ArubaOS 6.5.4.9

a Hewlett Packard
Enterprise company

Release Notes

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 Enterprise Company. To obtain such source code, send a check or money order in the amount of US $10.00 to:

Hewlett Packard Enterprise Company
Attn: General Counsel
3000 Hanover Street
Palo Alto, CA 94304
USA

Revision History

The following table provides the revision history of this document.

Table 1: *Revision History*

Revision	Change Description
Revision 04	Added description of support for U730L modem.
Revision 03	Removed duplicate bug 167050 and 170409 from known bug 166800. Removed known bug 177152.
Revision 02	Added description of enhancement to wlxBSSIDIsup and wlxBSSIDIsdown traps.
Revision 01	Initial release.

The ArubaOS 6.5.4.9 release notes includes the following topics:

- New Features describes the new features and enhancements introduced in this release.
- Regulatory Updates lists the regulatory updates in this release.
- Resolved Issues lists the issues resolved in this release.
- Known Issues lists the issues identified in this release.
- Upgrade Procedure describes the procedures for upgrading your WLAN network to the latest ArubaOS release version.

Supported Browsers

The following browsers are officially supported for use with ArubaOS WebUI:

- Microsoft Internet Explorer 11 on Windows 7 and Windows 8
- Microsoft Edge (Microsoft Edge 38.14393.0.0 and Microsoft EdgeHTML 14.14393) on Windows 10
- Firefox 58 and later on Windows 7, Windows 8, Windows 10, and macOS
- Apple Safari 9.0 or later on macOS
- Google Chrome 67 and later on Windows 7, Windows 8, Windows 10, and macOS

Contacting Support

Table 2: *Contact Information*

Main Site	arubanetworks.com
Support Site	support.arubanetworks.com
Airheads Social Forums and Knowledge Base	community.arubanetworks.com
North American Telephone	1-800-943-4526 (Toll Free) 1-408-754-1200

International Telephone	arubanetworks.com/support-services/contact-support/
Software Licensing Site	hpe.com/networking/support
End-of-life Information	arubanetworks.com/support-services/end-of-life/
Security Incident Response Team	Site: arubanetworks.com/support-services/security-bulletins/ Email: sirt@arubanetworks.com

This chapter describes the new features and/or enhancements introduced in ArubaOS 6.5.4.9. For more information about these features, refer to the *ArubaOS 6.5.4.x User Guide*.

AP-Wireless

Mute AP Radio

Starting from this release, the **rf dot11a-radio-profile** and **rf dot11g-radio-profile** commands include the **am-tx-mute** parameter. Enable the **am-tx-mute** parameter to prevent an AP that operates in the AM or spectrum mode from creating spurious transmissions during AP boot. By default, the **am-tx-mute** is disabled.

Enable the **am-tx-mute** parameter in the **rf dot11a-radio-profile** or **rf dot11g-radio-profile** command only for APs that operate in the AM or spectrum mode.

To enable the am-tx-mute parameter:

```
(host) (config) #rf dot11a-radio-profile default
(host) (config) (rf dot11a-radio-profile "default")#am-tx-mute
```

Remote AP

Support for U730L Modem

ArubaOS 6.5.4.9 supports U730L modem on AP-203R, AP-203RP, and AP-303H Remote APs and branch controllers. The U730L modem requires to be setup in the enterprise mode before it can be plugged into the USB port of a Remote AP.

To enable the U730L modem in enterprise mode:

1. Plug the U730L modem into a laptop running Windows or MacOS and ensure that the wireless adapter is MiFi USB730L. Disable all other adapters or interfaces.
2. Navigate to http://my.usb/labtestinfo in a web browser.
3. Click **Enterprise Mode**.
4. Click **OK** in the pop-up window.

Wait for the U730L modem to reboot and come up before unplugging it from the laptop. You can either watch the LED on the U730L modem for re-initialization or observe the modem adapter in the laptop. The modem adapter temporarily goes down and reconnects after about 30 seconds.

To check if the U730L modem is converted to enterprise mode:

1. Check the name of the U730L modem adapter under **Network Connections** in a laptop running Windows. The name of the U730L modem changes from **MiFi USB730L** to **RNDIS**.
2. Plug the modem into the USB port of a Remote AP and reboot the Remote AP.
3. Check **Product_ID** in the console output of the Remote AP. If **Product_ID** is **9032**, the U730L modem is converted to enterprise mode. If **Product_ID** is **9030**, the U730L modem is not converted to enterprise mode. In the following example, the U730L modem is not converted to enterprise mode:

```
USB Plugged in: Vendor_ID=1410 Product_ID=9032
USB is not provisoned mannually, goto automatic provision.
```

SNMP

Enhancements to LinkUp and LinkDown Traps (Bug-174533)

Starting from this release, the **IfDescr** and **IfName** objects are added to the **LinkUp** and **LinkDown** traps to include the description and name details of the interface.

Enhancements to wlxBSSIDIsup and wlxBSSIDIsdown Traps (Bug-185196)

Starting from this release, the name of the AP is added to the **wlxBSSIDIsup** and **wlxBSSIDIsdown** traps. The output of the **show snmp trap-queue** command lists the name and MAC address of the access points associated with the BSSID.

WarmStart and ColdStart Traps (Bug-176862)

Starting from this release, the **warmstart** and **coldstart** traps are added. The **warmstart** trap indicates graceful purposeful reload or restart of the controller. The **coldstart**trap indicates ungraceful restart or reload of the controller where the configuration may have changed.

Chapter 3
Regulatory Updates

This chapter describes the regulatory updates in ArubaOS 6.5.4.9.

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 default Downloadable Regulatory Table (DRT) version is part of ArubaOS 6.5.4.9:

- DRT-1.0_66781

For a complete list of countries and the regulatory domains in which the APs are certified for operation, refer to the Downloadable Regulatory Table or the DRT Release Notes at support.arubanetworks.com.

The FCC has changed the rules for operation in all of the 5 GHz bands. For more information, refer to the *FCC DFS Regulatory Change Impact and Resolution Plan - Support Advisory* available in Support Advisories.

This chapter describes the issues resolved in ArubaOS 6.5.4.9.

Table 3: *Resolved Issues in ArubaOS 6.5.4.9*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
163295 179432 181438	**Symptom:** An AP sent beacons without CAC. This issue is resolved by allowing an AP to send beacons with CAC. **Scenario:** This issue occurred when an AP booted with DFS channels. This issue was observed in 300 Series access points running ArubaOS 6.5.4.3.	AP Regulatory	300 Series access points	ArubaOS 6.5.4.3	ArubaOS 6.5.4.9
165788	**Symptom:** A user was unable to remove stale entries from a standby controller. The fix allows the user to delete stale entries from the standby controller. **Scenario:** This issue was observed in a standby controller running ArubaOS 6.4.4.12 or later versions in a master-standby topology.	Station Management	All platforms	ArubaOS 6.4.4.12	ArubaOS 6.5.4.9
165804	**Symptom:** A HTTP security header was not detected on ports 8080 or 8088 in a controller. This issue is resolved by enabling the HTTP security header in the **httpd** configuration file. **Scenario:** This issue was observed in controllers running ArubaOS 6.5.3.3.	Controller-Platform	All platforms	ArubaOS 6.5.3.3	ArubaOS 6.5.4.9

Table 3: *Resolved Issues in ArubaOS 6.5.4.9*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
165908 170224 171074 171396 173372 174322 174370 174917 175009 177151 177457 177662 178307 180558 180741 181173 183588 185596 186993 187232 187418	**Symptom:** The **kernel** process in a controller crashed and the controller rebooted unexpectedly. The log file listed the reason for the event as **control processor kernel panic**. The fix ensures that the controller works as expected. **Scenario:** This issue was observed in controllers running ArubaOS 6.5.4.3.	Controller-Platform	All platforms	ArubaOS 6.5.4.3	ArubaOS 6.5.4.9
167028	**Symptom:** The SNMP walk reported the speed of a 1 Gbps Ethernet port in an AP as greater than 1 Gbps. The fix ensures that the SNMP walk reports the correct speed of the Ethernet port in the AP. **Scenario:** This issue occurred when the **STM** process incorrectly calculated the speed of the Ethernet port in an AP. This issue was observed in access points running ArubaOS 6.5.1.5 or later versions.	Air Management - IDS	All platforms	ArubaOS 6.5.1.5	ArubaOS 6.5.4.9
168363	**Symptom:** A client experienced packet loss. The fix ensures that the client does not experience packet loss. **Scenario:** This issue occurred when the CPU utilization in a controller was high. This issue was observed in 7240 controllers running ArubaOS 6.4.3.6.	Controller-Datapath	7240 controllers	ArubaOS 6.4.3.6	ArubaOS 6.5.4.9

Table 3: *Resolved Issues in ArubaOS 6.5.4.9*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
172149 184985	**Symptom:** A controller crashed and rebooted unexpectedly. The log file listed the reason for the event as **Control Processor Kernel Panic**. The fix ensures that the controller works as expected. **Scenario:** This issue occurred when DPI was enabled in a controller. This issue was observed in controllers running ArubaOS 6.5.3.0.	Controller-Datapath	All platforms	ArubaOS 6.5.3.0	ArubaOS 6.5.4.9
172506	**Symptom:** A controller discarded the first TCP SYN packet when a client connected to a FTP server. The fix ensures that the controller works as expected. **Scenario:** This issue occurred when DPI was enabled in a controller. This issue was observed in controllers running ArubaOS 6.4.4.14.	Controller-Datapath	All platforms	ArubaOS 6.4.4.14	ArubaOS 6.5.4.9
173906	**Symptom:** The NTP authentication keys were not automatically deleted on a standby controller after they are deleted on the master controller. The fix ensures that the NTP authentication keys are synchronized correctly between the standby controller and the master controller. **Scenario:** This issue was observed in controllers running ArubaOS 6.5.3.3 or later versions.	Controller-Platform	All platforms	ArubaOS 6.5.3.3	ArubaOS 6.5.4.9
174271	**Symptom:** A controller sent egress RTP traffic through its uplink (management) port although a policy based routing was configured to send egress RTP traffic on port 0/0/3. The fix ensures that the controller sends egress RTP traffic through the port that is configured in policy based routing. **Scenario:** This issue was observed in controllers running ArubaOS 6.5.3.3 or later versions.	Routing	All platforms	ArubaOS 6.5.3.3	ArubaOS 6.5.4.9
174823 175163	**Symptom:** The **Authentication** process in a controller crashed unexpectedly. The fix ensures that the **Authentication** process works as expected. **Scenario:** This issue occurred when the **aaa test-server verbose** command was executed. This issue was observed in controllers running ArubaOS 6.5.3.3 or later versions.	Base OS Security	All platforms	ArubaOS 6.5.3.3	ArubaOS 6.5.4.9

Table 3: *Resolved Issues in ArubaOS 6.5.4.9*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
175387	**Symptom:** APs blocked ARP requests which had the same IP address as that of local DHCP server of AP. The fix ensures the following: ■ AP datapath does not block the ARP request from the AP with the DHCP VLAN address. ■ If there is a wired or wireless client connected to AP and has the same IP address, the ARP reply is dropped by ARP as an ARP spoof. But, if this IP address does not belong to a client that is connected to AP, the ARP reply is forwarded. **Scenario:** This issue occurred when a route-cache entry was added with the AP local DHCP address and VLAN. But, when an ARP request which was with the same IP address as that of the AP's DHCP server was received by the AP, the AP datapath dropped the ARP request due to a mismatch in VLAN information. This issue was observed in access points running ArubaOS 6.4.4.0 or later versions.	AP Datapath	All platforms	ArubaOS 6.5.4.4	ArubaOS 6.5.4.9
176062	**Symptom:** A controller did not retain the configured member 0/0/2 on its static port channel interface. The fix ensures that the controller retains the configured member 0/0/2 on its static port channel interface. **Scenario:** This issue occurred when a controller was rebooted. This issue was observed in controllers running ArubaOS 6.5.4.4.	Port-Channel	All platforms	ArubaOS 6.5.4.4	ArubaOS 6.5.4.9
176105	**Symptom:** The boot environment configuration of an AP was lost and the AP rebooted unexpectedly. The fix ensures that the boot environment configuration of the AP is backed up. If the AP reboots without the boot environment configuration, the backup copy is restored and the AP boots as expected. **Scenario:** This was observed in AP-205 access points running ArubaOS 6.4.3.5.	AP-Platform	AP-205 access points	ArubaOS 6.4.3.5	ArubaOS 6.5.4.9
176562	**Symptom:** An AP that operated in monitor mode transmitted ACK frame with empty AMT on both 2.4 GHz and 5 GHz radios. Enhancements to the wireless driver resolved this issue. **Scenario:** This was observed in AP-205 access points running ArubaOS 6.5.4.8.	AP-Wireless	All platforms	ArubaOS 6.5.4.8	ArubaOS 6.5.4.9

Table 3: *Resolved Issues in ArubaOS 6.5.4.9*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
176927	**Symptom:** High channel utilization and beacon failure were observed in an AP and the issues continued until the AP was rebooted. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue was observed in access points running ArubaOS 6.5.3.4 or later versions.	AP-Wireless	All platforms	ArubaOS 6.5.3.4	ArubaOS 6.5.4.9
177045 180877	**Symptom:** An AP rebooted unexpectedly. The log file listed the reason for the event as **external watchdog reset**. The fix ensures that the AP works as expected. **Scenario:** This issue occurred when radio in the AP tried to reset PHY and the driver was stuck. This issue was observed in AP-203H and AP-207 access points running ArubaOS 6.5.4.8.	Port-Channel	AP-203H and AP-207 access points	ArubaOS 6.5.4.8	ArubaOS 6.5.4.9
178075 181721	**Symptom:** A client experienced lower download speed than normal. Enhancements to the wireless driver ensure that higher download speed is available in noisy conditions. **Scenario:** This issue occurred in a noisy environment on the 2.4 GHz channel. This issue was observed in 300 Series access points running ArubaOS 6.5.3.3.	SDN	300 Series access points	ArubaOS 6.5.3.3	ArubaOS 6.5.4.9
178114 180746	**Symptom:** A Remote AP established an IPsec tunnel with a controller but failed to come up on the controller. The fix ensures that the Remote AP works as expected. **Scenario:** This issue occurred when the MTU was not adjusted automatically. This issue was observed in AP-305 access points running ArubaOS 6.5.1.8 or later versions	SDN	AP-305 access points	ArubaOS 6.5.1.8	ArubaOS 6.5.4.9
178119	**Symptom:** A client was unable to connect to an AP. The fix ensures that the client can connect to the AP. **Scenario:** This issue occurred when the AP stopped broadcasting the configured SSID. This issue was observed in AP-225 and AP-325 access points running ArubaOS 6.4.4.0 or later versions.	AP-Platform	AP-225 and AP-325 access points	ArubaOS 6.4.4.0	ArubaOS 6.5.4.9

Table 3: *Resolved Issues in ArubaOS 6.5.4.9*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
178317 184539	**Symptom:** The BLE in an AP did not beacon. This issue is resolved by allowing only one APB operation at a time. **Scenario:** This issue was observed in AP-203H, AP-203R, AP-205H, 210 Series, 220 Series, 300 Series, 310 Series, 320 Series, 330 Series, and 360 Series access points running ArubaOS 6.5.4.7.	BLE	AP-203H, AP-203R, AP-205H, 210 Series, 220 Series, 300 Series, 310 Series, 320 Series, 330 Series, and 360 Series access points	ArubaOS 6.5.4.7	ArubaOS 6.5.4.9
178324	**Symptom:** The 5 GHz channel of an outdoor AP switched to channel 46 which was excluded in the regulatory-domain-profile. This issue is resolved by sending only the outdoor channel EIRP list for an outdoor AP. **Scenario:** This issue occurred when an outdoor AP randomly picked up a channel designated for use by an indoor AP from the exhaustive EIRP list. This issue was observed in outdoor access points running ArubaOS 6.4.4.0 or later versions.	AP-Platform	All platforms	ArubaOS 6.4.4.0	ArubaOS 6.5.4.9
178824 180650	**Symptom:** A client that was connected to an AP displayed low signal strength. The fix ensures that the correct signal strength is displayed. **Scenario:** This issue occurred when a client associated with the G radio of the AP. This issue was observed in AP-207 access points running ArubaOS 6.5.4.5 or later versions.	AP-Platform	AP-207 access points	ArubaOS 6.5.4.5	ArubaOS 6.5.4.9
179056 180149 180324 180214 180774 184967	**Symptom:** The status of the AP is displayed as **DOWN** in the WebUI but displayed as **UP** when the **show ap database long** command was executed. The fix ensures that the status of the AP is displayed correctly in the WebUI and CLI. **Scenario:** This issue was observed in controllers running ArubaOS 6.5.3.6.	AP-Platform	All platforms	ArubaOS 6.5.3.6	ArubaOS 6.5.4.9
180118	**Symptom:** An AP broadcasted an SSID that was configured with opensystem encryption as WEP SSID. The fix ensures that the AP broadcasts the SSID with the correct encryption. **Scenario:** This issue was observed in access points running ArubaOS 6.5.3.3.	AP-Platform	All platforms	ArubaOS 6.5.3.3	ArubaOS 6.5.4.9

Table 3: *Resolved Issues in ArubaOS 6.5.4.9*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
181401	**Symptom:** A mesh AP came up with **ML** (unlicensed) flags. The fix ensures that the mesh AP works as expected. **Scenario:** This issue occurred after a VRRP failover. This issue was observed in access points running ArubaOS 6.4.4.17 as a mesh portal.	AP-Platform	All platforms	ArubaOS 6.4.4.17	ArubaOS 6.5.4.9
181418 183863	**Symptom:** The **ISAKMPD** process in a controller crashed and the controller rebooted unexpectedly. The fix ensures that the controller works as expected. **Scenario:** This issue occurred because of memory corruption. This issue was observed in 7240 controllers running ArubaOS 6.5.1.5.	IPsec	All platforms	ArubaOS 6.5.1.5	ArubaOS 6.5.4.9
181564	**Symptom:** A Remote AP lost its gateway ARP. The fix ensures that the AP ignores the ICMP redirect message and retains its gateway ARP. **Scenario:** This issue occurred when a switch sent an ICMP redirect message to an AP indicating that a better route was available. The AP changed its routes and the traffic was blocked. This issue was observed in access points running ArubaOS 6.5.3.1.	Remote AP	All platforms	ArubaOS 6.5.3.1	ArubaOS 6.5.4.9
183072 189384	**Symptom:** The **datapath** process in a controller crashed and the controller rebooted unexpectedly. The fix ensures that the controller works as expected. **Scenario:** This issue occurred when a client sent FTP traffic and NAT was applied. During an aged session deletion, the controller freed an entry that accounted the NAT sequence number changes twice and led to a crash in the **datapath** process. This issue was observed in controllers running ArubaOS 6.5.4.8.	DPI	All platforms	ArubaOS 6.5.4.8	ArubaOS 6.5.4.9
183124	**Symptom:** An AP that operated in AM mode sent an ACK frame with empty AMT when a NULL BSS was received. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue occurred in APs that used ESDK version 5.0.9.1. This issue was observed in AP-203H, AP-203R, AP-203RP, and AP-207 access points running ArubaOS 6.5.3.8 in AM mode.	AP-Wireless	AP-203H, AP-203R, AP-203RP, and AP-207 access points	ArubaOS 6.5.3.8	ArubaOS 6.5.4.9

Table 3: *Resolved Issues in ArubaOS 6.5.4.9*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
185022	**Symptom:** A Remote AP established an IPsec tunnel with a controller but failed to come up on the controller. The fix ensures that the Remote AP comes up on the controller. **Scenario:** This issue occurred when the MTU was not adjusted automatically. This issue was observed in AP-305 access points running ArubaOS 6.5.1.8.	AP Datapath	AP-305 access points	ArubaOS 6.5.1.8	ArubaOS 6.5.4.9
186050	**Symptom:** The policy based routing in a controller did not route TCP-5060 traffic. The fix ensures that policy based routing routes the TCP-5060 traffic correctly. **Scenario:** This issue was observed in controllers running ArubaOS 6.5.1.9.	Policy Based Routing	All platforms	ArubaOS 6.5.1.9	ArubaOS 6.5.4.9
186509	**Symptom:** A client failed dynamic WEP reauthentication with an AP. This issue is resolved by not dropping the unencrypted Rx EAPOL frames when dynamic WEP reauthentication is enabled. **Scenario:** This issue occurred when the wireless driver dropped unencrypted Rx EAPOL frames after the WEP key was set. This issue was observed in AP-305, AP-315, and AP-335 access points running ArubaOS 6.5.4.8 and operated in bridge mode.	AP-Wireless	AP-305, AP-315, and AP-335 access points	ArubaOS 6.5.4.8	ArubaOS 6.5.4.9

This chapter describes the known and outstanding issues identified in ArubaOS 6.5.4.9.

Table 4: *Known Issues in ArubaOS 6.5.4.9*

Bug ID	Description	Component	Platform	Reported Version
154625 155709 155894 156383 158536 161789	**Symptom:** The VRRP state changes although heartbeats are not missed. **Scenario:** This issue occurs when a standby controller inadvertently transitions to master state because the master controller delays the processing of VRRP advertisements. This issue is observed in controllers running ArubaOS 6.5.0.3 in a local-master topology. **Workaround:** Disable debug logs and syslog server. Increase the advertisement interval.	Controller-Platform	All platforms	ArubaOS 6.5.0.3
157199	**Symptom:** An AP crashes unexpectedly. The log file lists the reason for the event as **kernel BUG at kernel/timer.c:869!**. **Scenario:** This issue is observed in AP-225 access points running ArubaOS 6.5.2.0. **Workaround:** None.	AP-Wireless	AP-225 access points	ArubaOS 6.5.2.0
158149 176715	**Symptom:** The BLE scanning in an AP is slow and fewer BLE devices are reported. **Scenario:** This issue is observed in AP-207 access points running ArubaOS 6.5.2.0 or later versions. **Workaround:** None.	BLE	AP-207 access points	ArubaOS 6.5.2.0
161655	**Symptom:** Some high-frequency radio statistics like Tx time, Rx time, and Rx clear are not collected correctly per beacon period in an AP. **Scenario:** This issue is observed in access points running ArubaOS 6.5.2.0. **Workaround:** None.	AP-Platform	All platforms	ArubaOS 6.5.2.0
166426	**Symptom:** A master and standby controllers reboot unexpectedly. The log file lists the reason for the event as **Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:60)**. **Scenario:** This issue is observed in controllers running ArubaOS 6.5.1.9 in a master-standby topology. **Workaround:** None.	Controller-Datapath	All platforms	ArubaOS 6.5.1.9

Table 4: *Known Issues in ArubaOS 6.5.4.9*

Bug ID	Description	Component	Platform	Reported Version
166800	**Symptom:** False detections of type-5 radars are triggered in the FCC domain. **Scenario:** This issue is observed in access points running ArubaOS 6.5.1.9. **Workaround:** None.	AP-Wireless	All platforms	ArubaOS 6.5.1.9
168789	**Symptom:** An AP with 802.1X supplicant configuration fails to boot. **Scenario:** This issue occurs when an ACL denies a DNS response from DNS server. This issue is observed in access points running ArubaOS 6.5.4.0 or later versions. **Workaround:** None.	AP-Platform	All platforms	ArubaOS 6.5.4.0
169622	**Symptom:** A syslog server reports the **aruba_change_channel 512 channel 6 mode 3 not found** error for some APs. **Scenario:** This issue is observed in AP-314 and AP-315 access points running ArubaOS 6.5.1.5. **Workaround:** None.	AP-Wireless	AP-314 or AP-315 access points	ArubaOS 6.5.1.5
170037 170055	**Symptom:** An AP does not discover a master controller through ADP. **Scenario:** This issue occurs when a static IP address is configured in an AP and the ACL denies ADP packets. This issue is observed in access points running ArubaOS 6.5.4.2. **Workaround:** None.	AP-Platform	All platforms	ArubaOS 6.5.4.2
171840 177067 179206	**Symptom:** A downloaded role becomes invalid in a controller. **Scenario:** This issue occurs when an access-list name is configured using uppercase characters. This issue is observed in controllers running ArubaOS 6.5.4.4. **Workaround:** None.	Role/VLAN Derivation	All platforms	ArubaOS 6.5.4.4
173353	**Symptom:** The **TM** column (time used by MGMT frames) in the output of the **show ap radio-summary dot11g** command always displays the value **100**. **Scenario:** This issue is observed in access points running ArubaOS 6.5.3.4. **Workaround:** None.	AP-Platform	All platforms	ArubaOS 6.5.3.4

Table 4: *Known Issues in ArubaOS 6.5.4.9*

Bug ID	Description	Component	Platform	Reported Version
174670 178706	**Symptom:** An LACP port channel receives multiple warning messages, **LACP: Disabling Collection and Distribution on port 0/0/0 LAG 0.** **Scenario:** This issue occurs when the port channel is in trusted mode and the trusted VLAN list for the port channel does not have the default VLAN in its list. This issue is observed in controllers running ArubaOS 6.5.3.5. **Workaround:** None.	Port-Channel	All platforms	ArubaOS 6.5.3.5
175852	**Symptom:** A controller displays the **Save failed: Module Authentication is busy. Please try later** error when the user attempts to save the configuration. **Scenario:** This issue is observed in controllers running ArubaOS 6.5.3.3 or later versions. **Workaround:** None.	Base OS Security	All platforms	ArubaOS 6.5.3.3
176344	**Symptom:** A controller does not retain the cached ACR license. **Scenario:** This issue is observed in controllers running ArubaOS 6.5.3.3-FIPS. **Workaround:** None.	Licensing	All platforms	ArubaOS 6.5.3.3-FIPS
176774 177016	**Symptom:** An AP crashes and reboots unexpectedly. **Scenario:** This issue is observed in AP-225 access points running ArubaOS 6.5.1.4. **Workaround:** None.	AP-Wireless	AP-225 access points	ArubaOS 6.5.1.4
177017	**Symptom:** An AP crashes and reboots unexpectedly. The log file lists the reason for the event as **Kernel panic - not syncing: Fatal exception in interrupt**. **Scenario:** This issue is observed in AP-225 access points running ArubaOS 6.5.1.4. **Workaround:** None.	AP-Wireless	AP-225 access points	ArubaOS 6.5.1.4
177205	**Symptom:** The **STM** process in a controller crashes and the controller reboots unexpectedly. The log file lists the reason for the event as **unexpected stm (Station management) runtime error at data_path_handler, 1324, data_path_handler: recv - Network is down** **Scenario:** This issue is observed in 7220 controllers running ArubaOS 6.5.3.4. **Workaround:** None.	Station Management	7220controllers	ArubaOS 6.5.3.4
177652 182718	**Symptom:** The value of the AP uptime displayed in the CLI is different from the value displayed in the **Dashboard > Access Points** WebUI page. **Scenario:** This issue is observed in controllers running ArubaOS 6.5.4.2. **Workaround:** None.	WebUI	All platforms	ArubaOS 6.5.4.2

Table 4: *Known Issues in ArubaOS 6.5.4.9*

Bug ID	Description	Component	Platform	Reported Version
178329	**Symptom:** The **show ap active** command shows incorrect 5 GHz channel information. **Scenario:** This issue is observed in access points running ArubaOS 6.5.3.4. **Workaround:** None.	AP-Wireless	All platforms	ArubaOS 6.5.3.4
179121 186434	**Symptom:** A controller does not log enabling or disabling audit trail in the audit trail log or system log. **Scenario:** This issue occurs when the **audit-trail**, **audit-trail all**, **no audit-trail**, and **no audit-trail all** commands are executed. This issue is observed in controllers running ArubaOS 6.5.3.4. **Workaround:** None.	Logging	All platforms	ArubaOS 6.5.3.4
179150 178445 178593 179787 179847 182020	**Symptom:** The memory in the wireless driver of an AP is corrupted. **Scenario:** This issue is observed in access points running ArubaOS 6.5.4.5. **Workaround:** None.	AP-Wireless	All platforms	ArubaOS 6.5.4.5
179360	**Symptom:** A controller displays the **Module L2TP is busy. Please try later** error message and does not provide L2TP IP address. **Scenario:** This issue is observed in controllers running ArubaOS 6.5.2.0. **Workaround:** None.	IPsec	All platforms	ArubaOS 6.5.2.0
179408	**Symptom:** A controller log displays the **|localdb| |wl-sync| Skipping db_sync** messages. **Scenario:** This issue is observed in 7220 controllers running ArubaOS 6.5.3.4. **Workaround:** None.	802.1X	All platforms	ArubaOS 6.5.3.4
179939	**Symptom:** A user is not able to configure the **radius-interim-accounting** parameter in the **aaa profile** command. **Scenario:** This issue occurs when the **dhcp-option-12** parameter in the **aaa derivation-rules** command and the **enforce-dhcp** parameter in **aaa profile** command are enabled. This issue is observed in controllers running ArubaOS 6.5.3.7 or later versions. **Workaround:** None.	Base OS Security	All platforms	ArubaOS 6.5.3.7

Table 4: *Known Issues in ArubaOS 6.5.4.9*

Bug ID	Description	Component	Platform	Reported Version
179970	**Symptom:** The **flags** column in the output of the **show ap bss-table** displays wrong characters for wired clients. **Scenario:** This issue is observed in controllers running ArubaOS 6.5.4.7. **Workaround:** None.	Station Management	All platforms	ArubaOS 6.5.4.7
180094	**Symptom:** The console output of an AP shows **asap_user_set_acl: no name for id 0** message with the MAC address of the associated clients. **Scenario:** This issue is observed in access points running ArubaOS 6.5.3.6. **Workaround:** None.	Management Auth and User Rights	All platforms	ArubaOS 6.5.3.6
181221 187011	**Symptom:** A client is unable to connect to a controller. **Scenario:** This issue occurs when enforce DHCP is enabled and route IP table buffer overflows. This issue is observed in controllers running ArubaOS 6.5.4.6. **Workaround:** None.	Controller-Datapath	All platforms	ArubaOS 6.5.4.6
181926	**Symptom:** A controller reboots unexpectedly. The log file lists the reason for the event as **Soft Watchdog reset (Intent:cause:register de:86:70:4)** **Scenario:** This is observed in 7240 controllers running ArubaOS 6.5.4.2. **Workaround:** None.	Controller-Platform	All platforms	ArubaOS 6.5.4.2
182342 183735	**Symptom:** An AP transmits an over the air frame on all scan channels that include all regulatory domain channels, rare channels, and DFS channels. **Scenario:** This issue is observed in 300 Series, 310 Series, 320 Series, 330 Series, and 360 Series access points running ArubaOS 6.5.4.0. **Workaround:** None.	AP-Wireless	300 Series, 310 Series, 320 Series, 330 Series, and 360 Series access points	ArubaOS 6.5.4.0
182960	**Symptom:** A controller shows the **tar crashError tar'ing(1). May have run out of space** error message. **Scenario:** This issue occurs when a user executes the **tar crash** command to generate the **crash.tar** file in a controller. This issue is observed in controllers running ArubaOS 6.5.3.6. **Workaround:** None.	Controller-Platform	All platforms	ArubaOS 6.5.3.6

Table 4: *Known Issues in ArubaOS 6.5.4.9*

Bug ID	Description	Component	Platform	Reported Version
183358	**Symptom:** A controller reboots unexpectedly. The log file lists the reason for the event as **Reboot Cause: Nanny rebooted machine - fpapps process died (Intent:cause:register 34:86:50:2)**. **Scenario:** This issue is observed in controllers running ArubaOS 6.5.3.6. **Workaround:** None.	Controller-Datapath	All platforms	ArubaOS 6.5.3.6
186224	**Symptom:** A client is unable to connect to a bridge mode virtual AP after a VLAN assignment failure. **Scenario:** This issue occurs when the VLAN in a controller is removed and the clients associated with the virtual AP are deauthenticated. This issue is observed in controllers running ArubaOS 6.5.4.6. **Workaround:** None.	Station Management	All platforms	ArubaOS 6.5.4.6
186266	**Symptom:** An AP reboots unexpectedly. The log file lists the reason for the event as **Out of memory**. **Scenario:** This issue is observed in AP-105 access points running ArubaOS 6.5.4.3. **Workaround:** None.	SDN-Platform	AP-105 access points	ArubaOS 6.5.4.3

Chapter 6
Upgrade Procedure

This chapter details the software upgrade procedures. Aruba best practices recommend that you schedule a maintenance window for upgrading your controllers.

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

Topics in this chapter include:

Upgrade Caveats

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

- 120 Series access points, 600 Series, 3000 Series, M3, and 6000 controllers are not supported in ArubaOS 6.5.x. Do not upgrade to ArubaOS 6.5.x if your deployment contains a mix of these controllers in a master-local setup.
- If your controller is running ArubaOS 6.4.0.0 or later versions, do not use a Windows-based TFTP server to copy the ArubaOS image to the nonboot partition of the controller for upgrading or downgrading. Use FTP or SCP to copy the image.
- Starting from ArubaOS 6.4.x, you cannot create redundant firewall rules in a single ACL. ArubaOS will consider a rule redundant if the primary keys are the same. The primary key is made up of the following variables:
  - source IP or alias
  - destination IP or alias

- proto-port or 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 following 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) #!
(host)(config) #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
```

- 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 29.)

Failure to Upgrade to ArubaOS 6.5.0.0-FIPS

Customers upgrading from any FIPS version of ArubaOS prior to ArubaOS 6.5.0.0-FIPS to ArubaOS 6.5.0.0-FIPS or later version may experience symptoms that indicate an upgrade failure. Symptoms may include the apparent loss of configuration, being unable to gain administrative access to the controller, and/or the hostname of the controller being set back to the default value.

This condition is caused by a change in the FIPS requirement for the strength of the hashing algorithm that is used to protect the configuration file from outside tampering. Starting from ArubaOS 6.5.0.0-FIPS, all versions of ArubaOS are changed to use the stronger hashing algorithm to meet FIPS requirements. This change is known to create a challenge when upgrading or downgrading a controller between ArubaOS 6.4.0.0-FIPS version and ArubaOS 6.5.0.0-FIPS version. In some instances the new stronger hash value may be missing or incorrect. This may cause the controller to not boot normally.

The most common scenario is when a controller has been booted with any version of ArubaOS 6.5.0.0-FIPS or later version, is subsequently downgraded to any version of ArubaOS 6.4.0.0-FIPS or prior versions, and then at any point in the future is upgraded back to any version ArubaOS 6.5.0.0-FIPS or later version.

To restore service, Aruba recommends to roll back the ArubaOS to the previous version. This can be accomplished by:

1. Connect an administrative terminal to the console port of the controller.
2. Power cycle the controller to reboot it.
3. On the administrative terminal, interrupt the boot process when prompted to enter the cpboot bootloader.

4. Execute the **osinfo** command to display the versions of ArubaOS hosted on partition 0 and partition 1.
5. Execute the **def_part 0** or **def_part 1** command depending on which partition hosts the previous version ArubaOS 6.4.0.0-FIPS or later version.
6. Execute the **reset** or **bootf** to reboot the controller.

This restores the controller to the previous version of ArubaOS and controller configuration. Contact Aruba support for instructions to proceed with the upgrade.

GRE Tunnel-Type Requirements

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

- ArubaOS 6.5.4.9 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 endpoint 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 6.5.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 27 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 27 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 27 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 27.

For proper operation, all controllers in the network must be upgraded with the same version of ArubaOS software. For redundant environments such as VRRP, 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 6.5.4.9

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

Instructions on Installing FIPS Software

Before you install a FIPS version of the software on a controller that is currently running a non-FIPS version of the software, follow the procedure below. If you are currently running a FIPS version of the software on the controller, you do not have to perform a **write erase** to reset the configuration as mentioned in step 2.

Follow the steps below to install the FIPS software on a controller 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 6.5.4.9

The following sections provide the procedures for upgrading the controller to ArubaOS 6.5.4.9 by using the WebUI and the CLI.

Install Using the WebUI

CAUTION

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 27.

NOTE

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 a Recent Version of ArubaOS

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

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

NOTE

When upgrading from an existing ArubaOS 6.4.x release, it is required to set AMON packet size manually to a desired value. However, the packet size is increased to 32K by default for fresh installations of ArubaOS 6.4.3.9.

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 6.5.4.9 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.

NOTE

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. Choose the nonboot partition from the **Partition to Upgrade** radio button.
8. Choose **Yes** in the **Reboot Controller After Upgrade** radio button to automatically reboot after upgrading. Choose **No**, if you do not want the controller to reboot immediately.

Upgrade will not take effect until you reboot the controller.

9. Choose **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 27 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.

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 27.

Upgrading From a Recent Version of ArubaOS

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

- ArubaOS 3.4.4.1 or later

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

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

1. Download ArubaOS 6.5.4.9 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**.
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 7000 Series and 7200 Series controllers.

6. Execute the **show image version** command to verify that the new image is loaded.
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 27 for information on creating a backup.

Downgrading

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

Database versions are not compatible between different ArubaOS releases.

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 6.5.4.9 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 27.
2. Verify that the control plane security is disabled.
3. Set the controller to boot with the previously saved pre-ArubaOS 6.5.4.9 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 6.5.4.9 flash backup from the file stored on the controller. Do not restore the ArubaOS 6.5.4.9 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 6.5.4.9, the changes do not appear in RF Plan in the downgraded ArubaOS version.
   - If you installed any certificates while running ArubaOS 6.5.4.9, 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 6.5.4.9 image.

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.