ArubaOS 6.4.3.3

Release Notes

aruba®
NETWORKS
an HP company

Contents

ArubaOS 6.4.3.3 is a software patch release that includes new features and enhancements along with fixes to the issues identified in previous releases.

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

Chapter Overview

- New Features on page 9 provides a description of features and enhancements introduced in this release of ArubaOS.
- Regulatory Updates on page 15 lists the regulatory updates in this release of ArubaOS.
- Resolved Issues on page 17 lists and describes the issues resolved in this release of ArubaOS.
- Known Issues and Limitations on page 23 lists and describes the known and outstanding issues identified in this release of ArubaOS.
- Upgrade Procedure on page 25 describes the procedures for upgrading a controller to this release of ArubaOS.

For new features, resolved issues, and known issues and limitation prior to this release, 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.

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, or AP-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 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 the ArubaOS 6.4.3.3 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 features or enhancements introduced in this release of ArubaOS. For more information about features introduced in ArubaOS 6.4.x, refer to the *ArubaOS 6.4.x User Guide*.

5 GHz Spur Immunity

Starting from ArubaOS 6.4.3.3, the **Spur Immunity** setting is introduced. Configure this setting if high channel utilization is observed in the 5 GHz radio of an AP-130 Series access point in a noise-free environment resulting in client association and throughput issues. This setting appears in the controller WebUI only if the AP model is AP-130 Series. You can configure this setting using the controller WebUI or CLI.

In the WebUI

Log in to the controller WebUI and follow the instructions below.

1. Navigate to the **Configuration > WIRELESS > AP Configuration** page.
2. In the **AP Group** tab, click the desired profile.
3. In the **Profiles** list, navigate to the **RF Management > 802.11a radio** profile menu.
4. In the **Advanced** tab of the **Profile Details** section, configure the **Spur Immunity** setting.

Setting the spur immunity to a higher value may decrease the AP RF coverage.

Configure this parameter under the supervision of Aruba Technical Support.

In the CLI

You can configure the 5 GHz spur immunity in the controller CLI as well. A new **spur-immunity** parameter is introduced in the **rf dot11a-radio-profile** command.

rf dot11a-radio-profile

The following new parameter is introduced in the **rf dot11a-radio-profile** command:

Parameter	Description	Range	Default
`spur-immunity`	Spur Immunity for 5 GHz radio. This parameter fine-tunes the Cyclic Power Threshold (CPT) of a 5 GHz radio. The value specified here is the offset from the base value of 2 dB (for example, setting the CPT value to 1 corresponds to 2 + 1 = 3 dB. Similarly, setting the CPT value to 10 corresponds to 2+10 = 12 dB). Use this parameter when high channel utilization is observed in the 5 GHz radio of AP-130 Series access points in a noise-free environment causing client association or throughput issues. Adjust the CPT value to eliminate the spur impacts. Range definition is as follows: • 0: default CPT • 1-19: CPT growth from default (3 dB to 21 dB) • 20: Setting this parameter to 20 sets the cell-size-reduction value to 1. Cell-size-reduction is the receive coverage area of the AP. **NOTE:** Configure this parameter under the supervision of Aruba Technical Support. **NOTE:** Setting the spur immunity to a higher value may decrease the AP RF coverage. **NOTE:** This parameter is applicable for AP-130 Series access points only. The controller ignores this parameter if configured for non-AP-130 Series access points.	0-20 CPT	0 CPT

You can verify the configured value by executing the **show rf dot11a-radio-profile** command.

show rf dot11a-radio-profile

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

Parameter	Description
`Spur Immunity`	Displays the spur immunity value for 802.11a radio.

Example

The following example displays the spur immunity value for an 802.11a radio.

```
(host) #show rf dot11a-radio-profile default

802.11a radio profile "default"
-------------------------------
Parameter                                   Value
---------                                   -----
Radio enable                                Enabled
Mode                                        ap-mode
High throughput enable (radio)              Enabled
Very high throughput enable (radio)         Enabled
Channel                                     36
Transmit EIRP                               15 dBm
Non-Wi-Fi Interference Immunity             2
Spur Immunity                               0
...
```

. . .
. . .

BLE Operation Mode

Starting from ArubaOS 6.4.3.3, the **BLE Operation Mode** setting is introduced. This setting determines how the built-in Bluetooth Low Energy (BLE) chip in the AP functions. You can configure this setting using the controller WebUI or CLI.

In the WebUI

Log in to the controller WebUI and follow the instructions below.

1. Navigate to the **Configuration > WIRELESS > AP Configuration** page.
2. In the **AP Group** tab, click the desired profile.
3. In the **Profiles** list, navigate to the **AP > AP system** profile menu.
4. In the **Advanced** tab of the **Profile Details** section, configure the **BLE Operation Mode** setting described in Table 3.

Table 3: *BLE Operation Modes*

Mode	Description
Beaconing	The AP's built-in BLE chip functions as an iBeacon combined with beacon management functionality.
Disabled	The AP's built-in BLE chip is turned off. This is the default setting.
DynamicConsole	The AP's built-in chip functions as a regular iBeacon combined with beacon management functionality. However, when the link to the controller is lost, the built-in chip temporarily enables access to the AP console over BLE. This state of the BLE device may be rolled back to any of the other modes if the AP receives a different configuration setting for the **BLE Operation Mode** setting from the new LMS.
PersistentConsole	The AP's built-in chip provides access to the AP console over BLE using a mobile application. This functionality is the superset of the **Beaconing** mode.

BLE is disabled on the ArubaOS FIPS build.

In the CLI

You can configure the BLE operation mode in the controller CLI as well. A new **ble-op-mode** parameter is introduced in the **ap system-profile** command.

ap system-profile

The following new parameter is introduced in the **ap system-profile** command:

Parameter	Description

`ble-op-mode`
`Beaconing`
`Disabled`
`DynamicConsole`
`PersistentConsole`
	Determines how the built-in Bluetooth Low Energy (BLE) chip in the AP functions. BLE chip can be in one of the following four modes:
	• **Beaconing**: The AP's built-in BLE chip functions as an iBeacon combined with beacon management functionality.
	• **Disabled**: The AP's built-in BLE chip is turned off. This is the default setting.
	• **DynamicConsole**: The AP's built-in chip functions as a regular iBeacon combined with beacon management functionality. However, when the link to the controller is lost, the built-in chip temporarily enables access to the AP console over BLE. This state of the BLE device may be rolled back to any of the other modes if the AP receives a different configuration setting for the **ble-op-mode** parameter from the new LMS.
	• **PersistentConsole**: The AP's built-in chip provides access to the AP console over BLE using a mobile application. This functionality is the superset of the **Beaconing** mode.
	NOTE: BLE is disabled on ArubaOS FIPS build.

You can verify the configured value by executing the **show ap system-profile** command.

show ap system-profile

The following new parameter is introduced as part of the output of the **show ap system-profile** command:

Parameter	Description
`BLE Operation Mode`	Displays the BLE operation mode of the AP.

Example

The following example displays the BLE operation mode.

```
(host) #show ap system-profile default

AP system profile "default"
---------------------------
Parameter                               Value
---------                               -----
RF Band                                 g
RF Band for AM mode scanning            all
Native VLAN ID                          1
Tunnel Heartbeat Interval               1
Session ACL                             ap-uplink-acl
...
...
...
BLE Endpoint URL                        N/A
BLE Auth Token                          N/A
BLE Operation Mode                      Disabled
```

Modified Commands

The following command is modified in ArubaOS 6.4.3.3.

show crypto-local isakmp key

The following new parameter is introduced in the **show crypto-local isakmp key** command:

Parameter	Description
`peer <peer-ip> | fqdn <ike-id-fqdn>`	Displays the Internet Security Association and Key Management Protocol (ISAKMP) local pre-shared keys (PSKs) configured by IP address or Fully Qualified Domain Name (FQDN).

Example

The following example displays the ISAKMP local PSKs configured by IP address:

```
(host) #show crypto-local isakmp key peer 192.0.2.22

ISAKMP Local Pre-Shared keys configured by Address
--------------------------------------------------
IP address of the host  Subnet Mask Length  Key       Representation
----------------------  ------------------  ---       --------------
192.0.2.22              32                  ********   Text-based
```

The output of this command includes the following parameters.

Parameter	Description
`IP address of the host`	Displays the remote peer gateway IP address.
`Subnet Mask Length`	Displays the subnet mask (in bit format) of the remote peer gateway IP address.
`Key`	Displays the ISAKMP PSK. The characters are hidden.
`Representation`	Displays the ISAKMP PSK representation method. The possible values are: • Text-based • Hex-based

Chapter 3
Regulatory Updates

This chapter describes the regulatory updates in this release of ArubaOS.

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

The following default Downloadable Regulatory Table (DRT) version is part of ArubaOS 6.4.3.3:

- DRT-1.0_50775

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

This chapter describes the issues resolved in this release of ArubaOS. This release is a software patch release that includes fixes for CVE-2015-0288, CVE-2015-0289, and CVE-2015-0209. Additionally, the following issues are resolved in this release.

AirGroup

Table 4: *AirGroup Fixed Issues*

Bug ID	Description
118239	**Symptom:** A multicast DNS (mDNS) memory leak was observed in ArubaOS 6.4.2.6. This issue is resolved by removing an invalid 'missing record timer'. **Scenario:** This issue was observed in controllers running ArubaOS 6.4.2.6 but was not limited to any specific controller model. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.2.6.

AP-Platform

Table 5: *AP-Platform Fixed Issues*

Bug ID	Description
116882	**Symptom:** All access points in the network failed to respond and displayed **2ID** flags in the **Monitoring > CONTROLLER > Access Points** page of the controller WebUI. This issue is resolved by rejecting clients with a spurious MAC address. **Scenario:** This issue was observed in 7240 controllers running ArubaOS 6.4.2.0 in a master-standby topology. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.2.0.

AP-Wireless

Table 6: *AP-Wireless Fixed Issues*

Bug ID	Description
109200 111257	**Symptom:** An AP-225 access point crashed occasionally after upgrading to ArubaOS 6.3.1.12. This issue is resolved by implementing internal code changes. **Scenario:** This issue occurred when **AirTime Fairness (ATF)** was enabled on the controller and the clients connected to send traffic. This issue was observed in 7240 controllers running ArubaOS 6.3.1.12. **Platform:** AP-220 Series access points. **Reported Version:** ArubaOS 6.3.1.12.
112640	**Symptom:** A user experienced loss of multicast and unicast data. This issue is resolved by clearing the Network Allocation Vector (NAV) radio register when beacon fails. **Scenario:** This issue was observed rarely in specific RF environments with very short intervals of WiFi/non-WiFi spurs in the air or because of a hardware problem. This issue was observed in AP-125 access points connected to controllers running ArubaOS 6.4.2.3. **Platform:** AP-125 access points. **Reported Version:** ArubaOS 6.4.2.3.
114447	**Symptom:** Users experienced interference when they made calls using Ascom i75 voice phones. This issue is resolved by changing the value of the draining threshold from 2 to 5. **Scenario:** This issue was observed in 7240 controllers after upgrading from ArubaOS 6.3.1.5 to ArubaOS 6.4.2.4. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.2.4.
117599	**Symptom:** An AP-214 access point performed a false RADAR detection. This issue is resolved by addressing a specific RF signal pattern. **Scenario:** This issue was observed under certain RF conditions in AP-214 access point connected to controllers running ArubaOS 6.4.2.6. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.2.6.

Base OS Security

Table 7: *Base OS Security Fixed Issues*

Bug ID	Description
112704	**Symptom:** The **show crypto isakmp key** command failed to print entries after configuring more than 500 crypto pre-shared key entries. This issue is resolved by ensuring that the controller displays the entries after configuring more than 500 pre-shared key entries. **Scenario:** This issue was observed in controllers running ArubaOS 6.1.0.0 or later versions. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.3.0.
119088	**Symptom:** Clients running Apple iOS 9 were not able to authenticate with M3 controller in EAP-TLS mode but clients running iOS 8 were able to authenticate with the same controller. This issue is resolved by using the TLS version from the handshake protocol header. **Scenario:** This issue was observed in clients running iOS 9 connected to controllers running ArubaOS 6.4.3.0. This issue occurred because of the use of negotiated TLS version instead of the TLS version from the handshake protocol to calculate the pre-master secret key. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.3.0.

Captive Portal

Table 8: *Captive Portal Fixed Issues*

Bug ID	Description
116559	**Symptom:** The Captive Portal login page did not load properly for Apple devices that used iPass Wireless Internet Service Provider roaming (WISPr) clients or devices that used Boingo WISPr clients. This issue is resolved by adding validations to bypass the meta-refresh mechanism for clients that use the iPass or Boingo user-agent. **Scenario:** This issue was observed in ArubaOS 6.4.x and 6.3.x with Captive Portal page enhancements. The Captive Portal page enhancements that were introduced to serve an interim landing page with meta-refresh tag to filter non-browser-based clients did not work for some clients. This issue was not limited to any specific controller model. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.2.6.

Controller-Datapath

Table 9: *Controller-Datapath Fixed Issues*

Bug ID	Description
117543	**Symptom:** AppRF failed to block Adult/pornograph application category sites randomly. This issue is resolved by improving the WebCC and AppRF rule resolution method to converge on the WebCC action faster. **Scenario:** This issue was observed when WebCC rules followed by AppRF rules in a user role ACL needed more packets to classify the application correctly. As a result, the WebCC rule action was not taken or was delayed. This issue was observed in 7000 Series and 7200 Series controllers running ArubaOS 6.4.2.6 **Platform:** 7000 Series and 7200 Series controllers. **Reported Version:** ArubaOS 6.4.2.6.
118885	**Symptom:** Access points were unable to receive Aruba Discovery Protocol (ADP) messages. This issue is resolved by adding a validation so that the deletion of route-cache for CPsec AP is not skipped. **Scenario:** After rebootstrap, the AP did not get a new IP and the route-cache for the older IP was not retained. This issue was observed in 7210 controllers running ArubaOS 6.4.2.3. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.2.3.
119311	**Symptom:** A 7220 controller rebooted unexpectedly. The log file for the event listed the reason as **Reboot Cause: Datapath timeout (Intent:cause:register 56:86:0:2)**. This issue is resolved by not sending the packets for encryption if the station is not ready to accept data or on the verge of getting deleted. **Scenario:** This issue occurred under the following circumstances: • A race condition while encrypting data to 802.11ac clients. • The client traffic was getting encrypted. • The station was getting disassociated simultaneously. This issue was observed only with 802.11ac clients with the **AMSDU Transmit** parameter enabled on the controller running ArubaOS 6.4.2.x or ArubaOS 6.4.3.x. **Platform:** 7200 Series controllers. **Reported Version:** ArubaOS 6.4.2.5.

Controller-Platform

Table 10: *Controller-Platform Fixed Issues*

Bug ID	Description
114607 114994	**Symptom:** After the **httpd** process crashed, nanny process died and the controller was unable to restart the crashed processes. This issue is resolved by restarting the controller. **Scenario:** This issue was observed when a process tracked by nanny was killed and nanny restarted the process. If other processes were killed when the nanny was killed, then these processes were not restarted and the controller rebooted. This issue was observed in controllers running ArubaOS 6.4.2.2. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.2.2.
115092	**Symptom:** An SNMP query to retrieve the temperature from the controller returned an incorrect value. This issue is resolved by implementing internal code changes. **Scenario:** This issue occurred when an SNMP query to retrieve the controller's temperature failed. This issue was observed in 7000 Series controllers running ArubaOS 6.4.2.5 or later. **Platform:** 7000 Series controllers. **Reported Version:** ArubaOS 6.4.2.5.

IPsec

Table 11: *IPsec Fixed Issues*

Bug ID	Description
115373	**Symptom:** The ClearPass Policy Manager server failed to correlate authentication with accounting sessions for VIA connections that terminated on the controller. This issue is resolved by skipping the validation between **macuser->last_authserver** and **user->authserver**. **Scenario:** This issue was observed in VIA clients, when the Class attribute sent by the RADIUS server was not included in the accounting packets. This issue was observed in 7220 controllers running ArubaOS 6.4.2.4. **Platform:** 7220 controllers. **Reported Version:** ArubaOS 6.4.2.4.

RADIUS

Table 12: *RADIUS Fixed Issues*

Bug ID	Description
112071	**Symptom:** High values were observed in the **ExpAuthTm** column in the output of the **show aaa authentication-server radius statistics** command after upgrading a controller from ArubaOS 6.3.1.9 to ArubaOS 6.4.2.3. This issue is resolved by implementing internal code changes. **Scenario:** This issue occurred in 6000 controllers running ArubaOS 6.4.2.3. **Platform:** 6000 controllers. **Reported Version:** ArubaOS 6.4.2.3.
115370	**Symptom:** Though the user entered correct credentials the first time, subsequent authentication failed if the user entered incorrect credentials the previous time. This issue is resolved by clearing the entries in the last server when there is an authentication failure. **Scenario:** This issue occurred when subsequent authentication requests were sent to the last server in the **server-group**. This issue was observed in 3600 controllers running ArubaOS 6.4.2.5. **Platform:** 3600 controllers. **Reported Version:** ArubaOS 6.4.2.5.

Remote AP

Table 13: *Remote AP Fixed Issues*

Bug ID	Description
116102	**Symptom:** Customers were unable to access uplink devices as the route-cache on the AP uplink never expired that resulted in devices unable to send Gratuitous Address Resolution Protocol (GARP) packet. The fix ensures that the AP validations for stale ARP and then notifies the route-cache to delete the entry. **Scenario:** This issue was observed when the uplink device used the static IP address and did not send the GARP packets. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.2.6.

This chapter describes the known and outstanding issues identified in this release of ArubaOS.

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

AP-Wireless

Table 14: *AP-Wireless Known Issues*

Bug ID	Description

115865	**Symptom:** Clients experience connectivity issues on the 802.11g radios of AP-105 and AP-225 access points.
	Scenario: This issue is observed in AP-105 and AP-225 access points connected to 7240 controllers running ArubaOS 6.4.2.5 when the **striping-ip** parameter is configured as part of the **ap-lacp-striping-ip** command.
	Platform: AP-105 and AP-225 access points.
	Reported Version: ArubaOS 6.4.2.5.
	Workaround: Remove the **striping-ip** from the **ap-lacp-striping-ip** command.
	`(host) (config) #ap-lacp-striping-ip`
	`(host) (AP LACP LMS map information) #no striping-ip`

ARM

Table 15: *ARM Known Issues*

Bug ID	Description
113843	**Symptom:** After changing the **cm-band-a-min-signal** value to 10 in arm-profile, cellular hand-off assist is triggered even if the clients are associated with 2.4 GHz at strong signal strength. **Scenario:** This issue is observed in controllers running ArubaOS 6.4.0.3 but is not limited to any specific controller model. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.0.3. **Workaround:** None.

Base OS Security

Table 16: *Base OS Security Known Issues*

Bug ID	Description
117141	**Symptom:** Authentication with certificate or PSK-based VIA using IKEv1 or IKEv2 fails. **Scenario:** This issue is specific to Dell Defender acting as an external RADIUS server. Certificate or PSK-based VIA with IKEv1 or IKEv2 fails because the authentication process in the controller sends the external IP address of the VIA client as the Frame-IP-Address to the Dell Defender RADIUS server and the RADIUS server responds back with the same IP address. The authentication process considers this IP address as the inner IP of the VIA client. As the inner and external IP addresses are the same, IKE rejects the connection. This issue is observed in controllers running any version of ArubaOS. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.2.5. **Workaround:** None.

Controller-Platform

Table 17: *Controller-Platform Known Issues*

Bug ID	Description
109472 116831	**Symptom:** An increase in WebCC memory is observed when there is a connectivity issue to the Webroot® server. Due to this, after some time, the available/free memory decreases and to recover the memory, processes are killed. If a core process is terminated, the controller restarts. **Scenario:** Nonreachability of a host causes a memory leak. This issue was observed in controllers running ArubaOS 6.4.2.x or ArubaOS 6.4.3.x. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.2.3. **Workaround:** None.
115433	**Symptom:** The client is able to access the controller using the WebUI, but is unable to initiate an SSH session with the controller when the uplink connection changes from wired to cellular. **Scenario:** This issue is observed in 7010 controllers running ArubaOS 6.4.2.5. **Platform:** 7010 controllers. **Reported Version:** ArubaOS 6.4.2.5. **Workaround:** Apply bandwidth contract for Point-to-Point protocol interface of 10 Mbps.

Voice

Table 18: *Voice Known Issues*

Bug ID	Description
118114	**Symptom:** The **UCM** module crashes after accessing corrupted memory. **Scenario:** This issue is observed in some instances when the last CDR of a user, who is not associated with the wireless network, is deleted. This results in free memory, which when accessed immediately by another process causes a race condition and the restarts the **UCM** module. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.2.5. **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 with 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 28.)

GRE Tunnel-Type Requirements

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

- ArubaOS 6.4.3.3 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 27 to copy the **crash.tar** file to an external server, and then execute the **tar clean crash** command to delete the file from the controller.
- **Flash Backups:** Use the procedures described in Backing up Critical Data on page 27 to back up the flash directory to a file named **flash.tar.gz**, and then execute the **tar clean flash** command to delete the file from the controller.
- **Log files:** Execute the **tar logs** command to compress log files to a file named **logs.tar**. Use the procedures described in Backing up Critical Data on page 27 to copy the **logs.tar** file to an external server, and then execute the **tar clean logs** command to delete the file from the controller.

Backing up Critical Data

It is important to frequently back up all critical configuration data and files on the compact flash file system to an external server or mass storage device. At the very least, you should include the following files in these frequent backups:

- Configuration data
- WMS database
- Local user database
- Licensing database
- Floor plan JPEGs

- Custom captive portal pages
- x.509 certificates
- Controller Logs

Backing up and Restoring Compact Flash in the WebUI

The WebUI provides the easiest way to back up and restore the entire compact flash file system. The following steps describe how to back up and restore the compact flash file system using the WebUI on the controller:

1. Click the **Configuration** tab.
2. Click **Save Configuration** at the top of the page.
3. Navigate to the **Maintenance > File > Backup Flash** page.
4. Click **Create Backup** to back up the contents of the compact flash file system to the **flashbackup.tar.gz** file.
5. Click **Copy Backup** to copy the file to an external server.

   You can later copy the backup file from the external server to the compact flash file system using the file utility in the **Maintenance > File > Copy Files** page.
6. To restore the backup file to the Compact Flash file system, navigate to the **Maintenance > File > Restore Flash** page and click **Restore**.

Backing up and Restoring Compact Flash in the CLI

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

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

   ```
   (host) # write memory
   ```
2. Execute the **backup** command to back up the contents of the compact flash file system to the **flashbackup.tar.gz** file.

   ```
   (host) # backup flash
   Please wait while we tar relevant files from flash...
   Please wait while we compress the tar file...
   Checking for free space on flash...
   Copying file to flash...
   File flashbackup.tar.gz created successfully on flash.
   ```
3. Execute the **copy** command to transfer the backup flash file to an external server or storage device.

   ```
   (host) copy flash: flashbackup.tar.gz ftp: <ftphost> <ftpusername> <ftpuserpassword>
   <remote directory>
   (host) copy flash: flashbackup.tar.gz usb: partition <partition-number>
   ```

   You can later transfer the backup flash file from the external server or storage device to the compact flash file system by executing the **copy** command.

   ```
   (host) # copy tftp: <tftphost> <filename> flash: flashbackup.tar.gz
   (host) # copy usb: partition <partition-number> <filename> flash: flashbackup.tar.gz
   ```
4. Execute the **restore** command to untar and extract the **flashbackup.tar.gz** file to the compact flash file system.

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

Upgrading in a Multicontroller Network

In a multicontroller network (a network with two or more Aruba controllers), special care must be taken to upgrade all controllers based on the controller type (master or local). Be sure to back up all controllers being upgraded, as described in Backing up Critical Data on page 27.

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.

Upgrading to ArubaOS 6.4.3.3

The following sections provide the procedures for upgrading the controller to ArubaOS 6.4.3.3 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 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 6.4.3.3.

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

Follow step 2 to step 11 of the procedure described in Upgrading From a Recent Version of ArubaOS on page 29 to install the interim version of ArubaOS, and then repeat steps 1 through 11 of the procedure to download and install ArubaOS 6.4.3.3.

Upgrading From a Recent Version of ArubaOS

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

- 3.4.4.1 or later
- 5.0.3.1 or latest version of 5.0.x
- 6.0.1.0 or later 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 6.4.3.3 from the customer support site.
2. Upload the new software image(s) to a PC or workstation on your network.
3. Validate the SHA hash for a software image:
   a. Download the **Aruba.sha256** file from the download directory.
   b. To verify the image, load the image onto a Linux system and execute the **sha256sum <filename>** command or use a suitable tool for your operating system that can generate a **SHA256** hash of a file.
   c. Verify that the output produced by this command matches the hash value found on the support site.

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

4. Log in to the ArubaOS WebUI from the PC or workstation.
5. Navigate to the **Maintenance > Controller > Image Management** page.
   a. Select the **Local File** option.
   b. Click **Browse** to navigate to the saved image file on your PC or workstation.
6. Select the downloaded image file.
7. 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 27 for information on creating a backup. If the flash (Provisioning/Backup) image version string shows the letters *rn*, for example, 3.3.2.11-rn-3.0, note those AP names and IP addresses. 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 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 29.

Follow steps 2 through 7 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 7 of the procedure to download and install ArubaOS 6.4.3.3.

Upgrading From a Recent Version of ArubaOS

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

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

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

1. Download ArubaOS 6.4.3.3 from the customer support site.
2. Open an SSH session on your master (and local) controllers.
3. Execute the **ping** command to verify the network connection from the target controller to the SCP/FTP/TFTP server.

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

   or

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

   or

   ```
   (hostname)# 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**.

   ```
   (hostname) #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.

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

   or

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

   or

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

or

```
(hostname)# 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.

```
(hostname)# show image version

---------------------------------
Partition               : 0:0 (/dev/hda1) **Default boot**
Software Version        : ArubaOS 6.4.3.3 (Digitally Signed - Production Build)
Build number            : 50954
Label                   : 50954
Built on                : Fri Jul 24 01:55:05 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.

```
(hostname)# reload
```

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

```
(hostname)# show version
```

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

1. Log in to the CLI to verify that all your controllers are up after the reboot.
2. Execute the **show ap active** command to determine if your APs are up and ready to accept clients.
3. Execute the **show ap database** command to verify that the number of access points and clients are what you expected.
4. Test a different type of client for each access method that you use and in different locations when possible.
5. Complete a backup of all critical configuration data and files on the compact flash file system to an external server or mass storage facility. See Backing up Critical Data on page 27 for information on creating a backup.

Installing the FIPS Version of ArubaOS 6.4.3.3

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

Instructions on Installing FIPS Software

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

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

1. Install the FIPS version of the software on the controller.

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

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

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 6.4.3.3 are lost after the downgrade (this warning does not apply to upgrades from ArubaOS 3.4.x to ArubaOS 6.1).

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 6.4.3.3 to 5.0.3.2, changes made to WIPS in ArubaOS 6.x prevent the new predefined IDS profile assigned to an AP group from being recognized by the older version of ArubaOS. This unrecognized profile can prevent associated APs from coming up, and can trigger a profile error.

These new IDS profiles begin with *ids-transitional* while older IDS profiles do not include *transitional*. If you have encountered this issue, execute the **show profile-errors** and **show ap-group** commands to view the IDS profile associated with the AP group.

When reverting the controller software, whenever possible, use the previous version of software known to be used on the system. Loading a release not previously confirmed to operate in your environment could result in an improper configuration.

Before You Begin

Before you reboot the controller with the preupgrade software version, you must perform the following steps:

1. Back up your controller. For details, see Backing up Critical Data on page 27.
2. Verify that the control plane security is disabled.
3. Set the controller to boot with the previously saved pre-ArubaOS 6.4.3.3 configuration file.
4. Set the controller to boot from the system partition that contains the previously running ArubaOS image.

   When you specify a boot partition (or copy an image file to a system partition), the software checks to ensure that the image is compatible with the configuration file used on the next controller reload. An error message is displayed if system boot parameters are set for incompatible image and configuration files.
5. After downgrading the software on the controller, perform the following steps:
   - Restore pre-ArubaOS 6.4.3.3 flash backup from the file stored on the controller. Do not restore the ArubaOS 6.4.3.3 flash backup file.
   - You do not need to reimport the WMS database or RF Plan data. However, if you have added changes to RF Plan in ArubaOS 6.4.3.3, the changes do not appear in RF Plan in the downgraded ArubaOS version.
   - If you installed any certificates while running ArubaOS 6.4.3.3, you need to reinstall the certificates in the downgraded ArubaOS version.

Downgrading Using the WebUI

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

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

Downgrading Using the CLI

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

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

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

   or

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

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

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

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

   In the following example, partition 1, the backup system partition, contains the backup release ArubaOS 6.1.3.2. Partition 0, the default boot partition, contains the ArubaOS 6.4.3.3 image.

   ```
   (host) #show image version
   ---------------------------------
   Partition               : 0:0 (/dev/hda1) **Default boot**
   Software Version        : ArubaOS 6.4.3.3 (Digitally Signed - Production Build)
   Build number            : 50954
   Label                   : 50954
   Built on                : Fri Jul 24 01:55:05 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 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.