WebUI, the controller may display the **Error getting information: command is not supported on this platform** message. This error occurs when you upgrade the controller from the WebUI and navigate to the **Configuration** tab as soon as the controller completes rebooting. This error is expected and disappears after clearing the Web browser cache.

---

### 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 6.4.4.3.

- For controllers running ArubaOS 3.x.versions earlier than ArubaOS 3.4.4.1, download the latest version of ArubaOS 3.4.5.x.
- For controllers running ArubaOS 3.x or those running ArubaOS 5.0.x versions earlier than ArubaOS 5.0.3.1, download and install the latest version of ArubaOS 5.0.4.x.
- For controllers running ArubaOS 6.0.0.0 or 6.0.0.1 versions, download and install the latest version of ArubaOS 6.0.1.x.

Follow step 2 to step 11 of the procedure described in [Upgrading From a Recent Version of ArubaOS on page 28](#) to install the interim version of ArubaOS, and then repeat steps 1 through 11 of the procedure to download and install ArubaOS 6.4.4.3.

## Upgrading From a Recent Version of ArubaOS

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

- ArubaOS 3.4.4.1 or later versions of ArubaOS
- ArubaOS 5.0.3.1 or latest version of ArubaOS 5.0.x
- ArubaOS 6.0.1.0 or later versions of ArubaOS 6.x

Install the ArubaOS software image from a PC or workstation using the 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 6.4.4.3 from the customer support site.
2. Upload the new software image(s) to a PC or workstation on your network.
3. Validate the SHA hash for a software image:
  - a. Download the **Aruba.sha256** file from the download directory.
  - b. To verify the image, load the image onto a Linux system and execute the **sha256sum <filename>** command or use a suitable tool for your operating system that can generate a **SHA256** hash of a file.
  - c. Verify that the output produced by this command matches the hash value found on the support site.




---

The ArubaOS image file is digitally signed, and is verified using RSA2048 certificates preloaded on the controller at the factory. Therefore, even if you do not manually verify the SHA hash of a software image, the controller will not load a corrupted image.

---

4. Log in to the ArubaOS WebUI from the PC or workstation.
5. Navigate to the **Maintenance > Controller > Image Management** page.
  - a. Select the **Local File** option.
  - b. Click **Browse** to navigate to the saved image file on your PC or workstation.
6. Select the downloaded image file.
7. Click the nonboot partition from the **Partition to Upgrade** radio button.
8. Click **Yes** in the **Reboot Controller After Upgrade** radio button to automatically reboot after upgrading. Click **No**, if you do not want the controller to reboot immediately.




---

Note that the upgrade will not take effect until you reboot the controller.

---

9. Click **Yes** in the **Save Current Configuration Before Reboot** radio button.
10. Click **Upgrade**.

When the software image is uploaded to the controller, a popup window displays the **Changes were written to flash successfully** message.

11. Click **OK**.

If you chose to automatically reboot the controller in step 8, the reboot process starts automatically within a few seconds (unless you cancel it).

12. When the reboot process is complete, log in to the WebUI and navigate to the **Monitoring > NETWORK > All WLAN Controllers** page to verify the upgrade.

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

1. Log in to the WebUI to verify all your controllers are up after the reboot.
2. Navigate to the **Monitoring > NETWORK > Network Summary** page to determine if your APs are up and ready to accept clients. In addition, verify that the number of access points and clients are what you would expect.
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. See [Backing up Critical Data on page 25](#) for information on creating a backup. If the flash (Provisioning/Backup) image version string shows the letters *rn*, for example, 3.3.2.11-rn-3.0, note those AP names and IP addresses. The RAP-5/RAP-5WN reboots to complete the provisioning image upgrade.

## Install Using the CLI



---

Confirm that there is at least 40 MB of free memory and at least 60 MB of flash space available for an upgrade using the CLI. For details, see [Memory Requirements on page 25](#).

---

### Upgrading From an Older Version of ArubaOS

Before you begin, verify the version of ArubaOS currently running on your controller. For more information, see [Upgrading From an Older Version of ArubaOS on page 27](#).

Follow steps 2 through 7 of the procedure described in [Upgrading From a Recent Version of ArubaOS on page 29](#) to install the interim version of ArubaOS, and then repeat steps 1 through 7 of the procedure to download and install ArubaOS 6.4.4.3.

### Upgrading From a Recent Version of ArubaOS

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

- ArubaOS 3.4.4.1 or later version of ArubaOS
- ArubaOS 5.0.3.1 or latest version of ArubaOS 5.0.x
- ArubaOS 6.0.1.0 or later versions of ArubaOS 6.x

To install the ArubaOS software image from a PC or workstation using the CLI on the controller:

1. Download ArubaOS 6.4.4.3 from the customer support site.
2. Open an SSH session on your master (and local) controllers.
3. Execute the **ping** command to verify the network connection from the target controller to the SCP/FTP/TFTP server.

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

or

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

or

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

4. Execute the **show image version** command to check if the ArubaOS images are 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**.

```
(host) #show image version
```

```
-----  
Partition           : 0:0 (/dev/hal)  
Software Version    : ArubaOS 6.4.4.0 (Digitally Signed - Production Build)  
Build number        : 51745  
Label               : 51745  
Built on            : Fri Sep 18 02:28:34 PDT 2015  
-----  
Partition           : 0:1 (/dev/hda2) **Default boot**  
Software Version    : ArubaOS 6.4.4.2 (Digitally Signed - Production Build)  
Build number        : 52482  
Label               : 52482  
Built on            : Wed Nov 11 13:07:11 PDT 2015
```

5. Execute the **copy** command to load the new image onto the nonboot partition.

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

or

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

or

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

or

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



---

The USB option is available on the 7010, 7030, and 7200 Series controllers.

---

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

```
(host)# show image version
```

```
-----  
Partition           : 0:0 (/dev/hda1) **Default boot**  
Software Version    : ArubaOS 6.4.4.3 (Digitally Signed - Production Build)  
Build number        : 52647  
Label               : 52647  
Built on            : Fri Nov 20 15:10:48 PDT 2015  
-----  
Partition           : 0:1 (/dev/hda2)  
Software Version    : ArubaOS 6.4.4.2 (Digitally Signed - Production Build)  
Build number        : 52482  
Label               : 52482  
Built on            : Wed Nov 11 13:07:11 PDT 2015
```

7. Reboot the controller.

```
(host)# reload
```

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

```
(host)# show version
```

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

1. Log in to the CLI to verify that all your controllers are up after the reboot.
2. Execute the **show ap active** command to determine if your APs are up and ready to accept clients.
3. Execute the **show ap database** command to verify that the number of access points and clients are what you 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 25](#) for information on creating a backup.

## Downgrading

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



---

If you upgraded from ArubaOS 3.3.x to ArubaOS 5.0, the upgrade script encrypts the internal database. New entries created in ArubaOS 6.4.4.3 are lost after the downgrade (this warning does not apply to upgrades from ArubaOS 3.4.x to ArubaOS 6.1).

---



---

If you downgrade to a pre-6.1 configuration that was not previously saved, some parts of your deployment may not work as they previously did. For example, when downgrading from ArubaOS 6.4.4.3 to 5.0.3.2, changes made to WIPS in ArubaOS 6.x prevent 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 have encountered this issue, execute the **show profile-errors** and **show ap-group** commands to view the IDS profile associated with the 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 preupgrade software version, you must perform the following steps:

1. Back up your controller. For details, see [Backing up Critical Data on page 25](#).
2. Verify that the control plane security is disabled.
3. Set the controller to boot with the previously saved pre-ArubaOS 6.4.4.3 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 is displayed if system boot parameters are set for incompatible image and configuration files.
5. After downgrading the software on the controller, perform the following steps:
  - Restore pre-ArubaOS 6.4.4.3 flash backup from the file stored on the controller. Do not restore the ArubaOS 6.4.4.3 flash backup file.

- You do not need to reimport the WMS database or RF Plan data. However, if you have added changes to RF Plan in ArubaOS 6.4.4.3, the changes do not appear in RF Plan in the downgraded ArubaOS version.
- If you installed any certificates while running ArubaOS 6.4.4.3, you need to reinstall the certificates in the downgraded ArubaOS version.

## Downgrading Using the WebUI

The following section describes how to use the WebUI to downgrade the software on the controller.

1. If the saved preupgrade 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 preupgrade configuration file.
  - b. For **Destination Selection**, enter a file name (other than default.cfg) for Flash File System.
2. Set the controller to boot with your preupgrade configuration file by navigating to the **Maintenance > Controller > Boot Parameters** page.
  - a. Select the saved preupgrade configuration file from the **Configuration File** drop-down list.
  - 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) by performing the following steps:
  - 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 preupgrade 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 section describes how to use the CLI to downgrade the software on the controller.

1. If the saved preupgrade 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 preupgrade configuration file.
 

```
(host) # 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 1, the backup system partition, contains the backup release ArubaOS 6.1.3.2. Partition 0, the default boot partition, contains the ArubaOS 6.4.4.3 image.



```
#show image version
-----
Partition          : 0:0 (/dev/hda1) **Default boot**
Software Version   : ArubaOS 6.4.4.3 (Digitally Signed - Production Build)
Build number       : 52647
Label              : 52647
Built on           : Fri Nov 20 15:10:48 PDT 2015
-----
Partition          : 0:1 (/dev/hda2)
Software Version   : ArubaOS 6.4.4.2 (Digitally Signed - Production Build)
Build number       : 52482
Label              : 52482
Built on           : Wed Nov 11 13:07:11 PDT 2015
```

4. Set the backup system partition as the new boot partition.

```
(host) # boot system partition 1
```

5. Reboot the controller.

```
(host) # reload
```

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

```
(host) # show image version
```

## Before You Call Technical Support

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

1. Provide a detailed network topology (including all the devices in the network between the user and the Aruba controller with IP addresses and Interface numbers if possible).
2. Provide the wireless device's make and model number, OS version (including any service packs or patches), wireless Network Interface Card (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) of when the problem first occurred. If the problem is reproducible, list the exact steps taken to re-create 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.