ArubaOS 6.4.2.19

a Hewlett Packard
Enterprise company

Release Notes

Copyright Information

© Copyright 2017 Hewlett Packard Enterprise Development LP.

Open Source Code

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

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

Revision History

The following table lists the revisions of this document.

Table 1: *Revision History*

Revision	Change Description
Revision 01	Initial release.

ArubaOS 6.4.2.19 is a software patch release that includes fixes to the issues identified in previous ArubaOS releases.

NOTE

See the Upgrade Procedure on page 25 for instructions on how to upgrade your controller to this release.

Chapter Overview

- New Features on page 10 provides a description of features and enhancements introduced in ArubaOS 6.4.2.19.
- Regulatory Updates on page 12 describes the regulatory updates in ArubaOS 6.4.2.19.
- Resolved Issues on page 13 describes the issues resolved in ArubaOS 6.4.2.19.
- Known Issues on page 17 describes the known and outstanding issues identified in ArubaOS 6.4.2.19.
- Upgrade Procedure on page 25 describes the procedures for upgrading a controller to ArubaOS 6.4.2.19.
- Acronyms and Abbreviations on page 37 provides a list of acronyms and abbreviations used across this document.

NOTE

For information regarding prior releases, refer to the corresponding Release Notes on support.arubanetworks.com.

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.

AP Settings Triggering a Radio Restart

Changing the following settings triggers the radio to restart on the 200 Series, 210 Series, 220 Series, or 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

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

Profile	Settings
	▪ 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 6.4.2.19 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, 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	hpe.com/networking/support
End-of-life Information	arubanetworks.com/support-services/end-of-life/
Security Incident Response Team	Site: arubanetworks.com/support-services/security-bulletins/ Email: sirt@arubanetworks.com

This section describes the new features and/or enhancements introduced in ArubaOS 6.4.2.19. For more information about features, refer to the *ArubaOS 6.4.x User Guide*.

Modified Command

The following command is modified in ArubaOS 6.4.2.19.

aaa profile

The following new parameter is introduced in the **aaa profile** command:

Parameter	Description	Range	Default
max-ip ipv4 wireless <max_ipv4_users>	Control the number of IPv4 addresses that can be associated to single wireless user. **WARNING:** Increasing the **max-ip** limit may prevent the system from scaling to maximum users on all controllers. For more information, refer to Usage Guidelines on page 10.	1-32	2

Usage Guidelines

Changing the **max-ip ipv4 wireless** parameter from the default value is recommended for special deployments. If your WLAN has multiple device IPs associated to single MAC address, you can increase the value from the default value of 2.

The default value is 2 IPv4 users per wireless user, which means the total number of IPv4 users created can be a maximum of two times the license. If you configure 32 **max-ip** IPv4 users , then the total number of IPv4 users is 32 times the license. This can prevent the controller from scaling to the maximum limit of IP users. Total number of IPv4 users can be scaled down to offset this issue.

Increasing the value of the **max-ip ipv4 wireless** parameter may increase the look-up time due to an increase in the creation and deletion of IPv4 users on the controller. In a deployment where there is Captive Portal and 802.1X authentication implemented, increasing the number of IPv4 users may further deplete the performance.

Example

The following sample command configures 3 **max-ip ipv4** users for a wireless client in the AAA profile:

```
(host) (config) #aaa profile Max-IP
(host) (AAA Profile "Max-IP") #max-ip ipv4 wireless 3
```

Regulatory Updates

This topic describes the regulatory updates in ArubaOS 6.4.2.19.

NOTE

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.

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

The following default Downloadable Regulatory Table (DRT) version is part of ArubaOS 6.4.2.19:

- DRT-1.0_57815

This release includes the issues resolved in ArubaOS 6.4.2.19.

Table 4: *Resolved Issues in ArubaOS 6.4.2.19*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
122695 128425 134457	**Symptom**: A RAP failed to come online and the log file indicated the reason as **check_aruba_vid: STRAP License not available**. The fix ensures that the RAPs come up successfully. **Scenario**: This issue occurred after upgrading ArubaOS from a lower version without RAP configuration to a higher version with RAP configuration.	Licensing	All platforms	ArubaOS 6.4.4.1	ArubaOS 6.4.2.19
126440 127145 140733 144633	**Symptom:** Clients lost connectivity and were unable to send/receive traffic when debug log was enabled. This issue is resolved by removing the reason name mapping in the debug logs for the error codes received from the 802.11K beacon reports. **Scenario:** This issue occurred because the background code value that was mapped to the corresponding string for 802.11K beacon report was out of range. This issue was observed in controllers running ArubaOS 6.3.x or ArubaOS 6.4.x.	Station Management	All platforms	ArubaOS 6.3.1.14	ArubaOS 6.4.2.19
128916 132353 133884 138015	**Symptom:** Users were denied access to the network by the controller and the log file indicated the reason as **drop pkt as ip not assigned through dhcp**. The fix ensures that the DHCP enforcement is successful. **Scenario:** This issue occurred when the dhcp enforcement failed. This issue was observed in controllers running ArubaOS 6.3.1.16.	Controller-Datapath	All platforms	ArubaOS 6.3.1.6	ArubaOS 6.4.2.19
135949	**Symptom:** Bridge users failed to pass traffic. The fix ensures that the bridge users can successfully pass traffic.	AP-Datapath	All platforms	ArubaOS 6.4.3.6	ArubaOS 6.4.2.19

Table 4: *Resolved Issues in ArubaOS 6.4.2.19*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
	Scenario: This issue was observed when a vast number of users connected to a decrypt-tunnel forwarding mode virtual AP profile and then disconnected. The AP added L2 user entry for the decrypt-tunnel forwarding mode users. The AP did not delete the L2 user entries when the decrypt-tunnel forwarding mode clients disconnected. The user entries reached the maximum threshold and when the client tried to connect to the bridge virtual AP, the AP failed to create user entries for the bridge users. This issue was observed in controllers running ArubaOS 6.3.1.x, ArubaOS 6.4.2.x, ArubaOS 6.4.3.x, or ArubaOS 6.4.4.x.				
136349	**Symptom:** A controller sent the IP address in the port field and 0.0.0.0 as the remote address in a TACACS+ accounting packet, resulting in security warnings. The fix ensures that the controller sends the same IP address in the port field as well as the remote IP address. **Scenario:** This issue was observed when TACACS+ accounting was enabled for command execution and a user logged in using SSH. This issue was observed in controllers running ArubaOS 6.4.3.6.	TACACS	All platforms	ArubaOS 6.4.3.6	ArubaOS 6.4.2.19
139416 142197	**Symptom:** A client faced connectivity issue when an AP switched channels randomly. This issue is resolved by deleting a timer before it is started in AP mode only. **Scenario:** This issue occurred under the following circumstances: • Multiple AP-225 access points did not have wireless association for a long duration. • Excessive channel switching occurred because of RADAR detect trigger. • 5 GHz radio did not accept associations and transmission of frames was stalled until the AP was rebooted. This issue was observed in AP-225 access points running ArubaOS 6.4.2.14.	AP-Wireless	200 Series, 210 Series, 220 Series, and 270 Series access points	ArubaOS 6.4.2.14	ArubaOS 6.4.2.19
140923	**Symptom:** APs on a local controller rebooted and lost connectivity randomly. The fix ensures that the APs handle the ANQP queries from the clients appropriately when Hotspot 2.0 is enabled. **Scenario:** This issue occurred if Hotspot 2.0 was enabled on a virtual AP and when a client sent a malformed ANQP query to the AP. This issue was observed in APs running ArubaOS 6.2.2.0 or later versions.	Station Management	All platforms	ArubaOS 6.4.2.14	ArubaOS 6.4.2.19

Table 4: *Resolved Issues in ArubaOS 6.4.2.19*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
140057 142265 145485 150171	**Symptom:** An AP was unable to establish a GRE tunnel with the controller. The fix ensures that upon receiving the VLAN delete message, STM does not delete the virtual AP. **Scenario:** This issue occurred because the controller incorrectly deleted a virtual AP while deleting a user derived VLAN of the SSID. This issue was not limited to any specific controller model or ArubaOS version.	Station Management	All platforms	ArubaOS 6.4.2.14	ArubaOS 6.4.2.19
141567 147002 150219 150220 150221 150875 151246	**Symptom:** An Administrator was unable to blacklist a wireless client from the **Monitoring > CONTROLLER > Clients** page of the WebUI. The fix ensures that a client can be blacklisted using the WebUI. **Scenario:** This issue was observed in controllers running ArubaOS 6.4.x versions.	WebUI	All platforms	ArubaOS 6.5.0.0	ArubaOS 6.4.2.19
142682 144337	**Symptom:** An AP crashed and rebooted unexpectedly. The log file for the event listed the reason as **Reboot Reason: Reboot caused by kernel panic**. The fix ensures that the AP works as expected. **Scenario:** This issue occurred when the AP restarted and synchronized ACL configuration from the controller. This issue was observed in controllers running ArubaOS 6.4.4.8.	AP-Platform	All platforms	ArubaOS 6.4.4.8	ArubaOS 6.4.2.19
145486 146896 148292	**Symptom:** The configuration on the master controller failed to synchronize with the local controller. The fix ensures that the synchronization between the master and the local is successful. **Scenario:** Although centralized licensing was enabled and synchronized and licenses were available, access points displayed the **IL** flag, where **I** indicates inactive and **L** indicates unlicensed. This issue was observed in 7240 controllers running ArubaOS 6.4.3.7.	Master-Local	7240 controllers	ArubaOS 6.4.3.7	ArubaOS 6.4.2.19
145658	**Symptom:** A controller crashed when the size of /tmp/.fpcli_cfg_diff and /tmp/.fpcli_cfg_diff_enc temporary files increased. The issue is resolved by increasing the temporary files size limit to 1 MB. A warning message is also added to the output of **show configuration diff** command if the temporary file size crosses 1 MB. **Scenario:** This issue occurred when the ip routes were added and removed continuously using a script and the **write memory** command was not performed. This issue was observed in controllers running ArubaOS 6.3.1.18.	Controller-Platform	All platforms	ArubaOS 6.3.1.18	ArubaOS 6.4.2.19

Table 4: *Resolved Issues in ArubaOS 6.4.2.19*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
146685	**Symptom:** Clients experienced low throughput for specific SSIDs. This issue is resolved bymoving the unallocated bandwidth tokens into the shared pool. **Scenario:** This issue occurred when 3 virtual APs were enabled with no clients and ArubaOS recycled their bandwidth tokens and added them in the shared pool. However, when the 3 virtual APs were disabled, the shared pool was empty and the bandwidth tokens were lost. This issue was observed in controllers running ArubaOS 6.4.2.6.	AP-Wireless	All platforms	ArubaOS 6.4.2.6	ArubaOS 6.4.2.19
147195	**Symptom:** The value of **NAS-Port-Type** RADIUS attribute was incorrectly set to **"Wireless-IEEE802.11"(19)** instead of **"Ethernet"(15)** while authenticating RAP with external server. This issue is resolved by setting the value of **NAS-Port-Type** to **"Ethernet"(15)**. **Scenario:** This issue was observed in controllers running ArubaOS 6.3.1.16.	RADIUS	All platforms	ArubaOS 6.3.1.16	ArubaOS 6.4.2.19
148103	**Symptom:** One-way audio was observed in Vocera communication badges. The fix ensures that a redirect flag is added to a session if it belongs to a roamed client. **Scenario:** This issue was observed under the following circumstances: • The clients performed an L3 roaming. • The roamed client made a call to a client associated to the controller as a local client. For the roamed client, the controller acted as a foreign agent. Since, there was no Redirect flag, upstream traffic from the roamed client was not getting tunneled to home agent causing one way audio. This issue was observed in controllers running ArubaOS 6.4.2.x or later versions.	UCC	All platforms	ArubaOS 6.4.2.13	ArubaOS 6.4.2.19
148113	**Symptom:** A client failed to get an IP address when it roamed between APs. The fix ensures that the client gets an appropriate IP address when it roams between APs. **Scenario:** This issue was observed under the following circumstances: • L3 mobility was enabled globally. • Mobile-IP was disabled on the virtual AP. Mobile-IP changed the bridge entry even when the client roamed across APs terminating on the same controller. This issue was observed in controllers running ArubaOS 6.4.2.8.	Mobility	All platforms	ArubaOS 6.4.2.8	ArubaOS 6.4.2.19

Known Issues

This section describes the known and outstanding issues identified in ArubaOS 6.4.2.19.

Table 5: *Known Issues in ArubaOS 6.4.2.19*

Bug ID	Description	Component	Platform	Reported Version
104169	**Symptom:** The user fails to add Source Network Address Translation (SRC-NAT) using the controller WebUI when ESI policy is enabled. **Scenario:** This issue is observed in controllers running ArubaOS 6.3.x or ArubaOS 6.4.x. **Workaround:** None.	Policy-Based Routing	All platforms	ArubaOS 6.4.0.3
104570 106866	**Symptom:** The **Diagnostics** > **ACCESS POINT** > **System Status** page of the controller WebUI fails to display the status of the specified access point. **Scenario:** This issue is observed when the AP that belongs to an AP group contains multiple virtual AP profiles. This issue is not limited to any specific controller model or ArubaOS release version. **Workaround:** None.	WebUI	All platforms	ArubaOS 6.4.2.0
104874 139962 149550 150743 151483	**Symptom:** Stale entries are present in both the controller and the AP association tables but not in the AP driver's client table, or vice versa. **Scenario:** This issue may occur if APs are up for several weeks. This issue is not limited to any specific controller or AP model and ArubaOS release version. **Workaround:** Restart the STM process on the AP by executing the following command: `(host) (config) # ap process restart ap-name <name> stm`	Station Management	All platforms	ArubaOS 6.4.3.0
105935 141556	**Symptom:** VPN clients cannot connect to the network as the RADIUS authentication events match to an incorrect service. **Scenario:** This issue occurs because the controller sends the same VSAs to the RADIUS server for both VPN and non-VPN clients. This issue is not limited to any specific controller model or ArubaOS version. **Workaround:** None.	Base OS Security	All platforms	ArubaOS 6.4.3.0
111813	**Symptom:** SNMP **walk** and **get** operations stop working. **Scenario:** Executing the **snmp-server source controller-ip** command breaks the SNMP connectivity when IPv6 is disabled. This issue is not limited to any specific controller model and ArubaOS release version.	SNMP	All platforms	ArubaOS 6.4.2.3

Table 5: *Known Issues in ArubaOS 6.4.2.19*

Bug ID	Description	Component	Platform	Reported Version
	Workaround: None.			
112912	**Symptom:** When the **show inventory** command is executed, the **System Serial #** value is displayed as **Unknown**. **Scenario:** This issue occurs when **nvram lock** is held up by another process. This issue is observed in controllers running ArubaOS 6.4.x. **Workaround:** None.	Hardware Management	All platforms	ArubaOS 6.4.1.0
114495	**Symptom:** An AP incorrectly transmits DHCPv6 solicit messages instead of information-request messages. **Scenario:** This issue occurs in an IPv6 network when the **M** flag is set to 0 and the **O** flag is set to 1 in RA. This issue is observed in controllers running ArubaOS 6.4.2.3. **Workaround:** None.	AP-Platform	All platforms	ArubaOS 6.4.2.3
115260 128209	**Symptom:** When an administrator tries to hard reboot a controller, it fails to reboot with the error, **not enough space on flash**. **Scenario:** This issue occurs occasionally due to a database file corruption. This issue is observed in controllers running ArubaOS 6.4.2.3 or later versions. **Workaround:** Contact technical support to remove the corrupted database file.	Controller-Platform	All platforms	ArubaOS 6.4.2.12
115276 115418	**Symptom:** When clients connect to an AP that is configured in bridge forwarding mode age out, multiple RAPs crash unexpectedly. **Scenario:** This issue is observed in controllers running ArubaOS 6.4.2.2. **Workaround:** None.	AP-Wireless	All platforms	ArubaOS 6.4.2.2
117740	**Symptom:** An AP working in D-Tunnel or A-MPDU mode shows high channel utilization and clients receive frame rates lesser than 54 Mbps. **Scenario:** This issue is observed when software encryption is enabled in controllers running ArubaOS 6.4.2.6-FIPS. **Workaround:** None.	AP-Wireless	All platforms	ArubaOS 6.4.2.6
118120	**Symptom:** Multiple DHCP processes are running even when an AP is connected to the network with no DHCP configuration on the AP VLAN. **Scenario:** This issue is observed while configuring the static IPv6 address on the AP. This issue is observed in APs running ArubaOS 6.4.2.6 or later versions. **Workaround:** None.	AP-Platform	All platforms	ArubaOS 6.4.2.6

Table 5: *Known Issues in ArubaOS 6.4.2.19*

Bug ID	Description	Component	Platform	Reported Version
121020 124020 134232 138600 140885	**Symptom:** An AP crashes unexpectedly. The log file for the event lists the reason as **Reboot caused by kernel panic: Fatal exception**. **Scenario:** This issue occurs due to a memory leak in the APs. This issue is observed in 210 Series, 220 Series, 270 Series access points running ArubaOS 6.4.2.3. **Workaround:** None.	AP-Wireless	210 Series, 220 Series, 270 Series access points	ArubaOS 6.4.2.3

124136
138762
	Symptom: Clients fail 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 an HA setup, when no VLAN is assigned for the virtual AP profile that is configured in tunnel mode. This issue is observed in controllers running ArubaOS 6.4.2.5 or later versions.
	Workaround: Configure a VLAN ID in the virtual AP profile 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

124275 151661	**Symptom:** All clients continue to obtain IP addresses from the same VLAN even though a RADIUS server VSA specifies a VLAN pool with multiple VLANs. **Scenario:** This issue is observed when a RADIUS server VSA overrides the virtual AP VLANs with a different VLAN pool that is configured with the even assignment type. This issue is observed in a controller running ArubaOS 6.4.2.6 or later versions. **Workaround:** Change the VLAN assignment type from **even** to **hash** using the following CLI command: `(host) (config) #vlan-name <name> assignment hash`	Station Management	All platforms	ArubaOS 6.4.2.6
124286 129845 131026 153451	**Symptom:** The datapath process crashes in a controller. **Scenario:** This issue is observed in a controller running ArubaOS 6.4.3.1. **Workaround**: None.	Controller-Datapath	All platforms	ArubaOS 6.4.3.1
124767 124841	**Symptom:** Media traffic is not prioritized and call details are not visible for SIP calls on the UCC dashboard. **Scenario:** This issue is observed when large segmented SIP signaling messages are broken in to multiple segments and delivered out of order. This issue is not limited to any specific controller model or ArubaOS release version. **Workaround:** None.	Unified Communication	All platforms	ArubaOS 6.4.2.4
125862	**Symptom:** Users are unable to add a VLAN range to the port channel from the **Configuration > NETWORK >Ports >Port-Channel** page of the WebUI.	WebUI	All platforms	ArubaOS 6.4.2.5

Table 5: *Known Issues in ArubaOS 6.4.2.19*

Bug ID	Description	Component	Platform	Reported Version

	Scenario: This issue is observed in both master and local controllers in a master-standby-local topology running ArubaOS 6.4.x.
	Workaround: Add the VLAN to the port channel using the following CLI commands:
	`(host) (config) #interface port-channel <id>`
	`(host) (config-channel)#switchport trunk allowed vlan <vlan-range>`			

126926	**Symptom:** Few Google Chromecast applications do not work when AirGroup is enabled on the controller. **Scenario:** This issue occurs due to a change in the Google cast support to the applications query for Chromecast. This issue is observed in controllers running ArubaOS 6.4.x. **Workaround:** None.	AirGroup	All platforms	ArubaOS 6.4.2.10
127998 134133 146879	**Symptom:** A controller crashes unexpectedly. The log file for the event lists the reason as **Datapath timeout (Heartbeat Initiated) (Intent:cause:register 53:86:0:2c)**. **Scenario:** This issue occurs because the Ethernet driver does not allocate header room. This issue is observed in 7000 Series and 7200 Seriescontrollers running ArubaOS 6.4.2.x. **Workaround:** None.	Controller-Datapath	7000 Series and 7200 Seriescontrollers	ArubaOS 6.4.2.12
128552	**Symptom**: All clients lose connectivity when multiple clients switch to hardware sleep mode. **Scenario**: This issue is observed when multiple clients switch to hardware sleep mode without sending a deauthentication request for a duration equal to the ageout timer (default: 1000 seconds). This issue is observed in 200 Series, 210 Series, 220 Series, and 270 Series access points running ArubaOS 6.4.2.8. **Workaround:** None.	AP-Platform	200 Series, 210 Series, 220 Series, and 270 Series access points	ArubaOS 6.4.2.8
128916 132353 133884 138015	**Symptom:** Users are denied access by the controller and an error message **drop pkt as ip not assigned through dhcp** is displayed. **Scenario:** This issue occurs when the DHCP enforcement fails. This issue is observed in controllers running ArubaOS 6.3.1.16. **Workaround:** None.	Controller-Datapath	All platforms	ArubaOS 6.3.1.6
129096 148150	**Symptom:** The LDAP connection on the controller keeps resetting due to a search failure. As a result, 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 servers support anonymous queries.	LDAP	All platforms	ArubaOS 6.4.2.12

Table 5: *Known Issues in ArubaOS 6.4.2.19*

Bug ID	Description	Component	Platform	Reported Version
131118 133267	**Symptom**: A datapath timeout crash is observed in the controller. **Scenario**: The log files for the event indicates that the crash occurs when fragmented DHCP packets are received by datapath. This issue is observed in controllers running ArubaOS 6.4.x. **Workaround**: None.	Controller-Datapath	All platforms	ArubaOS 6.4.2.5

131445
136572
	Symptom: When roaming using 802.11r fast handoff, clients get an IP address from a VLAN mapped in the virtual AP profile although they are supposed to get an IP address from a VLAN derived from 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

132382	**Symptom**: If a username includes an apostrophe, users are unable to add it in the RAP whitelist database from the **Configuration > Wireless > AP Installation > Whitelist** page of the WebUI. **Scenario**: This issue is caused by a previous entry that is enclosed in single quotes. This issue is observed in a master controller running ArubaOS 6.4.2.3 or later versions in a master-standby topology. **Workaround**: Avoid using apostrophe in the username field when making changes in the WebUI. Alternately, you can use the CLI command to update the same: `(host) #whitelist-db rap add mac-address <mac address of the AP> ap-group <AP group name> ap-name <Name of the AP> description <description> full-name <username with apostrophe>`	WebUI	All platforms	ArubaOS 6.4.2.3
132814 141325 143132 151547	**Symptom:** An AP reboots unexpectedly. The log file for the event lists the reason as **reboot reason: Reboot caused by kernel panic**. **Scenario:** This issue is observed in 210 Series, 220 Series, or 270 Series access points running ArubaOS 6.4.2.6. **Workaround:** None.	AP-Wireless	210 Series, 220 Series, and 270 Series access points	ArubaOS 6.4.2.6
134147 150805	**Symptom:** Clients fail to discover Apple TV in an AirGroup-enabled network.	AirGroup	All platforms	ArubaOS 6.4.2.13

Table 5: *Known Issues in ArubaOS 6.4.2.19*

Bug ID	Description	Component	Platform	Reported Version

	Scenario: This issue is seen in a master-local topology when full synchronization of database is enabled on the master controller. During a full synchronization, AirGroup deletes all AirGroup services and restores it back, but does not delete the cache entries and resets the AirGroup server count to zero. This issue is observed in controllers running ArubaOS 6.4.2.13 or later versions.
	Workaround: Configure partial configuration synchronization on the master controller:
	`(host-master) (config) #cfgm set sync-type snapshot`
	`(host-master) (config) #write memory`
	Disable and enable AirGroup mDNS on each local controller:
	`(host-local) (config) #airgroup mdns disable`
	`(host-local) (config) #airgroup mdns enable`
	`(host-local) (config) #write memory`			

134646	**Symptom:** An **accounting-stop** message with wrong values is sent when posting an XML user-add request to a controller. **Scenario:** This issue occurs when the user-add request is posted to an authenticated Captive Portal user. The **accounting-stop** contains all zeroes and the framed IP address is 0.0.0.0. This issue is observed in controllers running ArubaOS 6.4.2.12. **Workaround:** None.	XML API	All platforms	ArubaOS 6.4.2.12
135029 137672 150310	**Symptom:** The **Monitoring > NETWORK > All Access Points** pages of the WebUI displays an incorrect user count. **Scenario:** There is a mismatch in the user count when seen in the **Monitoring** and **Dashboard** page of the WebUI. This issue is not seen in the CLI. This issue is observed in controllers running ArubaOS 6.4.2.12, ArubaOS 6.4.3.x, or ArubaOS 6.4.4.x. **Workaround:** Execute the following CLI command to view the actual client count: `(host) #show ap association`	WebUI	All platforms	ArubaOS 6.4.2.12
137196	**Symptom:** A controller fails to respond and reboots unexpectedly. The log file for the event lists the reason as **Reboot Cause: Datapath timeout**. **Scenario:** This issue occurs when VIA is used with SSL fallback. This issue is not limited to any specific controller model or ArubaOS version. **Workaround:** None.	Base OS Security	All platforms	ArubaOS 6.4.0.3
137549	**Symptom:** The **no export-route** parameter under the **aaa authentication vpn** command does not work as expected.	OSPF	All platforms	ArubaOS 6.4.2.13

Table 5: *Known Issues in ArubaOS 6.4.2.19*

Bug ID	Description	Component	Platform	Reported Version
	Scenario: This issue occurs because the inner IP of Instant AP VPN is distributed over OSPF after the **no export-route** parameter is configured under the **aaa authentication vpn** command. This issue is observed in controllers running ArubaOS 6.4.3.x or ArubaOS 6.4.4.x. **Workaround:** None.			
137617 143207 148674 150451 150737 153028 153679	**Symptom:** User is unable to access the WebUI. **Scenario:** The issue occurs when the HTTP process is busy, because of which the controller no longer responds to new incoming connections. This issue is observed in controllers running ArubaOS 6.4.3.5 or later versions. **Workaround:** None.	Web Server	All platforms	ArubaOS 6.4.3.5
138093	**Symptom:** The STM process crashes multiple times in the controller. **Scenario:** The backup LMS fails to handle a large number of AP fallback. The controller runs out of memory and fails to restart the STM process. This issue is observed in controllers running ArubaOS 6.4.2.x and ArubaOS 6.5.x. **Workaround:** None.	Station Management	All platforms	ArubaOS 6.4.2.8
140113 140886 144529 151560	**Symptom:** The controller user-table displays an incorrect user-role for a wireless client connected to an IAP in an IAP-VPN deployment. **Scenario:** This issue occurs because the controller fails to inherit the role from the previous user entry and derives an incorrect or new role for the client when it switches from one SSID to another across VLANs. **Workaround:** None.	RAP-NG	All platforms	ArubaOS 6.4.4.6
140327 144285 144288 144438 147584	**Symptom:** Memory usage of the **authentication** process in a controller increases gradually. **Scenario:** This issue occurs because of a slow memory leak. This issue is observed in controllers running ArubaOS 6.4.2.x or ArubaOS 6.4.3.x. **Workaround:** None.	Base OS Security	All platforms	ArubaOS 6.4.3.3
140582	**Symptom:** Some Vocera clients show Searching For Server (SFS) events after associating with an AP. **Scenario:** This issue is observed in M3controllers running ArubaOS 6.4.2.13. **Workaround:** None.	Unified Communications and Collaboration	M3controllers	ArubaOS 6.4.2.13
141822 143282	**Symptom:** The process handling authentication requests crashes due to a segmentation fault while sending RADIUS-accounting packets.	RADIUS	All AP platforms	ArubaOS 6.4.2.12

Table 5: *Known Issues in ArubaOS 6.4.2.19*

Bug ID	Description	Component	Platform	Reported Version
	Scenario: This issue occurs when you make the following changes to a AAA profile which is used by a client associated to the WLAN: • Modify the RADIUS accounting server-group assigned in the AAA profile to a different server-group. • Enable **multiple-server-accounting** which is originally disabled in the AAA profile. This issue is not limited to any specific controller model or ArubaOS version. **Workaround:** None.			
142678	**Symptom:** Adding an NTP server to the controller causes all the Instant AP VPN /RAP to reconnect without notification. Many Instant AP VPNs cannot recover as well. **Scenario:** This issue occurs when the NTP server tries to correct the time difference in the controller. This issue is not limited to any specific controller model or release version. **Workaround:** Reboot the controller after configuring the NTP server.	IPsec	All platforms	ArubaOS 6.4.2.13
143566	**Symptom:** The error **Module authentication is busy. Please try later.** is displayed when the command, **show reference user-role <role-name>** is executed. **Scenario:** This issue occurred when there were more than 212 entries for a given role in user derivation-rules or server-group derivation rules. This issue is observed in a master local topology with controllers running ArubaOS 6.4.2.16. **Workaround:** None.	Configuration	All platforms	ArubaOS 6.4.2.16
143836	**Symptom:** An Instant AP deployed as a campus AP, fails to come online on the controller using a 4G uplink. **Scenario:** This issue occurs when the AP uplink router MTU was changed to a value lesser than the length of the packet sent by the AP. This issue is observed in 100 Series access points running ArubaOS 6.4.2.12 or later versions. **Workaround:** None.	AP-Platform	100 Series access points	ArubaOS 6.4.2.12

144768
145436
	Symptom: Some APs reboot randomly with a reboot cause as **Critical process /aruba/bin/stm [pid 4040] DIED** when Hotspot 2.0 is enabled on a virtual AP.
	Scenario: This issue occurs when an AP receives and processes an invalid value in the ANQP query from a Hotspot 2.0 enabled client. This issue is observed in APs running ArubaOS 6.2.2 or later versions.
	Workaround: Disable Hotspot 2.0 from all the Hotspot profiles associated to any virtual AP. Execute the following command to disable Hotspot 2.0:
	`(host) (config) #wlan hotspot hs2-profile <profile-name>`
	`(host) (Hotspot 2.0 Profile "<profile-name>") #no hotspot-enable`
		Hotspot	All AP platforms	ArubaOS 6.4.2.17

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

CAUTION

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 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.
- If your controller is running ArubaOS 6.4.0.0 or later versions, do not use a Windows-based TFTP server to copy the ArubaOS image to the nonboot partition of the controller for upgrading or downgrading. Use FTP or SCP to copy the image.
- 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 following ACL, both ACE entries could not be configured in ArubaOS 6.4.x. When the second ACE is added, it overwrites the first.

```
(host) (config) #ip access-list session allowall-laptop
(host) (config-sess-allowall-laptop)# any any any  permit time-range test_range
(host) (config-sess-allowall-laptop)# any any any  deny
(host) (config-sess-allowall-laptop)#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 Multicontroller Network on page 29.)

GRE Tunnel-Type Requirements

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

- ArubaOS 6.4.2.19 continues to support L2 GRE tunnel type zero, but it is recommended to use a non-zero tunnel type.
- If both L2 and L3 tunnels are configured between endpoint devices, you must use a non-zero tunnel type for L2 GRE tunnels.

Important Points to Remember and Best Practices

Ensure a successful upgrade and optimize your upgrade procedure by taking the recommended actions provided in the following list. You should save this list for future use.

- Schedule the upgrade during a maintenance window and notify your community of the planned upgrade. This prevents users from being surprised by a brief wireless network outage during the upgrade.

- Avoid making any other changes to your network, such as configuration changes, hardware upgrades, or changes to the rest of the network during the upgrade. This simplifies troubleshooting.
- Know your network and verify the state of your network by answering the following questions:
  - How many APs are assigned to each controller? Verify this information by navigating to the **Monitoring > NETWORK > All Access Points** section of the WebUI, or by executing the **show ap active** and **show ap database** CLI commands.
  - How are those APs discovering the controller (DNS, DHCP Option, Broadcast)?
  - What version of ArubaOS is currently on the controller?
  - Are all controllers in a master-local cluster running the same version of software?
  - Which services are used on the controllers (employee wireless, guest access, remote AP, wireless voice)?
- Resolve any existing issues (consistent or intermittent) before you upgrade.
- If possible, use FTP to load software images to the controller. FTP is faster than TFTP and offers more resilience over slow links. If you must use TFTP, ensure the TFTP server can send over 30 MB of data.
- Always upgrade the non-boot partition first. If problems occur during the upgrade, you can restore the flash, and switch back to the boot partition. Upgrading the non-boot partition gives you a smoother downgrade path should it be required.
- Before you upgrade to this version of ArubaOS, assess your software license requirements and load any new or expanded licenses you may require. For a detailed description of these new license modules, refer to the “Software Licenses” chapter in the *ArubaOS 6.4.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.

CAUTION

In certain situations, a reboot or a shutdown could cause the controller to lose the information stored in its compact flash card. To avoid such issues, it is recommended that you 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 28 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 28 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 28 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 28.

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 6.4.2.19

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

Instructions on Installing FIPS Software

NOTE

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

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

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

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

Upgrading to ArubaOS 6.4.2.19

The following sections provide the procedures for upgrading the controller to ArubaOS 6.4.2.19 by using the WebUI and the CLI.

Install Using the WebUI

CAUTION

Confirm that there is at least 60 MB of free memory and at least 75 MB of flash space available for an upgrade using the WebUI. For details, see Memory Requirements on page 27.

NOTE

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

Upgrading From 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 6.4.2.19.

- 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 From a Recent Version of ArubaOS on page 31 to install the interim version of ArubaOS, and then repeat steps 1 through 11 of the procedure to download and install ArubaOS 6.4.2.19.

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
- 5.0.3.1 or latest version of 5.0.x
- 6.0.1.0 or later version of 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 6.4.2.19 from the customer support site.
2. Upload the new software image(s) to a PC or workstation on your network.
3. Validate the SHA hash for a software image:
   a. Download the **Aruba.sha256** file from the download directory.
   b. To verify the image, load the image onto a Linux system and execute the **sha256sum <filename>** command or use a suitable tool for your operating system that can generate a **SHA256** hash of a file.
   c. Verify that the output produced by this command matches the hash value found on the support site.

NOTE

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

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

NOTE

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 28 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

CAUTION

Confirm that there is at least 40 MB of free memory and at least 60 MB of flash space available for an upgrade using the CLI. For details, see Memory Requirements on page 27.

Upgrading From 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 30.

Follow steps 2 through 7 of the procedure described in Upgrading From a Recent Version of ArubaOS 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 6.4.2.19.

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

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

1. Download ArubaOS 6.4.2.19 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>
   ```

NOTE

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
   ```

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 28 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 6.4.2.19 are lost after the downgrade (this caution does not apply to upgrades from ArubaOS 3.4.x to ArubaOS 6.1).

CAUTION

If you do not downgrade to a previously saved pre-6.1 configuration, some parts of your deployment may not work as they previously did. For example, when downgrading from ArubaOS 6.4.2.19 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 28.
2. Verify that the control plane security is disabled.
3. Set the controller to boot with the previously saved pre-ArubaOS 6.4.2.19 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 6.4.2.19 flash backup from the file stored on the controller. Do not restore the ArubaOS 6.4.2.19 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 6.4.2.19, the changes do not appear in RF Plan in the downgraded ArubaOS version.

- If you installed any certificates while running ArubaOS 6.4.2.19, 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 6.4.2.19 image.

   ```
   (host) # 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.

The following table lists the acronyms and abbreviations used in Aruba documents.

Table 6: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
3G	Third Generation of Wireless Mobile Telecommunications Technology
4G	Fourth Generation of Wireless Mobile Telecommunications Technology
AAA	Authentication, Authorization, and Accounting
ABR	Area Border Router
AC	Access Category
ACC	Advanced Cellular Coexistence
ACE	Access Control Entry
ACI	Adjacent Channel interference
ACL	Access Control List
AD	Active Directory
ADO	Active X Data Objects
ADP	Aruba Discovery Protocol
AES	Advanced Encryption Standard
AIFSN	Arbitrary Inter-frame Space Number
ALE	Analytics and Location Engine

Table 6: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
ALG	Application Layer Gateway
AM	Air Monitor
AMON	Advanced Monitoring
AMP	AirWave Management Platform
A-MPDU	Aggregate MAC Protocol Data Unit
A-MSDU	Aggregate MAC Service Data Unit
ANQP	Access Network Query Protocol
ANSI	American National Standards Institute
AP	Access Point
API	Application Programming Interface
ARM	Adaptive Radio Management
ARP	Address Resolution Protocol
AVF	AntiVirus Firewall
BCMC	Broadcast-Multicast
BGP	Border Gateway protocol
BLE	Bluetooth Low Energy
BMC	Beacon Management Console
BPDU	Bridge Protocol Data Unit
BRAS	Broadband Remote Access Server

Table 6: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
BRE	Basic Regular Expression
BSS	Basic Service Set
BSSID	Basic Service Set Identifier
BYOD	Bring Your Own Device
CA	Certification Authority
CAC	Call Admission Control
CALEA	Communications Assistance for Law Enforcement Act
CAP	Campus AP
CCA	Clear Channel Assessment
CDP	Cisco Discovery Protocol
CDR	Call Detail Records
CEF	Common Event Format
CGI	Common Gateway Interface
CHAP	Challenge Handshake Authentication Protocol
CIDR	Classless Inter-Domain Routing
CLI	Command-Line Interface
CN	Common Name
CoA	Change of Authorization
CoS	Class of Service
CPE	Customer Premises Equipment

Table 6: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
CPsec	Control Plane Security
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
CRL	Certificate Revocation List
CSA	Channel Switch Announcement
CSMA/CA	Carrier Sense Multiple Access / Collision Avoidance
CSR	Certificate Signing Request
CSV	Comma Separated Values
CTS	Clear to Send
CW	Contention Window
DAS	Distributed Antenna System
dB	Decibel
dBm	Decibel Milliwatt
DCB	Data Center Bridging
DCE	Data Communication Equipment
DCF	Distributed Coordination Function
DDMO	Distributed Dynamic Multicast Optimization
DES	Data Encryption Standard
DFS	Dynamic Frequency Selection

Table 6: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
DFT	Discreet Fourier Transform
DHCP	Dynamic Host Configuration Protocol
DLNA	Digital Living Network Alliance
DMO	Dynamic Multicast optimization
DN	Distinguished Name
DNS	Domain Name System
DOCSIS	Data over Cable Service Interface Specification
DoS	Denial of Service
DPD	Dead Peer Detection
DPI	Deep Packet Inspection
DR	Designated Router
DRT	Downloadable Regulatory Table
DS	Differentiated Services
DSCP	Differentiated Services Code Point
DSSS	Direct Sequence Spread Spectrum
DST	Daylight Saving Time
DTE	Data Terminal Equipment
DTIM	Delivery Traffic Indication Message
DTLS	Datagram Transport Layer Security
DU	Data Unit

Table 6: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
EAP	Extensible Authentication Protocol
EAP-FAST	EAP-Flexible Authentication Secure Tunnel
EAP-GTC	EAP-Generic Token Card
EAP-MD5	EAP-Method Digest 5
EAP-MSCHAP EAP-MSCHAPv2	EAP-Microsoft Challenge Handshake Authentication Protocol
EAPoL	EAP over LAN
EAPoUDP	EAP over UDP
EAP-PEAP	EAP-Protected EAP
EAP-PWD	EAP-Password
EAP-TLS	EAP-Transport Layer Security
EAP-TTLS	EAP-Tunneled Transport Layer Security
ECC	Elliptical Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
EIGRP	Enhanced Interior Gateway Routing Protocol
EIRP	Effective Isotropic Radiated Power
EMM	Enterprise Mobility Management
ESI	External Services Interface
ESS	Extended Service Set

Table 6: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
ESSID	Extended Service Set Identifier
EULA	End User License Agreement
FCC	Federal Communications Commission
FFT	Fast Fourier Transform
FHSS	Frequency Hopping Spread Spectrum
FIB	Forwarding Information Base
FIPS	Federal Information Processing Standards
FQDN	Fully Qualified Domain Name
FQLN	Fully Qualified Location Name
FRER	Frame Receive Error Rate
FRR	Frame Retry Rate
FSPL	Free Space Path Loss
FTP	File Transfer Protocol
GBps	Gigabytes per second
Gbps	Gigabits per second
GHz	Gigahertz
GIS	Generic Interface Specification
GMT	Greenwich Mean Time
GPP	Guest Provisioning Page
GPS	Global Positioning System

Table 6: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
GRE	Generic Routing Encapsulation
GUI	Graphical User Interface
GVRP	GARP or Generic VLAN Registration Protocol
H2QP	Hotspot 2.0 Query Protocol
HA	High Availability
HMD	High Mobility Device
HSPA	High-Speed Packet Access
HT	High Throughput
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IAS	Internet Authentication Service
ICMP	Internet Control Message Protocol
IdP	Identity Provider
IDS	Intrusion Detection System
IE	Information Element
IEEE	Institute of Electrical and Electronics Engineers
IGMP	Internet Group Management Protocol
IGP	Interior Gateway Protocol
IGRP	Interior Gateway Routing Protocol

Table 6: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
IKE PSK	Internet Key Exchange Pre-shared Key
IoT	Internet of Things
IP	Internet Protocol
IPM	Intelligent Power Monitoring
IPS	Intrusion Prevention System
IPsec	IP Security
ISAKMP	Internet Security Association and Key Management Protocol
ISP	Internet Service Provider
JSON	JavaScript Object Notation
KBps	Kilobytes per second
Kbps	Kilobits per second
L2TP	Layer-2 Tunneling Protocol
LACP	Link Aggregation Control Protocol
LAG	Link Aggregation Group
LAN	Local Area Network
LCD	Liquid Crystal Display
LDAP	Lightweight Directory Access Protocol
LDPC	Low-Density Parity-Check
LEA	Law Enforcement Agency
LEAP	Lightweight Extensible Authentication Protocol

Table 6: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
LED	Light Emitting Diode
LEEF	Long Event Extended Format
LI	Lawful Interception
LLDP	Link Layer Discovery Protocol
LLDP-MED	LLDP–Media Endpoint Discovery
LMS	Local Management Switch
LNS	L2TP Network Server
LTE	Long Term Evolution
MAB	MAC Authentication Bypass
MAC	Media Access Control
MAM	Mobile Application Management
MBps	Megabytes per second
Mbps	Megabits per second
MCS	Modulation and Coding Scheme
MD5	Message Digest 5
MDM	Mobile Device Management
mDNS	Multicast Domain Name System
MFA	Multi-factor Authentication
MHz	Megahertz

Table 6: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
MIB	Management Information Base
MIMO	Multiple-Input Multiple-Output
MLD	Multicast Listener Discovery
MPDU	MAC Protocol Data Unit
MPLS	Multiprotocol Label Switching
MPPE	Microsoft Point-to-Point Encryption
MSCHAP	Microsoft Challenge Handshake Authentication Protocol
MSS	Maximum Segment Size
MSSID	Mesh Service Set Identifier
MSTP	Multiple Spanning Tree Protocol
MTU	Maximum Transmission Unit
MU-MIMO	Multi-User Multiple-Input Multiple-Output
MVRP	Multiple VLAN Registration Protocol
NAC	Network Access Control
NAD	Network Access Device
NAK	Negative Acknowledgment Code
NAP	Network Access Protection
NAS	Network Access Server Network-attached Storage
NAT	Network Address Translation

Table 6: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
NetBIOS	Network Basic Input/Output System
NIC	Network Interface Card
Nmap	Network Mapper
NMI	Non-Maskable Interrupt
NMS	Network Management Server
NOE	New Office Environment
NTP	Network Time Protocol
OAuth	Open Authentication
OCSP	Online Certificate Status Protocol
OFA	OpenFlow Agent
OFDM	Orthogonal Frequency Division Multiplexing
OID	Object Identifier
OKC	Opportunistic Key Caching
OS	Operating System
OSPF	Open Shortest Path First
OUI	Organizationally Unique Identifier
OVA	Open Virtual Appliance
OVF	Open Virtualization Format
PAC	Protected Access Credential

Table 6: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
PAP	Password Authentication Protocol
PAPI	Proprietary Access Protocol Interface
PCI	Peripheral Component Interconnect
PDU	Power Distribution Unit
PEAP	Protected Extensible Authentication Protocol
PEAP-GTC	Protected Extensible Authentication Protocol-Generic Token Card
PEF	Policy Enforcement Firewall
PFS	Perfect Forward Secrecy
PHB	Per-hop behavior
PIM	Protocol-Independent Multicast
PIN	Personal Identification Number
PKCS	Public Key Cryptography Standard
PKI	Public Key Infrastructure
PLMN	Public Land Mobile Network
PMK	Pairwise Master Key
PoE	Power over Ethernet
POST	Power On Self Test
PPP	Point-to-Point Protocol
PPPoE	PPP over Ethernet
PPTP	PPP Tunneling Protocol

Table 6: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
PRNG	Pseudo-Random Number Generator
PSK	Pre-Shared Key
PSU	Power Supply Unit
PVST	Per VLAN Spanning Tree
QoS	Quality of Service
RA	Router Advertisement
RADAR	Radio Detection and Ranging
RADIUS	Remote Authentication Dial-In User Service
RAM	Random Access Memory
RAP	Remote AP
RAPIDS	Rogue Access Point and Intrusion Detection System
RARP	Reverse ARP
REGEX	Regular Expression
REST	Representational State Transfer
RF	Radio Frequency
RFC	Request for Comments
RFID	Radio Frequency Identification
RIP	Routing Information Protocol
RRD	Round Robin Database

Table 6: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
RSA	Rivest, Shamir, Adleman
RSSI	Received Signal Strength Indicator
RSTP	Rapid Spanning Tree Protocol
RTCP	RTP Control Protocol
RTLS	Real-Time Location Systems
RTP	Real-Time Transport Protocol
RTS	Request to Send
RTSP	Real Time Streaming Protocol
RVI	Routed VLAN Interface
RW RoW	Rest of World
SA	Security Association
SAML	Security Assertion Markup Language
SAN	Subject Alternative Name
SCB	Station Control Block
SCEP	Simple Certificate Enrollment Protocol
SCP	Secure Copy Protocol
SCSI	Small Computer System Interface
SDN	Software Defined Networking
SDR	Software-Defined Radio

Table 6: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
SDU	Service Data Unit
SD-WAN	Software-Defined Wide Area Network
SFTP	Secure File Transfer Protocol
SHA	Secure Hash Algorithm
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SIRT	Security Incident Response Team
SKU	Stock Keeping Unit
SLAAC	Stateless Address Autoconfiguration
SMB	Small and Medium Business
SMB	Server Message Block
SMS	Short Message Service
SMTP	Simple Mail Transport Protocol
SNIR	Signal-to-Noise-Plus-Interference Ratio
SNMP	Simple Network Management Protocol
SNR	Signal-to-Noise Ratio
SNTP	Simple Network Time Protocol
SOAP	Simple Object Access Protocol
SoC	System on a Chip

Table 6: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
SoH	Statement of Health
SSH	Secure Shell
SSID	Service Set Identifier
SSL	Secure Sockets Layer
SSO	Single Sign-On
STBC	Space-Time Block Coding
STM	Station Management
STP	Spanning Tree Protocol
STRAP	Secure Thin RAP
SU-MIMO	Single-User Multiple-Input Multiple-Output
SVP	SpectraLink Voice Priority
TAC	Technical Assistance Center
TACACS	Terminal Access Controller Access Control System
TCP/IP	Transmission Control Protocol/ Internet Protocol
TFTP	Trivial File Transfer Protocol
TIM	Traffic Indication Map
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TLV	Type-length-value
ToS	Type of Service

Table 6: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
TPC	Transmit Power Control
TPM	Trusted Platform Module
TSF	Timing Synchronization Function
TSPEC	Traffic Specification
TTL	Time to Live
TTLS	Tunneled Transport Layer Security
TXOP	Transmission Opportunity
U-APSD	Unscheduled Automatic Power Save Delivery
UCC	Unified Communications and Collaboration
UDID	Unique Device Identifier
UDP	User Datagram Protocol
UI	User Interface
UMTS	Universal Mobile Telecommunication System
UPnP	Universal Plug and Play
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
USB	Universal Serial Bus
UTC	Coordinated Universal Time
VA	Virtual Appliance

Table 6: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
VBN	Virtual Branch Networking
VBR	Virtual Beacon Report
VHT	Very High Throughput
VIA	Virtual Intranet Access
VIP	Virtual IP Address
VLAN	Virtual Local Area Network
VM	Virtual Machine
VoIP	Voice over IP
VoWLAN	Voice over Wireless Local Area Network
VPN	Virtual Private Network
VRD	Validated Reference Design
VRF	Visual RF
VRRP	Virtual Router Redundancy Protocol
VSA	Vendor-Specific Attributes
VTP	VLAN Trunking Protocol
WAN	Wide Area Network
WebUI	Web browser User Interface
WEP	Wired Equivalent Privacy
WFA	Wi-Fi Alliance
WIDS	Wireless Intrusion Detection System

Table 6: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
WINS	Windows Internet Naming Service
WIPS	Wireless Intrusion Prevention System
WISPr	Wireless Internet Service Provider Roaming
WLAN	Wireless Local Area Network
WME	Wireless Multimedia Extensions
WMI	Windows Management Instrumentation
WMM	Wi-Fi Multimedia
WMS	WLAN Management System
WPA	Wi-Fi Protected Access
WSDL	Web Service Description Language
WWW	World Wide Web
WZC	Wireless Zero Configuration
XAuth	Extended Authentication
XML	Extensible Markup Language
XML-RPC	XML Remote Procedure Call
ZTP	Zero Touch Provisioning