ArubaOS 6.4.4.2

aruba®
NETWORKS
an HP 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 Company. To obtain such source code, send a check or money order in the amount of US $10.00 to:

Hewlett-Packard Company

Attn: General Counsel

3000 Hanover Street

Palo Alto, CA 94304

USA

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

ArubaOS 6.4.4.2 is a software patch release that includes new features and enhancements along with fixes to issues identified in previous releases.

Chapter Overview

- New Features on page 7 provides a description of features and enhancements introduced in this release.
- Regulatory Updates on page 8 lists the regulatory updates introduced in this release.
- Resolved Issues on page 9 lists and describes the issues resolved in this release.
- Known Issues and Limitations on page 14 lists and describes the known and outstanding issues identified in this release.
- Upgrade Procedure on page 19 describes the procedures for upgrading a controller to this release.

Important Points to Remember

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

AirGroup

Support for Wired Users

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

AP Settings Triggering a Radio Restart

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

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

Profile	Settings
802.11a/802.11g Radio Profile	• 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

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 6.4.4.2 Web User Interface (WebUI):

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

Contacting Support

Table 2: *Contact Information*

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

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

AP-Platform

Novatel U620L USB Modem

This release introduces support for the Novatel MiFi 4G LTE Global USB Modem – U620L. This USB modem is supported in AP-205H, AP-210 Series, AP-220 Series, and RAP-155.

IPsec

Deterministic Random Bit Generator

In ArubaOS FIPS builds, the Pseudo Random Number Generator (PRNG) is changed so that all calls to the legacy FIPS 186-2 RNG (covered by FIPS RNG certificate number 1343) are redirected to the Deterministic Random Bit Generator (DRBG) module (covered by FIPS DRBG certificate number 715). This change lets ArubaOS to be compliant with FIPS 140-2 transition rules for 2015.

Chapter 3
Regulatory Updates

This chapter describes the regulatory update in this release.

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

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

The following Downloadable Regulatory Table (DRT) file versions are supported in ArubaOS 6.4.4.2:

- DRT-1.0_52480

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

This chapter describes the issues resolved in this release.

AP-Platform

Table 3: *AP-Platform Resolved Issues*

Bug ID	Description
125640 125642 125643 125781	**Symptom:** AP-125 access points stopped responding and rebooted. The log files for the event listed the reason as **Reboot caused by kernel page fault at virtual address 00000000000000a8, epc == ffffffff80288cb8, ra == ffffffff8029fb04**. This issue is resolved by improving the Ethernet driver of the access point. **Scenario:** This issue was observed in AP-125 access points connected to controllers running ArubaOS 6.4.2.6. **Platform:** AP-125 access points. **Reported Version:** ArubaOS 6.4.2.6.
125777	**Symptom:** AP-125 access points stopped responding and rebooted. The log files for the event listed the reason as **Data bus error, epc == c000000000148330, ra == c000000000163bcc**. This issue is resolved by improving the wireless driver. **Scenario:** This issue was observed in AP-125 access points connected to controllers running ArubaOS 6.4.2.6. **Platform:** AP-125 access points. **Reported Version:** ArubaOS 6.4.2.6.

AP-Wireless

Table 4: *AP-Wireless Resolved Issues*

Bug ID	Description
116969	**Symptom:** The basic and beacon rates configuration for the VAPs of AP-325 access points was not specific to each SSID. This issue is resolved by enabling the beacon rates separately for different VAPs. **Scenario:** This issue was observed in AP-325 access points connected to controllers running ArubaOS 6.4.4.0. **Platform:** AP-325 access points. **Reported Version:** ArubaOS 6.4.4.0.
122088	**Symptom:** There was no Signal-to-Noise (SNR) for the fourth chain in the **debug client-stats off** or the **radio stats** command. This issue is resolved by adding the last SNR received to the fourth chain in the command. **Scenario:** This issue was observed in 3600 controllers running ArubaOS 6.4.4.0. **Platform:** 3600 controllers. **Reported Version:** ArubaOS 6.4.4.0.
122814	**Symptom:** A type 9 radar was detected multiple times. This issue is resolved by removing the signal with first pulse interval. **Scenario:** This issue was observed in access points connected to controllers running ArubaOS 6.4.2.6. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.2.6.

Table 4: *AP-Wireless Resolved Issues*

Bug ID	Description
123677	**Symptom:** Type 5 and type 7 radars were detected multiple times. This issue is resolved by eliminating type 5 and type 6 radars from the country codes. **Scenario:** This issue was observed in AP-214 access points connected to controllers running ArubaOS 6.4.2.6. **Platform:** AP-214 access points. **Reported Version:** ArubaOS 6.4.2.6.
124944	**Symptom:** AP-204 and AP-205 access points did not forward the packets received on the uplink port. This issue was caused by the unwanted bytes in a packet during Cyclic Redundancy Check 32 (CRC32). This issue is resolved by improving the means by which the SKBs are accessed during CRC32. **Scenario:** This issue was observed when CRC32 was distributed across two SKBs. This issue was observed in controllers running ArubaOS 6.4.2.6. **Platform:** AP-204 and AP-205access points. **Reported Version:** ArubaOS 6.4.2.6.
125889	**Symptom:** Pre-Shared Key (PSK) clients failed to associate with an access point. The log files for the event listed the reason as **Capability requested by STA unsupported by AP**. This issue is resolved by sending a VLAN discovery message when the VAP profile configuration changes. **Scenario:** This issue was observed when the VAP profile configuration was changed in a controller and the VAP profile did not have a VLAN assigned. This issue was observed in controllers running ArubaOS 6.4.2.x or ArubaOS 6.4.3.x. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.2.9.

AirGroup

Table 5: *AirGroup Resolved Issues*

Bug ID	Description
126646	**Symptom:** The multicast DNS (mDNS) module crashed in a controller. This issue is resolved by checking for the existence of a cleanup service and ending a timer to free the cleanup service. **Scenario:** This issue was observed when a full configuration synchronization occurred in a controller after 1 minute of disabling any AirGroup service. This issue was observed in controllers running ArubaOS 6.4.4.0 in master-local or VRRP topology. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.4.0.
128170	**Symptom:** When an AirGroup service was deleted, the multicast (DNS) mDNS module crashed in a controller. This issue is resolved by assigning a NULL value to a list after it is removed. **Scenario:** This issue was observed because a list was created when an AirGroup service was disabled and a NULL value was not assigned to the list when the list was removed. Later, if the same AirGroup service was deleted, the mDNS module crashed when it tried to access a list which was removed but not assigned a NULL value. This issue was observed in controllers running ArubaOS 6.4.4.2. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.4.2.

Base OS Security

Table 6: *Base OS Security Resolved Issues*

Bug ID	Description
112521 124886 125129 125567 126381	**Symptom:** The CPU usage for the authentication process spiked to 99% or 100%. Many clients did not complete the 802.1X authentication, especially during the busy hours. Although some users completed the 802.1X authentication, their user entries were not created. This issue is resolved by redesigning the 802.1X reauthentication to avoid a large list of timers. The reauthentication table entry expiration time is periodically compared with the current time to appropriately trigger 802.1X reauthentication within 2 minutes of the reauthentication interval. **Scenario:** This issue was observed when reauthentication was enabled in the 802.1X authentication profile and there were large number of users in the reauthentication table. As the number of users for reauthentication increased, the authentication process slowed down. Although the 802.1X authentication throughput rate was low, the CPU load for the authentication process spiked to a value above 90%. It took many CPU cycles to maintain the timers in a system with a large number of timers. Hence, many clients failed the 802.1X authentication or user entries were not created for those users who completed the 802.1X authentication, especially during the busy hours. This issue was observed in controllers running ArubaOS 6.4.2.4. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.2.4.
124441	**Symptom:** Output modifiers were not allowed for the **show firewall dns-names** command. This issue is resolved by allowing the output modifiers for the command. **Scenario:** This issue was observed in controllers running ArubaOS 6.4.2.8. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.2.8.
125987	**Symptom:** The authentication module crashed in a controller when processing messages for split-tunnel wired users. This issue is resolved by improving the means of retrieving the AAA profile. **Scenario:** This issue was observed because of a buffer overrun when accessing the AAA profile. This issue was observed in controllers running ArubaOS 6.4.3.2. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.3.2.

Captive Portal

Table 7: *Captive Portal Resolved Issues*

Bug ID	Description
121389	**Symptom:** When the Captive Portal (CP) certificate was changed from one custom certificate to another, the default certificate was used instead of the new custom certificate. This issue is resolved by adding a sleep timer between changes to the custom certificate. **Scenario:** This issue was observed because of a timing mismatch between changes to the custom certificate. This issue was observed in controllers running ArubaOS 6.4.3.2. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.3.2.

Controller-Platform

Table 8: *Controller-Platform Resolved Issues*

Bug ID	Description
122167	**Symptom:** An error message was displayed when calculating the authentication server response time. This issue is resolved by changing the log level of the error message from ERROR to DEBUG. **Scenario:** This issue was observed when an incorrect timestamp value was retrieved. This issue was observed in controllers running ArubaOS 6.4.2.8. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.2.8.

DHCP

Table 9: *DHCP Resolved Issues*

Bug ID	Description
122270	**Symptom:** The **write mem** command failed if there was a large number of DHCP pools in the controller. This issue is resolved by sending the configuration from the DHCP module to the CLI engine in multiple chunks that are smaller than 40 KB. **Scenario:** This issue was observed because a chunk of configuration exceeded 40 KB, the upper size limit of the message. This issue was observed in controllers running ArubaOS 6.4.2.8. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.2.8.

SNMP

Table 10: *SNMP Resolved Issues*

Bug ID	Description
124869	**Symptom:** The object identifiers displayed an incorrect number of power supply units. This issue is resolved by correcting the number of power supply units supported by a controller. **Scenario:** This issue was observed in 3000 Series controllers running ArubaOS 5.0.4.14. **Platform:** 3000 Series controllers. **Reported Version:** ArubaOS 5.0.4.14.

UCC

Table 11: *UCC Resolved Issues*

Bug ID	Description
126484	**Symptom:** The datapath module crashed in a controller. This issue is resolved by adding a check that avoids memory access beyond the buffer size. **Scenario:** This issue was observed when some attributes were absent in the STUN message for Facetime calls which led to memory access beyond the buffer size. This issue was observed in controllers running ArubaOS 6.4.4.0. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.4.0.

VRRP

Table 12: *VRRP Resolved Issues*

Bug ID	Description
114245	**Symptom:** A VRRP standby controller sometimes became the master controller. This issue is resolved by enhancing the VRRP timer logic. **Scenario:** This issue was observed because of an error in the VRRP timer logic. This issue was observed in 600 Series controllers running ArubaOS 6.3.1.2. **Platform:** 600 Series controllers. **Reported Version:** ArubaOS 6.3.1.2.

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

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

Support for AP-320 Series Access Points

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

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

AP-Datapath

Table 13: *AP-Datapath Known Issues*

Bug ID	Description
126237	**Symptom:** A wrong **BS** tag is applied for split-tunnel BSSID. Users do not obtain IP address and user traffic fails. **Scenario:** This issue is observed when a split-tunnel VAP is added with **BS** flag which indicates that the VAP is in both bridge and split-tunnel modes. This issue is observed in controllers running ArubaOS 6.4.1.12. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.1.12. **Workaround:** Do not enable split-tunnel mode VAPs and bridge mode VAPs simultaneously on the same access point.

AP-Platform

Table 14: *AP-Platform Known Issues*

Bug ID	Description
121629 124058	**Symptom:** AP-125 access points stop responding and reboot. The log files for the event list the reason as **NMI watchdog interrupt**. **Scenario:** This issue is observed in AP-125 access points connected to controllers running ArubaOS 6.4.2.6. **Platform:** AP-125 access points. **Reported Version:** ArubaOS 6.4.2.6. **Workaround:** None.

AP-Wireless

Table 15: *AP-Wireless Known Issues*

Bug ID	Description
124572	**Symptom:** The default threshold limit of transmission retries is reached and the jitter increases when voice calls are made from Intel 7260 802.11ac clients that are connected to AP-135 access points. **Scenario:** This issue is observed in AP-135 access points connected to controllers running ArubaOS 6.4.2.6. **Platform:** AP-135 access points. **Reported Version:** ArubaOS 6.4.2.6. **Workaround**: None.
126690	**Symptom:** Dell Latitude laptops do not obtain IP addresses when they are associated with AP-225 access points with PSK/WPA2-AES enabled. **Scenario**: This issue is observed when HT is disabled on the G band of the radio profile, HT is enabled in the SSID profile, and the access point is rebooted. This issue is observed in AP-225 access points connected to controllers running ArubaOS 6.4.2.12. **Platform**: AP-225 access points. **Reported Version**: ArubaOS 6.4.2.12. **Workaround**: After the access point boots, enable HT on the G band of the radio profile and then disable it.

AirGroup

Table 16: *AirGroup Known Issues*

Bug ID	Description
126433	**Symptom:** A controller reboots and displays the error **Nanny rebooted machine - fpapps process died**. **Scenario:** This issue is observed when changing a user list policy in ClearPass Policy Manager (CPPM) from one user to another and deleting the earlier user within 5 seconds after changing the policy. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.3.10. **Workaround:** None.
126926	**Symptom:** Chromecast applications do not work when AirGroup is enabled in a controller. **Scenario:** This issue is observed because of a change in the Google cast support to application queries for Chromecast. This issue is observed in controllers running ArubaOS 6.4.x or later versions of ArubaOS. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.2.10. **Workaround:** None.

Base OS Security

Table 17: *Base OS Security Known Issues*

Bug ID	Description
125232	**Symptom:** The user-role information and ACL-related configuration are lost when a controller reboots. **Scenario:** This issue is observed when controllers with a large time-range configuration reboot and the user-role information and ACL-related configuration are not saved. This issue is observed in controllers running ArubaOS 6.4.2.8. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.2.8. **Workaround:** Reduce the size of the time-range configuration.
126713	**Symptom:** A controller forwards the authentication requests to an out-of-service authentication server. **Scenario:** This issue is observed when an authentication server goes out of service after authenticating a user and the same authentication server is used for the next instance of authentication. This issue is observed in controllers running ArubaOS 6.4.2.5. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.2.5. **Workaround:** Add a check to ensure that the authentication server is in service.

Controller-Datapath

Table 18: *Controller-Datapath Known Issues*

Bug ID	Description

122939	**Symptom:** AP-2xx Series access points experience amplified packet loss during voice calls.
	Scenario: This issue is observed when spectrum monitoring is enabled on access points. This issue is observed in AP-2xx Series access points connected to controllers running ArubaOS 6.4.2.x, ArubaOS 6.4.3.x, or ArubaOS 6.4.4.x.
	Platform: AP-2xx Series access points.
	Reported Version: ArubaOS 6.4.2.5.
	Workaround: Disable spectrum monitoring. In the following example, spectrum monitoring is disabled for 802.11a radio profile:
	`(host)(config) #rf dot11a-radio-profile default`
	`(host) (802.11a radio profile "default") #no spectrum-monitoring`

126736	**Symptom:** Home Agent/Foreign Agent (HA/FA) configuration does not work with anchor table and clients that send DHCP discover with unicast flag. **Scenario:** This issue is observed in controllers running ArubaOS 6.4.3.4. **Platform**: All platforms. **Reported Version**: ArubaOS 6.4.3.4. **Workaround**: None.

DDS

Table 19: *DDS Known Issues*

Bug ID	Description
125225	**Symptom:** The DDS module shows high CPU utilization. **Scenario:** This issue is observed in 7240 controllers running ArubaOS 6.4.2.4. **Platform:** 7240 controllers. **Reported Version:** ArubaOS 6.4.2.4. **Workaround:** None.

IPv6

Table 20: *IPv6 Known Issues*

Bug ID	Description
125261	**Symptom:** High datapath utilization is observed in a controller. **Scenario:** This issue is observed when a network is flooded with unsolicited Neighbor Advertisement (NA) packets. This issue is observed in controllers running ArubaOS 6.4.3.1. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.3.1. **Workaround:** Add an ACL rule to deny unsolicited NA packets.

Mesh

Table 21: *Mesh Known Issues*

Bug ID	Description
124682 126989	**Symptom:** The broadcast traffic from a client or switch to the Ethernet 0 port of a mesh point is sent back. **Scenario:** This issue with broadcast traffic is observed in mesh networks when a client or switch is connected to the Ethernet 0 port of a mesh point. This issue is observed in controllers running ArubaOS 6.4.3.2. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.3.2. **Workaround:** None.

Station Management

Table 22: *Station Management Known Issues*

Bug ID	Description
124275	**Symptom:** All clients obtain an IP address from the same VLAN even though a RADIUS server Vendor-Specific Attribute (VSA) specifies a VLAN pool with multiple VLANs. **Scenario:** This issue is observed when a RADIUS server VSA overrides the VAP VLANs 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. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.2.6. **Workaround:** Change the VLAN assignment type from **Even** to **Hash**. In the following example, the VLAN assignment type is changed from **Even** to **Hash** by using the CLI: `(host) (config) #vlan-name <name> assignment hash`

WebUI

Table 23: *WebUI Known Issues*

Bug ID	Description
125862	**Symptom:** A user is unable to add a VLAN to the port channel in the **Trunk** mode through the WebUI. **Scenario:** This issue is observed in both master and local controllers running ArubaOS 6.4.2.5 in master-standby-local topology. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.2.5. **Workaround:** Use the CLI instead of the WebUI.

XML API

Table 24: *XML API Known Issues*

Bug ID	Description
102974 114831	**Symptom:** The authentication manager process crashes for bridge Captive Portal (CP) users. **Scenario:** This issue is observed when a reauthentication timer expires after the user table is emptied. This issue is observed in controllers running ArubaOS 6.4.0.3. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.0.3. **Workaround:** None.

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

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

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

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

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

- ArubaOS 6.4.x supports only the newer MIPS controllers (7200 Series, 7000 Series, M3, 3200XM, 3400, 3600, and 600 Series). Legacy PPC controllers (200, 800, 2400, SC1/SC2) and 3200 controllers are not supported. Do not upgrade to ArubaOS 6.4.x if your deployment contains a mix of MIPS and PPC controllers in a master-local setup.
- When upgrading the software in a multicontroller network (one that uses two or more Aruba controllers), special care must be taken to upgrade all the controllers in the network and to upgrade them in the proper sequence. (See Upgrading in a Multicontroller Network on page 23.)

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 21 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 21 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 21 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 21.

NOTE

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 6.4.4.2

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

Instructions on Installing FIPS Software

Follow the steps below 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 6.4.4.2

The following sections provide the procedures for upgrading the controller to ArubaOS 6.4.4.2 by using the WebUI or 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 21.

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 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 6.4.4.2.

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

Follow step 2 to step 11 of the procedure described in Upgrading From a Recent Version of ArubaOS on page 24 to install the interim version of ArubaOS, and then repeat steps 1 through 11 of the procedure to download and install ArubaOS 6.4.4.2.

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 6.4.4.2 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. 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.

Note that the 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 21 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 21.

Upgrading From an Older Version of ArubaOS

Before you begin, verify the version of ArubaOS currently running on your controller. For more information, see Upgrading From an Older Version of ArubaOS on page 23.

Follow steps 2 through 7 of the procedure described in Upgrading From a Recent Version of ArubaOS on page 25 to install the interim version of ArubaOS, and then repeat steps 1 through 7 of the procedure to download and install ArubaOS 6.4.4.2.

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

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

or

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

or

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

4. Execute the **show image version** command to check if the ArubaOS images are loaded on the controller's flash partitions. The partition number appears in the **Partition** row; **0:0** is partition 0, and **0:1** is partition 1. The active boot partition is marked as **Default boot**.

```
(host) #show image version
---------------------------------
Partition               : 0:0 (/dev/ha1)
Software Version        : ArubaOS 6.1.1.0 (Digitally Signed - Production Build)
Build number            : 28288
Label                   : 28288
Built on                : Thu Apr 21 12:09:15 PDT 2012
---------------------------------
Partition               : 0:1 (/dev/hda2) **Default boot**
Software Version        : ArubaOS 6.1.3.2 (Digitally Signed - Production Build)
Build number            : 38319
Label                   : 38319
Built on                : Fri June 07 00:03:14 2013
```

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

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

or

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

or

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

or

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

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

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

```
(host)# show image version

---------------------------------
Partition               : 0:0 (/dev/hda1) **Default boot**
Software Version        : ArubaOS 6.4.4.2 (Digitally Signed - Production Build)
Build number            : 52482
Label                   : 52482
Built on                : Wed Nov 11 13:07:11 PDT 2015
---------------------------------
Partition               : 0:1 (/dev/hda2)
Software Version        : ArubaOS 6.4.3.0 (Digitally Signed - Production Build)
Build number            : 49296
Label                   : 49296
Built on                : Sun Mar 15 01:15:24 PDT 2015
```

7. Reboot the controller.

```
(host)# reload
```

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

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

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

1. Log in to the CLI to verify that all your controllers are up after the reboot.
2. Execute the **show ap active** command to determine if your APs are up and ready to accept clients.
3. Execute the **show ap database** command to verify that the number of access points and clients are what you expected.
4. Test a different type of client for each access method that you use and in different locations when possible.
5. Complete a backup of all critical configuration data and files on the compact flash file system to an external server or mass storage facility. See Backing up Critical Data on page 21 for information on creating a backup.

Downgrading

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

If you upgraded from ArubaOS 3.3.x to ArubaOS 5.0, the upgrade script encrypts the internal database. New entries created in ArubaOS 6.4.4.2 are lost after the downgrade (this warning does not apply to upgrades from ArubaOS 3.4.x to ArubaOS 6.1).

If you downgrade to a pre-6.1 configuration that was not previously saved, some parts of your deployment may not work as they previously did. For example, when downgrading from ArubaOS 6.4.4.2 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 21.
2. Verify that the control plane security is disabled.
3. Set the controller to boot with the previously saved pre-ArubaOS 6.4.4.2 configuration file.
4. Set the controller to boot from the system partition that contains the previously running ArubaOS image.

   When you specify a boot partition (or copy an image file to a system partition), the software checks to ensure that the image is compatible with the configuration file used on the next controller reload. An error message 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 6.4.4.2 flash backup from the file stored on the controller. Do not restore the ArubaOS 6.4.4.2 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 6.4.4.2, the changes do not appear in RF Plan in the downgraded ArubaOS version.
- If you installed any certificates while running ArubaOS 6.4.4.2, you need to reinstall the certificates in the downgraded ArubaOS version.

Downgrading Using the WebUI

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

1. If the saved preupgrade configuration file is on an external FTP/TFTP server, copy the file to the controller by navigating to the **Maintenance > File > Copy Files** page.
   a. For **Source Selection**, select FTP/TFTP server, and enter the IP address of the FTP/TFTP server and the name of the preupgrade configuration file.
   b. For **Destination Selection**, enter a file name (other than default.cfg) for Flash File System.
2. Set the controller to boot with your preupgrade configuration file by navigating to the **Maintenance > Controller > Boot Parameters** page.
   a. Select the saved preupgrade configuration file from the **Configuration File** drop-down list.
   b. Click **Apply**.
3. Determine the partition on which your previous software image is stored by navigating to the **Maintenance > Controller > Image Management** page. If there is no previous software image stored on your system partition, load it into the backup system partition (you cannot load a new image into the active system partition) by performing the following steps:
   a. Enter the FTP/TFTP server address and image file name.
   b. Select the backup system partition.
   c. Click **Upgrade**.
4. Navigate to the **Maintenance > Controller > Boot Parameters** page.
   a. Select the system partition that contains the preupgrade image file as the boot partition.
   b. Click **Apply**.
5. Navigate to the **Maintenance > Controller > Reboot Controller** page. Click **Continue**. The controller reboots after the countdown period.
6. When the boot process is complete, verify that the controller is using the correct software by navigating to the **Maintenance > Controller > Image Management** page.

Downgrading Using the CLI

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

1. If the saved preupgrade configuration file is on an external FTP/TFTP server, use the following command to copy it to the controller:

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

   or

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

2. Set the controller to boot with your preupgrade configuration file.

   ```
   (host) # boot config-file <backup configuration filename>
   ```

3. Execute the **show image version** command to view the partition on which your previous software image is stored. You cannot load a new image into the active system partition (the default boot).

   In the following example, partition 1, the backup system partition, contains the backup release ArubaOS 6.1.3.2. Partition 0, the default boot partition, contains the ArubaOS 6.4.4.2 image.

```
#show image version
----------------------------------
Partition               : 0:0 (/dev/hda1) **Default boot**
Software Version        : ArubaOS 6.4.4.2 (Digitally Signed - Production Build)
Build number            : 52482
Label                   : 52482
Built on                : Wed Nov 11 13:07:11 PDT 2015
----------------------------------
Partition               : 0:1 (/dev/hda2)
Software Version        : ArubaOS 6.1.3.2 (Digitally Signed - Production Build)
Build number            : 38319
Label                   : 38319
Built on                : Fri June 07 00:03:14 2013
```

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 recreate the problem.
8. Provide any wired or wireless sniffer traces taken during the time of the problem.
9. Provide the controller site access information, if possible.