ArubaOS 6.4.4.5

Release Notes

a Hewlett Packard Enterprise company

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

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.

Contents

Revision History

The following table lists the revision history of this document.

Table 1: *Revision History*

Revision	Change Description
Revision 01	Initial release.

ArubaOS 6.4.4.5 is a software patch release that includes fixes to issues identified in previous ArubaOS releases.

Use the following links navigate to the corresponding topics:

- New Features on page 10 provides a description of features and enhancements introduced in ArubaOS 6.4.4.5.
- Regulatory Updates on page 11 lists the regulatory updates introduced in ArubaOS 6.4.4.5.
- Resolved Issues on page 12 lists the regulatory updates introduced in ArubaOS 6.4.4.5.
- Known Issues on page 20 lists and describes the known and outstanding issues identified in ArubaOS 6.4.4.5.
- Upgrade Procedure on page 27 describes the procedures for upgrading a controller to ArubaOS 6.4.4.5.

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 200 Series, AP-205H, 210 Series, 220 Series, and 270 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 2: *Profile Settings in ArubaOS 6.4.x*

Profile	Settings
802.11a/802.11g Radio Profile	• Channel • Enable Channel Switch Announcement (CSA) • CSA Count • High throughput enable (radio) • Very high throughput enable (radio) • TurboQAM enable • Maximum distance (outdoor mesh setting) • Transmit EIRP • Advertise 802.11h Capabilities • Beacon Period/Beacon Regulate • Advertise 802.11d Capabilities
Virtual AP Profile	• Virtual AP enable • Forward Mode • Remote-AP operation

SSID Profile	• ESSID
	• Encryption
	• Enable Management Frame Protection
	• Require Management Frame Protection
	• Multiple Tx Replay Counters
	• Strict Spectralink Voice Protocol (SVP)
	• Wireless Multimedia (WMM) settings
	  ▪ Wireless Multimedia (WMM)
	  ▪ Wireless Multimedia U-APSD (WMM-UAPSD) Powersave
	  ▪ WMM TSPEC Min Inactivity Interval
	  ▪ Override DSCP mappings for WMM clients
	  ▪ DSCP mapping for WMM voice AC
	  ▪ DSCP mapping for WMM video AC
	  ▪ DSCP mapping for WMM best-effort AC
	  ▪ DSCP mapping for WMM background AC

Table 2: *Profile Settings in ArubaOS 6.4.x*

Profile	Settings
High-throughput SSID Profile	• High throughput enable (SSID) • 40 MHz channel usage • Very High throughput enable (SSID) • 80 MHz channel usage (VHT)
802.11r Profile	• Advertise 802.11r Capability • 802.11r Mobility Domain ID • 802.11r R1 Key Duration • key-assignment (CLI only)
Hotspot 2.0 Profile	• Advertise Hotspot 2.0 Capability • RADIUS Chargeable User Identity (RFC4372) • RADIUS Location Data (RFC5580)

Supported Browsers

The following browsers are officially supported for use with ArubaOS 6.4.4.5 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 3: *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	licensing.arubanetworks.com
End-of-life Information	arubanetworks.com/support-services/end-of-life/
Security Incident Response Team (SIRT)	Site: arubanetworks.com/support-services/security-bulletins/ Email: sirt@arubanetworks.com

There are no new features introduced in ArubaOS 6.4.4.5.

Periodic regulatory changes may require modifications to the list of channels supported by an access point (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.

For a complete list of countries certified with different AP models, refer to the respective DRT release notes at support.arubanetworks.com.

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

The following default Downloadable Regulatory Table (DRT) file version is part of ArubaOS 6.4.4.5:

- DRT-1.0_53811

This release includes fixes for vulnerability documented in CVE-2015-7547. Additionally, the following issues are resolved in ArubaOS 6.4.4.5.

Table 4: *Resolved Issues in 6.4.4.5*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
117675	**Symptom:** After a client associated with a Virtual Access Point (VAP) in tunnel mode with dynamic WEP encryption, it did not send/receive traffic. This issue is resolved by setting null/dummy keys in all key IDs corresponding to WEP and setting cipher to none. **Scenario:** This issue was observed in 320 Series access points connected to controllers running ArubaOS 6.4.4.0.	AP-Wireless	320 Series access points	ArubaOS 6.4.4.0	ArubaOS 6.4.4.5
118685	**Symptom:** AP-175 access points rebooted. A memory monitor is added to identify the location of memory leakage. **Scenario:** This issue occurred because of memory leakage in the AP-175 access point running ArubaOS 6.3.1.15.	AP-Wireless	AP-175 access points	ArubaOS 6.3.1.15	ArubaOS 6.4.4.5
119884	**Symptom:** Clients did not send/receive traffic even though they were associated to access points. Improvements to the wireless driver resolved this issue. **Scenario:** Access point association was displayed as present in AP driver **debug client-table**, However, when the **show ap remote debug association**, **show ap remote debug mgmt-frames**, and **show ap association** commands were executed, the output displayed either stale information or no information for access point association in the Station Management (STM) table. This issue was observed in 200 Series access points connected to controllers running ArubaOS 6.4.2.6.	AP-Wireless	200 Series access points	ArubaOS 6.4.2.6	ArubaOS 6.4.4.5

Table 4: *Resolved Issues in 6.4.4.5*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
123239	**Symptom:** The **authentication** process stopped responding and crashed in a controller. The log files for the event listed the reason as **Control Processor Kernel Panic**. The fix ensures that the **authentication** process does not crash. **Scenario:** This issue occurred during an Enhanced Client or Proxy (ECP) authentication when the **authentication** process tried to access **user > l2role**, which was null. This issue was observed in controllers running ArubaOS 6.3.1.15.	Base OS Security	All platforms	ArubaOS 6.3.1.15	ArubaOS 6.4.4.5
123437	**Symptom:** A controller continued to display the **fpapps[3645]: <399816> <ERRS> |fpapps| hapiPortLinkStatus: Failed to read phy status on port 0/0/5** error message although the physical port of the controller was in service. The fix ensures that a controller does not generate such false alarms. **Scenario:** This issue was observed when Network Time Protocol (NTP) was configured in a controller. This issue was observed in 7000 Series and 7200 Seriescontrollers running ArubaOS 6.4.2.6.	Controller-Platform	7000 Series and 7200 Series controllers	ArubaOS 6.4.2.6	ArubaOS 6.4.4.5
123577 127545 132292	**Symptom:** The Virtual Router Redundancy Protocol (VRRP) link of a controller was unstable at random times. The log files for the event indicated a delay of few seconds in receiving Link Aggregation Control Protocol (LACP) keepalives. The fix ensures that the VRRP link is stable. **Scenario:** This issue occurred when a controller was configured with 1 second of master advertisement interval. This issue was observed in 7000 Series and 7200 Series controllers running ArubaOS 6.4.2.12 in master-local topology.	Controller-Platform	7000 Series and 7200 Series controllers	ArubaOS 6.4.2.12	ArubaOS 6.4.4.5

Table 4: *Resolved Issues in 6.4.4.5*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
125093 125740 126416 127424 128656 129183 129878 129970 131805 131867 131868 132090 132796 134178 134333 134567 135237 135347	**Symptom:** A controller stopped responding and rebooted. The log files for the event listed the reason as **datapath timeout**. The fix ensures that controllers do not experience any datapath timeout. **Scenario:** The datapath timeout occurred because the buffer replenish failed. This issue was observed in 7200 Series controllers running ArubaOS 6.4.2.x or ArubaOS 6.4.3.x.	Controller-Datapath	7200 Series controllers	ArubaOS 6.4.2.6	ArubaOS 6.4.4.5
125535	**Symptom:** After executing the **write memory** command on a master controller, few ACLs did not synchronize with the standby controller. The fix ensures that all ACLs synchronize with the standby controller. **Scenario:** This issue was observed in controllers running ArubaOS 6.4.2.x or ArubaOS 6.4.3.x in master-standby topology.	Captive Portal	All platforms	ArubaOS 6.4.2.3	ArubaOS 6.4.4.5
125572	**Symptom:** The **delete** command did not work for **Local Controller List For AP Whitelist Sync** and **Master Controller List For AP Whitelist Sync** under **Wireless > AP Installation > Whitelist > Campus AP** Or **Remote AP**. This issue is resolved sending a **delete** command. **Scenario:** This issue was observed in controllers running ArubaOS 6.3.1.18.	WebUI	All platforms	ArubaOS 6.3.1.18	ArubaOS 6.4.4.5

Table 4: *Resolved Issues in 6.4.4.5*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
126572	**Symptom:** A master controller failed to send SNMP traps for 200 Series access points. The fix ensures that a master controller sends the correct SNMP traps when there is a change in the transmit power level of an access point. **Scenario:** This issue was observed when the transmit power level of an access point changed. This issue was observed in 200 Series access points connected to controllers running ArubaOS 6.4.2.12.	ARM	200 Series access points	ArubaOS 6.4.2.12	ArubaOS 6.4.4.5
126670	**Symptom:** When an ACL name was removed or added from an interface, the applied count of the ACLs were not updated. This issue is resolved by ensuring that ACLs on a physical interface are not changed when the system is powered on. **Scenario:** This issue was observed when ACLs were changed on a physical interface. This was observed in controllers running ArubaOS 6.3.1.5.	Configuration	All platforms	ArubaOS 6.3.1.5	ArubaOS 6.4.4.5
126690	**Symptom:** Certain Dell Latitude laptops with Dell Wireless 1501 wireless adapter failed to get an IP address when associating with 200 Series, 210 Series, or 270 Series access points. This issue is resolved by improving the wireless driver of an access point. **Scenario:** This issue occurred because of wrong AP beacon. When HT is disabled in **rf dot11g-radio-profile** and enabled in **rf ht-ssid-profile**, AP beacon advertises HT IE. This issue is observed in 200 Series, 210 Series, or 270 Series access points connected to controllers running ArubaOS 6.4.2.x or ArubaOS 6.4.3.x.	AP-Wireless	200 Series, 210 Series, or 270 Series access points	ArubaOS 6.4.2.12	ArubaOS 6.4.4.5
127210 128489	**Symptom:** The **Print Preview** page in a Google Chrome Web browser was blank after logging in to a controller with the guest provisioning account. This issue is resolved by removing the reference to stylesheet. **Scenario:** This issue occurred because of a wrong reference to stylesheet. This issue was observed after logging in to a controller using Google Chrome 46.0.2490.71m web browser and previewing the page to print guest user credentials. This issue was observed in controllers running ArubaOS 6.3.1.x, ArubaOS 6.4.3.x, or ArubaOS 6.4.4.x.	WebUI	All platforms	ArubaOS 6.4.3.4	ArubaOS 6.4.4.5

Table 4: *Resolved Issues in 6.4.4.5*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
127359 131197 131432 132495	**Symptom:** AP-228 and 270 Series mesh portal and mesh point did not form a mesh link when they were connected to Cisco 3850 and 2960x Power Over Ethernet (POE) switches. This issue is resolved by adding a delay during the initial setup till the power profile changes to POE-AT. **Scenario:** This issue was observed in AP-228 and 270 Series access points connected to controllers running ArubaOS 6.4.3.x or ArubaOS 6.4.4.x.	Mesh	AP-228 and 270 Series access points	ArubaOS 6.4.3.5	ArubaOS 6.4.4.5
127421	**Symptom:** The **authentication** process crashed in a controller. This issue is resolved by clearing the memory pointers whenever the memory is freed. **Scenario:** This issue was observed in controllers with active Lightweight Directory Access Protocol (LDAP) server connections. This issue was observed in controllers running ArubaOS 6.4.3.x or later versions.	Base OS Security	All platforms	ArubaOS 6.4.3.1	ArubaOS 6.4.4.5
128348	**Symptom:** Intermittent high noise floor was observed in access points. This issue is resolved by increasing the NF calibration time on home channel. **Scenario:** This issue occurred when scanning was enabled and NF calibration parameters were not set correctly after returning to home channel. This issue was observed in access points connected to controllers running ArubaOS 6.4.4.1.	AP-Wireless	All platforms	ArubaOS 6.4.4.1	ArubaOS 6.4.4.5
128677	**Symptom:** An incorrect total number of APs was displayed in the WebUI under **WebUI > Monitoring**. This issue is resolved by calculating the total number of APs as the sum of wired AP and wireless AP and displaying the value in the WebUI. **Scenario:** This issue was observed in controllers running ArubaOS 6.3.1.15.	WebUI	All platforms	ArubaOS 6.3.1.15	ArubaOS 6.4.4.5

Table 4: *Resolved Issues in 6.4.4.5*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
128800	**Symptom:** Guest users were not removed from the user table after the user idle timer value that was configured in the Captive Portal (CP) profile expired. This issue is resolved by ensuring that if **l3role** has **cp-profile**, then use it to get the idle timeout, else get the idle timeout from the **cp-profile** in **l2role**. **Scenario:** This issue occurred when the user idle timeout that was configured in the CP profile was not considered for guest users and the guest users were timed out after the global user idle timeout expired. This issue was observed in controllers running ArubaOS 6.4.3.4.	Base OS Security	All platforms	ArubaOS 6.4.3.4	ArubaOS 6.4.4.5
129144	**Symptom:** Windows 10 clients running version 1511 were unable to connect to 802.1X SSID when termination was enabled on a controller. A workaround is added in the ArubaOS code whereby the controller sends a HELLO message with TLS v1.0 when the Advanced Cryptography (ACR) license is not available in the controller for clients initiating a TLS v1.2 session. **Scenario:** ArubaOS supports TLS v1.2 with Suite B which requires ACR license. Windows 10 clients with the new patch (OS Build 10586.3) seem to work with RSA certificates and TLS v1.2. This issue was observed in Windows 10 client with OS Build 10586.3 and controllers running ArubaOS 6.3.x or ArubaOS 6.4.x.	RADIUS	All platforms	ArubaOS 6.3.1.18	ArubaOS 6.4.4.5
130113 131653 131652	**Symptom:** RTP/RTCP packets were not prioritized in a Jabber voice conference call. This issue is resolved by adding a new IP address parameter in the media block to handle the video parameters. **Scenario:** This issue occurred when the connection details were over written because the IP address was common for different connections. This issue was observed in controllers running ArubaOS 6.5.0.0.	UCC	All platforms	ArubaOS 6.5.0.0	ArubaOS 6.4.4.5
131971 133165	**Symptom:** Wireless clients did not get IP address in DHCP-based derived VLAN and DHCP options based VLAN assignment did not work as expected. This issue is resolved by using station keys. **Scenario:** This issue occurred because of key mismatch in DHCP options based VLAN derivation. This issue was observed in controllers running ArubaOS 6.4.3.4.	Role/VLAN Derivation	All platforms	ArubaOS 6.4.3.4	ArubaOS 6.4.4.5

Table 4: *Resolved Issues in 6.4.4.5*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
132148	**Symptom:** AP-325 access points rebooted. The log files for the event listed the reason as **MSM HSL wait_for_xmitr is stuck**. This issue is resolved by resetting the UART and resuming the console. **Scenario:** This issue occurred because the UART was stuck. This issue was observed in AP-325 access points connected to controllers running ArubaOS 6.4.4.2.	AP Datapath	AP-325 access points	ArubaOS 6.4.4.2	ArubaOS 6.4.4.5
132239 134538	**Symptom:** AP-325 access points crashed and rebooted with the reason **Reboot caused by kernel panic: Aruba watchdog bark interrupt received on core 0**. This issue is avoiding SKB double free situations. **Scenario:** This issue occurred because of SKB double free situation. This issue was observed in AP-325 access points connected to controllers running ArubaOS 6.4.4.3.	AP-Wireless	AP-325 access points	ArubaOS 6.4.4.3	ArubaOS 6.4.4.5
132838	**Symptom:** When using the search option in the WebUI, the pagination was incorrect and a user could not navigate to other pages. This issue is resolved by resetting the pagination counter to 0 when changing the filter **All**, **IPV4**, and **IPV6**. **Scenario:** This issue was observed in controllers running ArubaOS 6.4.4.3.	WebUI	All platforms	ArubaOS 6.4.4.3	ArubaOS 6.4.4.5

Table 4: *Resolved Issues in 6.4.4.5*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
133140	**Symptom:** AP-205H access points did not complete 802.1X authentication when connected directly to a controller. This issue is resolved by configuring a rule in ARL to allow the EAPOL frames in AP-205H access points. **Scenario:** This issue occurred because the AP-205H access points dropped the EAPOL frames. This issue was observed when AP-205H access points were directly connected to untrusted ports of a controller running ArubaOS 6.4.3.6 over an Ethernet cable.	AP-Platform	AP-205H access points	ArubaOS 6.4.3.6	ArubaOS 6.4.4.5
133448	**Symptom:** IPsec association failed when IP NAT was configured outside on a branch office controller. This issue is resolved by adding checks for destination port. **Scenario:** This issue occurred when **IP NAT outside** was applied to VLAN 4094 on a branch office controller. A datapath session was created with a source network address translation rule and the IKE packets were source network address translated. As part of the network address translation, the source port in IKE packet was changed from 4500 to a different value and when route lookup was performed, the packet was not recognized as an IKE packet and the packet was not sent. This issue was observed in controllers running ArubaOS 6.4.3.2.	Controller-Datapath	All platforms	ArubaOS 6.4.3.2	ArubaOS 6.4.4.5
134678	**Symptom:** High Throughput (HT) and Very High Throughout (VHT) capable clients failed to connect at HT and VHT rates. Improvements in the AP wireless driver ensure that HT and VHT capable clients connect at HT and VHT rates. **Scenario:** This issue occurred after a VRRP failover. This issue was observed in 802.11ac-capable access points connected to controllers running ArubaOS 6.4.2.15, ArubaOS 6.4.3.x, or ArubaOS 6.4.4.x.	AP-Wireless	200 Series, 210 Series, and 270 Series access points	ArubaOS 6.4.2.15	ArubaOS 6.4.4.5

This chapter describes the known and outstanding issues identified in ArubaOS 6.4.4.5.

Support for 320 Series Access Points

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

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

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

Table 5: *Known Issues in 6.4.4.5*

Bug ID	Description	Component	Platform	Reported Version
88769 116040 116558 118874 124515 132671	**Symptom:** The **show crypto isakmp policy 10004** command incorrectly displays the hash algorithm as **Secure Hash Algorithm 160**. **Scenario:** This issue occurs for the default 10004 Internet Key Exchange (IKE) policy. This issue is observed in controllers running ArubaOS 6.4.x. **Workaround:** None.	IPsec	All platforms	ArubaOS 6.4.0.0
121020 124020	**Symptom**: Access points crash with the error **Reboot caused by kernel panic: Fatal exception** message. **Scenario:** This issue occurs because the memory is exhausted from several queues with several broadcasts. This issue is observed in AP-275 access points connected to controllers running ArubaOS 6.4.3.1. **Workaround**: None.	AP-Wireless	AP-275 access points	ArubaOS 6.4.3.1
123458	**Symptom**: Access points fail to send Link Layer Discovery Protocol-Media Endpoint Discovery (LLDP-MED) Type-Length-Value (TLV) information after receiving an LLDP packet from a Cisco VoIP phone. **Scenario**: This issue occurs when devices that support LLDP-MED are connected to the downlink Ethernet port of access points. This issue is observed in access points connected to controllers running ArubaOS 6.4.3.3. or later versions. **Workaround**: None.	AP-Platform	All platforms	ArubaOS 6.4.3.3

124136	**Symptom**: Clients are unable to connect to an SSID. The log file for the event lists the reason as, **Capability requested by STA unsupported by AP**.
	Scenario: This issue occurs during a failover in High Availability (HA) setup, when no Virtual Local Area Network (VLAN) is assigned for the Virtual Access Point (VAP) profile that is configured in tunnel mode
	Workaround: Configure a VLAN ID in the VAP profile by using the following CLI commands.
	`(host) (config) #wlan virtual-ap <profile-name>`
	`(host) (Virtual AP profile "<profile-name>") #vlan <vlan-id>`
		AP-Wireless	All platforms	ArubaOS 6.4.2.5

Table 5: *Known Issues in 6.4.4.5*

Bug ID	Description	Component	Platform	Reported Version
124275	**Symptom**: 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. **Scenario**: This issue occurs when a RADIUS server VSA overrides the VAP VLAN with a different VLAN pool that is configured with the **even** assignment type. This issue is observed in controllers running ArubaOS 6.4.2.6. **Workaround**: Change the VLAN assignment type from **even** to **hash** by using the following CLI command: `(host) (config) #vlan-name <name> assignment hash`	Station Management	All platforms	ArubaOS 6.4.2.6
124767 124841	**Symptom**: Call Detail Records (CDR) are unavailable or not generated properly for SIP calls initiated by clients that use large segmented packets for signaling. As a result, media traffic is not prioritized and call details are not visible on the UCC dashboard. **Scenario**: This issue is observed when SIP signaling messages are delivered in multiple segments that are received out of order. This issue is not limited to any specific controller model or ArubaOS version. **Workaround**: None.	Unified Communication	All platforms	ArubaOS 6.4.2.4.
125862	**Symptom**: Users are unable to add a Virtual Local Area Network (VLAN) to the port channel using the WebUI. **Scenario**: This issue is observed in both master and local controllers running ArubaOS 6.4.x in a master-standby-local topology. **Workaround**: Add the VLAN to the port channel using the CLI.	WebUI	All platforms	ArubaOS 6.4.2.5
126418	**Symptom**: When the **show ap database flags D** command is executed on a master controller, the output incorrectly displays a D flag (dirty or no configuration) for access points that have good configuration. **Scenario**: This issue is observed in controllers running ArubaOS 6.4.x in master-local topology. **Workaround**: None.	AP-Platform	All platforms	ArubaOS 6.4.2.10

Table 5: *Known Issues in 6.4.4.5*

Bug ID	Description	Component	Platform	Reported Version
126713	**Symptom**: A controller continues to send authentication requests to an authentication server that is out of service. **Scenario**: 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. **Workaround**: None.	Base OS Security	All platforms	ArubaOS 6.4.2.5
127848	**Symptom**: Access points do not reconnect their Point-to-Point Protocol over Ethernet (PPPoE) to the backup-LMS when the LMS is not available. **Scenario**: This issue is observed in AP-205 and AP-274 access points connected to controllers running ArubaOS 6.4.4.0. **Workaround**: None.	Remote AP	AP-205 and AP-274 access points	ArubaOS 6.4.4.0
128466	**Symptom**: A controller displays the **Invalid TLS version** error in authentication trace buffer after uploading a new certificate for Extensible Authentication Protocol-Protected Extensible Authentication Protocol (EAP-PEAP) authentication. This results in user authentication failure. **Scenario**: This issue occurs when a client finishes Transport Layer Security (TLS) for 802.1X authentication. The problem occurs while 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. **Workaround**: None.	Base OS Security	All platforms	ArubaOS 6.4.2.12
129043	**Symptom**: A controller reboots. The log file for the event lists the reason as **datapath timeout**. **Scenario**: This issue is observed in both master and local controllers running ArubaOS 6.4.3.4 in master-local topology. **Workaround**: None.	Controller-Datapath		
129096	**Symptom**: The Lightweight Directory Access Protocol (LDAP) connection in a controller resets. The controller is unable to authenticate or query the users using the LDAP server. **Scenario**: This issue is observed when a search request from a controller to an LDAP server is redirected to another LDAP server that does not support anonymous queries. This issue is not limited to any specific controller model or ArubaOS version. **Workaround**: Ensure that the referred LDAP server support anonymous queries.	LDAP	All platforms	ArubaOS 6.4.2.12

Table 5: *Known Issues in 6.4.4.5*

Bug ID	Description	Component	Platform	Reported Version
129464	**Symptom**: Clients take long time to connect after High Availability (HA) failover. The log file for the event lists the reason as, Station Up Message to Controller Timed Out. **Scenario**: This issue is observed in controllers running ArubaOS 6.4.3.2. **Workaround**: None.	AP-Wireless	All platforms	ArubaOS 6.4.3.2
129535 134047	**Symptom**: Access points do not receive LLDP packets from LAN ports. **Scenario**: This issue occurs because the BRCM header is positioned after the Ethernet header. This issue is observed in access points connected to controllers running ArubaOS 6.4.3.3. **Workaround**: None.	AP-Platform	All platforms	ArubaOS 6.4.3.3
130981	**Symptom**: A controller reboots. The log file for the event lists the reason as **datapath timeout**. **Scenario**: This issue occurs when a copy command with **** characters at the end of a command is executed. This issue is observed in controllers running ArubaOS 6.4.4.0. **Workaround**: None.	Controller-Platform	All platforms	ArubaOS 6.4.4.0
130983	**Symptom**: The Policy Based Routing (PBR) configuration in a standby controller is not retained after saving the configuration in a master controller. **Scenario**: This issue is observed in standby controllers running ArubaOS 6.4.4.1 in master-standby topology. **Workaround**: None.	Controller-Datapath	All platforms	ArubaOS 6.4.4.1
131118 133267	**Symptom**: : A controller reboots. The log file for the event lists the reason as **datapath timeout because of IP fragmentation**. **Scenario**: This issue is observed in 600 Series, 3000 Series, and M3 controllers running ArubaOS 6.4.x. **Workaround**: None.	Controller-Datapath	600 Series, 3000 Series, and M3controllers	ArubaOS 6.4.2.5

Table 5: *Known Issues in 6.4.4.5*

Bug ID	Description	Component	Platform	Reported Version

131445	**Symptom**: When roaming using 802.11r fast handoff, clients get an IP address from a Virtual Local Area Network (VLAN) mapped in the Virtual Access Point (VAP) profile although they are supposed to get an IP address from a VLAN derived from Vendor Specified Attribute (VSA).
	Scenario: This issue is observed for 802.1X authenticated clients when they roam using 802.11r fast handoff. This issue is observed in controllers running ArubaOS 6.3.x or ArubaOS 6.4.x.
	Workaround: Disable 802.11r capability from the SSID profile by using the following CLI commands:
	`(host) (config) #wlan ssid-profile default`
	`(host) (SSID Profile "default") #no dot11r-profile`
		Base OS Security	All platforms	ArubaOS 6.4.3.4

131815 131874 132843 133107	**Symptom**: The **Monitoring** page in the WebUI displays incorrect count of active clients when searched with filters like ESSID. Additionally, the **show ipv4 user-table rows <starting-row-number> <number-of-rows>** command displays more records than the pagination count. **Scenario**: This issue is caused by wrong application of filters on user entries. This issue is observed in controllers running ArubaOS 6.4.2.14 or later versions. **Workaround**: None.	WebUI	All platforms	ArubaOS 6.4.2.14
132382	**Symptom**: Users could not add a user name with **‘** character (apostrophe) in the RAP whitelist database using the WebUI. **Scenario**: This issue occurs because of a previous entry that is enclosed in ' characters (single quotes). This issue is observed in master controllers running ArubaOS 6.4.2.x in master-standby topology. **Workaround**: Do not use the ' character in the username field when making changes in the WebUI.	WebUI	All platforms	ArubaOS 6.4.2.3

Table 5: *Known Issues in 6.4.4.5*

Bug ID	Description	Component	Platform	Reported Version
133564	**Symptom**: AP-125 access points reboot. The log files for the event lists the reason as **Reboot caused by kernel page fault at virtual address 0000000100000007, epc == ffffffff80268c20, ra == ffffffff80268ba8**. **Scenario**: This issue is observed in AP-125 access points connected to controllers running ArubaOS 6.4.4.3. **Workaround**: None.	AP-Platforms	AP-125 access points	ArubaOS 6.4.4.3
134723	**Symptom**: A wired client does not complete wired EAP authentication in bridge mode with AP-205H access points. **Scenario**: This issue is observed in AP-205H access points connected to controllers running ArubaOS 6.4.3.6. **Workaround**: None..	AP-Platfroms	AP-205H access points	ArubaOS 6.4.3.6
134884 135077	**Symptom**: The **Uptime** value for some access points are displayed incorrectly in the **Monitoring > Controller > AccessPoints** page of the WebUI. **Scenario**: This issue occurs when the access points are in IP state for more than 35 days in a controller. This issue is observed in controllers running ArubaOS 6.4.2.14. **Workaround**: Execute the following CLI command to view the correct **Uptime** value (in the **tot-t** column of the output) of the access points on the controller: `(host) #show ap bss-table`	WebUI	All platforms	ArubaOS 6.4.2.14

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

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

- AP LLDP profile is not supported on 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 (600 Series, 3200XM, 3400, 3600, M3, 7000 Series, and 7200 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 Multi Network on page 1.)

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 1 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 1 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 1 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 1.

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 6.4.4.5

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 6.4.4.5

The following sections provide the procedures for upgrading the controller to ArubaOS 6.4.4.5 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 29.

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 6.4.4.5.

- For controllers 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 to ArubaOS 6.4.4.5 on page 32 to install the interim version of ArubaOS, and then repeat steps 1 through 11 of the procedure to download and install ArubaOS 6.4.4.5

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 6.4.4.5 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 1 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 29.

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 to ArubaOS 6.4.4.5 on page 32.

Follow steps 2 through 7 of the procedure described in Upgrading to ArubaOS 6.4.4.5 on page 32 to install the interim version of ArubaOS, and then repeat steps 1 through 7 of the procedure to download and install ArubaOS 6.4.4.5

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 6.4.4.5 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
   ```
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 Seriescontrollers.

6. Execute the **show image version** command to verify that the new image is loaded.
   ```
   (host)# show image version
   ```
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 1 for information on creating a backup.

Downgrading

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

CAUTION

If you upgraded from ArubaOS 3.3.x to ArubaOS 5.0, the upgrade script encrypts the internal database. New entries created in ArubaOS 6.4.4.5 are lost after the downgrade (this warning does not apply to upgrades from ArubaOS 3.4.x to ArubaOS 6.1).

CAUTION

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 6.4.4.5 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.

CAUTION

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 1.
2. Verify that the control plane security is disabled.
3. Set the controller to boot with the previously saved pre-ArubaOS 6.4.4.5 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 6.4.4.5 flash backup from the file stored on the controller. Do not restore the ArubaOS 6.4.4.5 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 6.4.4.5, the changes do not appear in RF Plan in the downgraded ArubaOS version.
   - If you installed any certificates while running ArubaOS 6.4.4.5, 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 6.4.4.2. Partition 0, the default boot partition, contains the ArubaOS 6.4.4.5 image.

   ```
   #show image version
   ```

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.