ArubaOS 8.4.0.1

aruba
a Hewlett Packard
Enterprise company

Release Notes

Open Source Code

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

Hewlett Packard Enterprise Company
6280 America Center Drive
San Jose, CA 95002
USA

Contents

Revision History

The following table provides the revision history of this document.

Table 1: *Revision History*

Revision	Change Description
Revision 04	Removed the **Migrating from ArubaOS 6.x to ArubaOS 8.x** section from **Upgrade Procedure** chapter as the Migration Tool is no longer supported.
Revision 03	Added bug **AOS-186076** in the **Known Issues** section.
Revision 02	Removed **AOS-154581** from the **Known Issues** section.
Revision 01	Initial release.

This ArubaOS release notes includes the following topics:

Throughout this document, branch controller and local controller are termed as managed device.

For the list of terms, refer Glossary.

Related Documents

The following guides are part of the complete documentation for the Aruba user-centric network:

- *ArubaOS Getting Started Guide*
- *ArubaOS User Guide*
- *ArubaOS CLI Reference Guide*
- *ArubaOS API Guide*
- Aruba *Mobility Master Licensing Guide*
- *Aruba Virtual Appliance Installation Guide*
- *Aruba Mobility Master Hardware Appliance Installation Guide*

Important Points

This section describes the important points to remember before you upgrade the managed device to this release of ArubaOS.

- If you use an image server to upgrade the managed device from the CLI, you must configure an upgrade profile on the Managed Network node.
- Ensure that the IANA timezone is configured exactly the same for each managed device. All the network nodes have to be NTP synchronized.

- Time changed manually in a managed device is not automatically adjusted for a scheduled upgrade.
- DST time change hour is not automatically adjusted for a scheduled upgrade.

Supported Browsers

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

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

Contacting Support

Table 2: *Contact Information*

Main Site	arubanetworks.com
Support Site	support.arubanetworks.com
Airheads Social Forums and Knowledge Base	community.arubanetworks.com
North American Telephone	1-800-943-4526 (Toll Free) 1-408-754-1200
International Telephone	arubanetworks.com/support-services/contact-support/
Software Licensing Site	lms.arubanetworks.com
End-of-life Information	arubanetworks.com/support-services/end-of-life/
Security Incident Response Team	Site: arubanetworks.com/support-services/security-bulletins/ Email: aruba-sirt@hpe.com

This chapter describes the features and/or enhancements introduced in this release.

AP Platform

510 Series Campus Access Points

The Aruba 510 Series Campus APs (AP-514 and AP-515) are high-performance, multi-radio wireless devices that can be deployed in either controller-based (ArubaOS) or controller less (ArubaInstant) network environments. These APs deliver high performance concurrent 2.4 GHz and 5 GHz 802.11ax Wi-Fi functionality with MIMO radios (2x2 in 2.4 GHz, 4x4 in 5 GHz), while also supporting legacy 802.11a/b/g/n/ac wireless services.

The Aruba 510 Series Campus APs are equipped with an integrated BLE and Zigbee radio that provide the following capabilities:

- Location beacon applications
- Wireless console access
- IoT gateway applications

Ethernet ports on the access points are used to connect the device to the wired networking infrastructure and provide (802.3at class 4) PoE power to the device. The access points are equipped with a USB-A port that is compatible with selected cellular modems and other peripherals. When active, this port can supply up to 5W/1A to a connected device.

The 510 Series Campus Access Points do not support UL MU-MIMO and DL MU-MIMO.

The following features are targeted for future releases and are currently not supported on the Aruba 510 Series Campus APs:

- Orthogonal Frequency Division Multiple Access (OFDMA)
- Transmit Beam Forming (TxBF)
- BSS Coloring
- Target Wait Time (TWT)
- Multi Band Operation (MBO)
- Spectrum analysis
- Mesh
- Cellular modem support
- 512 associated clients per radio (currently limited to 230 clients)

For complete technical details see the *Aruba 510 Series Campus APs Datasheet*. For installation instructions, see the *Aruba 510 Series Campus APs Installation Guide*.

This chapter describes the platforms supported in this release.

Mobility Master Platforms

The following table displays the Mobility Master platforms that are supported in this release.

Table 3: *Supported Mobility Master Platforms in ArubaOS 8.4.0.1*

Mobility Master Family	Mobility Master Model
Hardware Mobility Master	MM-HW-1K, MM-HW-5K, MM-HW-10K
Virtual Mobility Master	MM-VA-50, MM-VA-500, MM-VA-1K, MM-VA-5K, MM-VA-10K

Mobility Controller Platforms

The following table displays the controller platforms that are supported in this release.

Table 4: *Supported Mobility Controller Platforms in ArubaOS 8.4.0.1*

Controller Family	Controller Model
7000 Series	7005, 7008, 7010, 7024, 7030
7200 Series	7205, 7210, 7220, 7240, 7240XM, 7280

AP Platforms

The following table displays the AP platforms that are supported in this release.

Table 5: *Supported AP Platforms in ArubaOS 8.4.0.1*

AP Family	AP Model
100 Series	AP-104, AP-105
103 Series	AP-103
110 Series	AP-114, AP-115
130 Series	AP-134, AP-135
170 Series	AP-175AC, AP-175AC-F1, AP-175DC, AP-175DC-F1, AP-175P, AP-175P-F1
200 Series	AP-204, AP-205
203H Series	AP-203H
205H Series	AP-205H
207 Series	AP-207
203R Series	AP-203R, AP-203RP
210 Series	AP-214, AP-215
220 Series	AP-224, AP-225
228 Series	AP-228
270 Series	AP-274, AP-275, AP-277
300 Series	AP-304, AP-305
303 Series	AP-303, AP-303P
303H Series	AP-303H
310 Series	AP-314, AP-315
318 Series	AP-318

Table 5: *Supported AP Platforms in ArubaOS 8.4.0.1*

AP Family	AP Model
320 Series	AP-324, AP-325
330 Series	AP-334, AP-335
340 Series	AP-344, AP-345
360 Series	AP-365, AP-367
370 Series	AP-374, AP-375, AP-377
—	AP-387
510 Series	AP-514, AP-515
RAP 155 Series	RAP-155, RAP-155P
RAP 100 Series	RAP-108, RAP-109
RAP 3 Series	RAP-3WN, RAP-3WNP

Chapter 4
Regulatory Updates

This chapter contains the Downloadable Regulatory Table (DRT) file version introduced in this release.

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

The following DRT file version is part of this release:

- DRT-1.0_69377

This chapter describes the issues resolved in this release.

We have migrated to a new defect tracking tool and for tracking purposes, we will list both, the old and the new bug ids.

Table 6: *Resolved Issues in ArubaOS 8.4.0.1*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-146670 AOS-157311 AOS-182295	179034 193759	**Symptom:** Clients experienced poor performance with AP-305 access points. Improvements to the wireless driver resolved the issue. **Scenario:** The issue was observed in AP-305 access points running ArubaOS 8.3.0.0 or later versions.	AP-Wireless	AP-305 access points	ArubaOS 8.3.0.0
AOS-155976	191945	**Symptom:** Users were unable to provision an AP using the CLI command, **provision-ap** and an error message, **Internal error** was displayed. The fix ensures that the users are able to provision an AP. **Scenario:** This issue occurred when an IPv6 interface did not exist between the Mobility Master and managed devices but one existed between the managed devices and the APs. This issue was observed in managed devices running ArubaOS 8.3.0.3 or later versions.	AP-Platform	All platforms	ArubaOS 8.3.0.3
AOS-156646 AOS-157540	192901 194140	**Symptom:** Some APs were unable to connect to the managed device. The fix ensures that the APs are able to connect to the managed device. **Scenario:** This issue occurred when the managed device was upgraded from 8.3.0.3 FIPS version to 8.4.0.0 FIPS version. This issue was observed in AP-318, AP-387, 310 Series, 320 Series, and 370 Series access points connected to managed devices running ArubaOS 8.4.0.0 FIPS version.	AP-Platform	AP-318, AP-387, 310 Series, 320 Series, and 370 Series access points	ArubaOS 8.4.0.0 FIPS

Table 6: *Resolved Issues in ArubaOS 8.4.0.1*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-156894	193223	**Symptom:** An AP took longer than usual to transfer packets to clients. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue occurred when a Surface Pro client did not aggregate traffic. This issue was observed in 510 Series access points running ArubaOS 8.4.0.0.	AP-Wireless	510 Series access points	ArubaOS 8.4.0.0
AOS-157075	193445	**Symptom:** Users were unable to view the list of AirGroup servers in the WebUI. The fix ensures that the list of AirGroup servers are available in the WebUI. **Scenario:** This issue occurred when the clients connected to an AP moved to another AP. This issue was observed in 7240 controllers running ArubaOS 8.2.0.0 or later versions.	AirGroup	7240 controllers	ArubaOS 8.2.0.0
AOS-157162	193561	**Symptom:** UAC tunnel was not formed in a cluster. The log file listed the reason for the event as **Dynamic BSS tunnel could not be setup /Denied; AP not found in STM**. The fix ensures that the UAC tunnel is formed successfully an the events are not dropped. **Scenario:** This issue was observed in 7240 controllers running ArubaOS 8.2.2.3 in a cluster setup.	Cluster Manager	7240 controllers	ArubaOS 8.2.2.3
AOS-157348 AOS-157458	193815 194006	**Symptom:** The output of the **show license server-table** command displayed incorrect count of used licenses for APs. As a result, the APs failed to boot up and went into inactive and unlicensed state. The fix ensures that the correct license count is displayed and the APs work as expected. **Scenario:** This issue occurred when the centralized licensing server incorrectly added the licenses from standby Mobility Master. This issue was observed in Mobility Masters running ArubaOS 8.2.0.0 or later versions in a master-standby topology.	Licensing	All platforms	ArubaOS 8.2.0.0
AOS-183640	—	**Symptom:** A leak in the **MDNS** process was observed when the **show airgroup ap** or **tar logs** command was executed. This issue is resolved by fixing the memory leak in the **MDNS** process. **Scenario:** This issue occurred because of a memory leak in the **MDNS** process and this leak was significantly high in a large network with over 1000 APs. This issue was observed in Mobility Master Virtual Appliance running ArubaOS 8.3.0.0 or later versions.	AirGroup	All platforms	ArubaOS 8.3.0.6

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

We have migrated to a new defect tracking tool and for tracking purposes, we will list both, the old and the new bug ids.

Known Issues

Following are the known issues observed in this release.

Table 7: *Known Issues in ArubaOS 8.4.0.1*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-154564 AOS-155770 AOS-156549	189952 191667 192768	**Symptom:** The **SNMP** process crashes in a managed device. **Scenario:** This issue occurs when the **SNMP** process receives a request to query the table, **wlsxSwitchAccessPointTable**. This issue is observed in 7240XMcontrollers running ArubaOS 8.2.1.1 or later versions. **Workaround:** None.	SNMP	7240XM controllers	ArubaOS 8.2.1.1
AOS-155877	191816	**Symptom:** A managed device crashes and reboots unexpectedly. The log file lists the reason for the event as **Reboot Cause: Kernel Panic (Intent:cause:register 12:86:0:20).** **Scenario:** This issue is observed in 7205 stand-alone controllers running ArubaOS 8.2.2.0 or later versions. **Workaround:** None.	Controller-Platform	7205 stand-alone controllers	ArubaOS 8.2.2.0
AOS-155879	191818	**Symptom:** User is unable to delete or edit guest provisioning user on WebUI and CLI. **Scenario:** This issue occurs due to a trailing space that is added when adding a user. This issue is observed in Mobility Master Virtual Appliance running ArubaOS 8.2.0.2. **Workaround:** None	Base OS Security	All platforms	ArubaOS 8.2.0.2

Table 7: *Known Issues in ArubaOS 8.4.0.1*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-155927	191876	**Symptom:** Clients are getting de-authenticated when the User Anchor Controller (UAC) is down. **Scenario:** This issue is observed in managed devices running ArubaOS 8.2.1.1 or later versions. **Workaround:** None.	Station Management	All platforms	ArubaOS 8.2.1.1
AOS-156027	192034	**Symptom:** Access point stops broadcasting on 2.4 GHz radios. **Scenario:** This issue is observed in AP-105 access points connected to 7220controllers running ArubaOS 8.2.0.0. **Workaround:** None.	AP-Wireless	AP-105 access points	ArubaOS 8.2.0.0
AOS-156162 AOS-158131	192223 195005	**Symptom:** Managed devices are rebooting intermittently. The log file lists the reason for the event as **dds process died**. **Scenario:** This issue is observed in managed devices running ArubaOS 8.3.0.3 or later versions. **Workaround:** None.	HA-Lite	All platforms	ArubaOS 8.3.0.3
AOS-156247	192328	**Symptom:** Some managed devices are getting disconnected when the Mobility Master is rebooted. **Scenario:** This issue occurs due to corruption of the device whitelist database when configuration changes are made to the managed devices. This issue is observed in managed devices running ArubaOS 8.2.0.0 or later versions in a Mobility Master-Managed Device topology. **Workaround:** None.	Configuration	All platforms	ArubaOS 8.2.0.0
AOS-137345 AOS-156729	166773 193017	**Symptom:** The **profmgr** process in a Mobility Master crashes unexpectedly. **Scenario:** This issue occurs when the device configuration settings are replaced with new configuration settings. This issue is observed in Mobility Masters running ArubaOS 8.0.1.0 or later versions. **Workaround:** None.	Configuration	All platforms	ArubaOS 8.0.1.0
AOS-138468	168180	**Symptom:** The **profmgr** process in a managed device crashes when a single instance default profile is modified in the disaster recovery mode. **Scenario:** This issue is observed in managed devices running ArubaOS 8.0.1.0 or later versions. **Workaround:** None.	Configuration	All platforms	ArubaOS 8.0.1.0

Table 7: *Known Issues in ArubaOS 8.4.0.1*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-145747	177800	**Symptom:** Aruba Central agent debugging logs contain the hash value for the certificate sign challenge. **Scenario:** This issue is observed in managed devices running ArubaOS 8.0.1.0 or later versions. **Workaround:** None.	Logging	All platforms	ArubaOS 8.0.1.0
AOS-145876 AOS-157877	177969 194648	**Symptom:** On a 2.4 GHz radio, channel utilization is very low for few APs. **Scenario:** This issue is observed in AP-203R, AP-207, AP-315, and 340 Series access points running ArubaOS 8.3.0.0 or later versions. **Workaround:** None.	AP-Wireless	AP-203R, AP-207, AP-315, and 340 Series access points	ArubaOS 8.3.0.0
AOS-146624 AOS-155236	178976 190869	**Symptom:** Active APs are not displayed in the **Dashboard > Access Points** page in the WebUI. **Scenario:** This issue is observed in managed devices running ArubaOS 8.3.0.3 or later versions. **Workaround:** None.	Configuration	All platforms	ArubaOS 8.3.0.3
AOS-146720	179107	**Symptom:** A stand-alone controller displays the **Module licensemgr is busy. Please try later** error message while adding licenses. **Scenario:** This issue is observed in stand-alone controllers running ArubaOS 8.1.0.4 in a master - local topology. **Workaround:** None.	Licensing	All platforms	ArubaOS 8.1.0.4
AOS-147511	180406	**Symptom:** Clients are receiving IPv6 router advertisements randomly from different VLANs. **Scenario:** This issue is observed in managed devices running ArubaOS 8.2.1.0 or later versions. **Workaround:** None.	IPv6	All platforms	ArubaOS 8.2.1.0
AOS-148675	182073	**Symptom:** An AP crashes and reboots unexpectedly. The log file lists the reason for the event as **Kernel panic - not syncing: Rebooting the AP because of FW ASSERT: rcRateFind+229; ratectrl_11ac.c:2394**. **Scenario:** This issue is observed in AP-315 access points running ArubaOS 8.2.1.0. **Workaround:** None.	AP-Wireless	AP-315 access points	ArubaOS 8.2.1.0

Table 7: *Known Issues in ArubaOS 8.4.0.1*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-150122 AOS-151764	183973 186151	**Symptom:** Wireless clients failed to reconnect to the SSID after being dropped from the network. The managed device lists the following error messages: ■ **user repkey change failed** ■ **macuser repkey change failed** **Scenario:** This issue occurs when the GSM slot in a user channel is not deleted, which reduces the available GSM slots to zero. This issue is observed in managed devices running ArubaOS 8.2.1.1. **Workaround:** Reboot the managed device.	Base OS Security	All platforms	ArubaOS 8.2.1.1
AOS-150797	184849	**Symptom:** Clients are unable to make or receive calls. A **Network busy** error message is displayed. **Scenario:** This issue occurs when WMM is disabled on the managed device. This issue is observed in AP-315 access points running ArubaOS 8.2.1.1. **Workaround:** None.	WMM	AP-315 access points	ArubaOS 8.2.1.1
AOS-151012	185165	**Symptom:** A managed device crashes unexpectedly. The log file lists the reason for this event as **Reboot Cause: Reboot by Upgrade Manager Intent:cause:register 60:86:50:60).** **Scenario:** This issue is observed in managed devices running ArubaOS 8.2.1.1 or later versions. **Workaround:** None.	Controller-Platform	All platforms	ArubaOS 8.2.1.1
AOS-151355	185602	**Symptom:** Managed devices are unable to pass traffic to the nexthop VPN concentrator (VPNC) using policy-based routing. **Scenario:** This issue is observed in managed devices running ArubaOS 8.0.1.0 or later versions. **Workaround:** None.	Policy-Based Routing	All platforms	ArubaOS 8.0.1.0
AOS-151333	185579	**Symptom:** Invalid transmissions are observed when an AP boots up in the Air Monitor mode. **Scenario:** This issue is observed in 510 Series access points running ArubaOS 8.4.0.0. **Workaround:** None.	AP-Wireless	510 Series access points	ArubaOS 8.4.0.0

Table 7: *Known Issues in ArubaOS 8.4.0.1*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-151880	186310	**Symptom:** An AP sends multicast traffic to clients at a lower rate. **Scenario:** This issue occurs when **bcmc-optimization** is enabled and DMO is disabled. This issue is observed in AP-303P and AP-515 access points running ArubaOS 8.4.0.0. **Workaround:** None.	AP-Wireless	AP-303P and AP-515 access points	ArubaOS 8.4.0.0
AOS-152076 AOS-150739 AOS-151205	186605 184774 185405	**Symptom:** A managed device fails to establish IPsec tunnel on its primary uplink. **Scenario:** This issue occurs because the socket descriptor slots are not reused when the IP address is flapped in the **isakmpd** process. This issue is observed in managed devices running ArubaOS 8.0.1.0. **Workaround:** None.	Controller-Datapath	All platforms	ArubaOS 8.0.1.0
AOS-179895	186918	**Symptom:** Air time fairness feature is not functional although the value of the **shaping-policy** parameter is set to **default-access**. **Scenario:** This issue is observed in 510 Series access points running ArubaOS 8.4.0.0. **Workaround:** None.	AP-Wireless	510 Series access points	ArubaOS 8.4.0.0
AOS-152326	186957	**Symptom:** The beacon and probe response packets do not display the country capabilities information element for 5 GHz non-DFS channel. **Scenario:** This issue is observed in 510 Series access points running ArubaOS 8.4.0.0. **Workaround:** None.	AP-Wireless	510 Series access points	ArubaOS 8.4.0.0
AOS-152745	187566	**Symptom:** Some APs detect false radar signals and changes radio channels frequently **Scenario:** This issue is observed in AP-228, AP-305, 320 Series, and 340 Series access points running ArubaOS 8.3.0.1 or later versions. **Workaround:** None.	AP-Wireless	AP-228, AP-305, 320 Series, and 340 Series access points	ArubaOS 8.3.0.1
AOS-153169	188130	**Symptom:** AP crashes and reboots unexpectedly. The log files lists the reason for the event as **kernel panic: softlockup: hung tasks**. **Scenario:** This issue occurs because the firewall processes too many packets in one batch. This issue is observed in AP-303H access points running ArubaOS 8.3.0.1 or later versions. **Workaround:** None.	AP Datapath	AP-303H access points	ArubaOS 8.3.0.1

Table 7: *Known Issues in ArubaOS 8.4.0.1*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-153312	188308	**Symptom:** Video multicast frames are transmitted at the lowest configured rate on an AP. **Scenario:** This issue occurs when **mcast-rate-opt** parameter is enabled on the AP. This issue is observed in 510 Series access points running ArubaOS 8.4.0.0. **Workaround:** None.	AP-Wireless	510 Series access points	ArubaOS 8.4.0.0
AOS-153348	188356	**Symptom:** Clients reconnect to the AP frequently as the effective rates and advertised rates are not the same. **Scenario:** This issue is observed in 510 Series access points running ArubaOS 8.4.0.0. **Workaround:** None as the tx or basic rates cannot be modified.	AP-Wireless	510 Series access points	ArubaOS 8.4.0.0
AOS-153631	188717	**Symptom:** CSR does not work for 2G and 5G networks. **Scenario:** This issue is observed in 510 Series access points running ArubaOS 8.4.0.0 or later versions. **Workaround:** None.	AP-Wireless	510 Series access points	ArubaOS 8.4.0.0
AOS-153902	189090	**Symptom:** A client loses connectivity with an AP. **Scenario:** This issue occurs when the client forwards small bytes of packets but the managed device pads it with 0 bytes. This issue is observed in managed devices running ArubaOS 8.2.0.0 or later versions. **Workaround:** None.	Controller-Datapath	All platforms	ArubaOS 8.2.0.0
AOS-154056	189298	**Symptom:** System LED is blinking with a green light after an AP connects to a managed device and boots up. **Scenario:** This issue occurs when 2.4 GHz radio is disabled. This issue is observed in 510 Series access points running ArubaOS 8.4.0.0. **Workaround:** Modify any one of the 2.4 GHz radio profiles.	AP-Wireless	510 Series access points	ArubaOS 8.4.0.0
AOS-154217	189519	**Symptom:** Older Intel driver chipsets are unable to detect SSIDs with **high efficiency** enabled on the AP. **Scenario:** This issue is observed in 510 Series access points running ArubaOS 8.4.0.0 where the Intel driver is running a version prior to 20.70.x.x version. **Workaround:** Upgrade the Intel drivers to the latest version or disable the **high efficiency** parameter in the SSID profile by executing the following command : **(host) [node] # wlan he-ssid-profile default no high-efficiency-enable**	AP-Wireless	510 Series access points	ArubaOS 8.4.0.0

Table 7: *Known Issues in ArubaOS 8.4.0.1*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-154647	190062	**Symptom:** The output of the command, **show datapath frame all** does not display any value. **Scenario:** This issue is observed in 7240XM controllers running ArubaOS 8.2.1.1 or later versions. **Workaround:** None.	Controller-Datapath	7240XM controllers	ArubaOS 8.2.1.1
AOS-155080	190641	**Symptom:** The **FPAPPS** process in a Mobility Master crashes unexpectedly. **Scenario:** This issue occurs in Mobility Masters running ArubaOS 8.2.2.1 or later versions. **Workaround:** None.	VLAN	All platforms	ArubaOS 8.2.2.1
AOS-155092 AOS-157032	190654 193387	**Symptom:** APs reboot unexpectedly and experience packet loss. The log file lists the reason for the event as **Kernel Panic**. **Scenario:** This issue occurs when Jumbo frames are enabled between a managed device and the AP. This issue is observed in 510 Series access points running ArubaOS 8.4.0.0. **Workaround:** Disable Jumbo frames or set the framed-mtu <mtu> to 1500 or 1578 in the AP System profile.	AP-Wireless	510 Series access points	ArubaOS 8.4.0.0
AOS-155770 AOS-154564 AOS-156549	191667 189952 192768	**Symptom:** The **SNMP** process crashes in a managed device. **Scenario:** This issue occurs when the **SNMP** process receives a request to query the table, **wlsxSwitchAccessPointTable**. This issue is observed in 7240XM controllers running ArubaOS 8.2.1.1 or later versions. **Workaround:** None.	SNMP	7240XM controllers	ArubaOS 8.2.2.1
AOS-155847	191774	**Symptom:** Some APs running in 2G radio mode fail to transit from 1ss to 2ss power mode. **Scenario:** This issue occurs if there is a delay in the LLDP negotiation between an AP and a managed device. This issue is observed in 510 Series access points running ArubaOS 8.4.0.0. **Workaround:** None.	AP-Wireless	510 Series access points	ArubaOS 8.4.0.0
AOS-155927	191876	**Symptom:** Clients are getting de-authenticated when the User Anchor Controller (UAC) is down. **Scenario:** This issue is observed in managed devices running ArubaOS 8.2.1.1 or later versions. **Workaround:** None.	Station Management	All platforms	ArubaOS 8.2.1.1

Table 7: *Known Issues in ArubaOS 8.4.0.1*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-156162	192223	**Symptom:** Managed devices are rebooting intermittently. The log file lists the reason for the event as **dds process died**. **Scenario:** This issue is observed in managed devices running ArubaOS 8.3.0.3 or later versions. **Workaround:** None.	HA-Lite	All platforms	ArubaOS 8.3.0.3
AOS-156282	192378	**Symptom:** A client faces connectivity problem. **Scenario:** This issue occurs when the **enforce DHCP** feature is enabled. This issue is observed in managed devices running ArubaOS 8.3.0.4. **Workaround:** None.	Controller-Datapath	All platforms	ArubaOS 8.3.0.4
AOS-156283	192379	**Symptom:** APs are unable to connect to the stand-alone controller. **Scenario:** This issue occurs because the synchronized licenses are lost when the standby controller reboots. This issue is observed in stand-alone controllers running ArubaOS 8.3.0.4 in a stand-alone redundancy setup. **Workaround:** None.	Licensing	All platforms	ArubaOS 8.3.0.4
AOS-156552 AOS-154526	192771 189897	**Symptom:** The value returned from noise floor calculation is inaccurate when there is interference. **Scenario:** This issue is observed in 510 Series access points running ArubaOS 8.4.0.0. **Workaround:** None.	AP-Wireless	510 Series access points	ArubaOS 8.4.0.0
AOS-156874 AOS-156918 AOS-157515	193195 193249 194093	**Symptom:** Managed devices crash and reboot unexpectedly. The log file lists the reason for the event as **Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2)**. **Scenario:** This issue is observed in 7240XM controllers running ArubaOS 8.2.2.0 or later versions. **Workaround:** None.	Controller-Datapath	7240XM controllers	ArubaOS 8.2.2.0
AOS-157056	193423	**Symptom:** All the APs and Remote APs connected to the managed devices bootstrap after an **authentication** process crashes on the managed device. **Scenario:** This issue is observed in managed devices running ArubaOS 8.2.1.0 or later versions. **Workaround:** None.	Base OS Security	All platforms	ArubaOS 8.2.1.0

Table 7: *Known Issues in ArubaOS 8.4.0.1*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-157293	193731	**Symptom:** Clients are receiving IP addresses from a different VLANs each time they reconnect even though the **preserve-vlan** parameter is enabled using the command, **virtual-ap profile**. **Scenario:** This issue is observed in managed devices running ArubaOS 8.2.2.2 or later versions. **Workaround:** None.	Station Management	All platforms	ArubaOS 8.2.2.2
AOS-157600	194231	**Symptom:** AP crashes unexpectedly. The log file lists the reason for the event as **Reboot reason: BadAddr:100000000000338 PC:wlc_tso_hdr_length+0x0/0x78 [wl] Warm-reset**. **Scenario:** This issue is observed in 340 Series access points running ArubaOS 8.3.0.3. **Workaround:** None.	AP-Wireless	340 Series access points	ArubaOS 8.3.0.3
AOS-157878	194649	**Symptom:** The **Configuration > Profile > wlan ssid** page in the WebUI does not display all the available roles although the controller has a valid PEFNG license. **Scenario:** This issue occurs when a stand-alone controller is configured as a license client. This issue is observed in stand-alone controllers running ArubaOS 8.4.0.0. **Workaround:** None.	WebUI	All platforms	ArubaOS 8.4.0.0
AOS-157930	194725	**Symptom:** The DHCP option-82 configuration is lost once the managed device is restarted. **Scenario:** This issue is observed in managed devices running ArubaOS 8.4.0.0. **Workaround:** None.	DHCP	All platforms	ArubaOS 8.4.0.0
AOS-158238	195151	**Symptom:** 802.11 beacons can become corrupted due to the modification of wlan SSID profile transmit and basic rates, leading to client association issues and incorrect beacon transmit rates. **Scenario:** This issue is observed in 510 Series access points running ArubaOS 8.4.0.0. **Workaround:** None.	AP-Wireless	510 Series access points	ArubaOS 8.4.0.0

Table 7: *Known Issues in ArubaOS 8.4.0.1*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-158452	195458	**Symptom:** 802.11 beacons can become corrupted due to configuration of hidden SSIDs. **Scenario:** This issue is observed in 510 Series access points running ArubaOS 8.4.0.0. **Workaround:** If there are multiple SSIDs broadcast by one AP, they must all be hidden or all not hidden in order to avoid beacon corruption.	AP-Wireless	510 Series access points	ArubaOS 8.4.0.0
AOS-181971	—	**Symptom:** The video pauses for a few seconds on random clients. **Scenario:** This issue occurs when the clients are playing a DDMO converted 500Kbps video stream broadcasted by Windows Media Server and the radio resets are triggered by PSM watchdog every few seconds. This issue is observed in 510 Series access points running ArubaOS 8.4.0.1. **Workaround:** None.	AP-Wireless	510 Series access points	ArubaOS 8.4.0.1
AOS-186076 AOS-187884 AOS-189850 AOS-191866 AOS-192310 AOS-193177 AOS-193387	—	**Symptom:** The STM process crashes unexpectedly in a managed device in a cluster setup. **Scenario:** This issue occurs because some memory allocated for the client is not released after some clients disconnect from their UAC (User Anchor Controller) in a Cluster. This issue is observed in managed devicesrunning ArubaOS 8.4.0.0 or later versions. **Workaround:** None.	Station Management	All platforms	ArubaOS 8.4.0.0

Chapter 7
Upgrade Procedure

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

Read all the information in this chapter before upgrading your Mobility Master, managed device, master controller, and/or stand-alone controller.

Topics in this chapter include:

Important Points to Remember

To upgrade your managed device or Mobility Master:

- 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 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 the network by answering the following questions:
  - How many APs are assigned to each managed device? Verify this information by navigating to the **Dashboard** > **Access Points** page in the WebUI, or by executing the **show ap active** or **show ap database** commands.
  - How are those APs discovering the managed device (DNS, DHCP Option, Broadcast)?
  - What version of ArubaOS runs on your managed device?
  - Are all managed devices running the same version of ArubaOS?
  - What services are used on your managed device (employee wireless, guest access, Remote AP, wireless voice)?

- Resolve any existing issues (consistent or intermittent) before you upgrade.
- If possible, use FTP to load ArubaOS images to the managed device. 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 you encounter any issue 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, if required.
- Before you upgrade to this version of ArubaOS, assess your software license requirements and load any new or expanded licenses that you might require. For a detailed description of these new license modules, refer *Aruba Mobility Master Licensing Guide*.

Memory Requirements

All Aruba managed devices store critical configuration data on an onboard compact flash memory module. Ensure that there is always free flash space on the managed device. Loading multiple large files such as JPEG images for RF Plan can consume flash space quickly. Following are the best practices for memory management:

- Do not proceed with an upgrade unless 100 MB of free memory is available. Execute the **show memory** command to identify the available free memory. To recover memory, reboot the managed device. After the managed device comes up, upgrade immediately.
- Do not proceed with an upgrade unless 150 MB of flash space is available. Execute the **show storage** command to identify the available flash space. If the output of the **show storage** command indicates that there is insufficient flash memory, free some used memory. Copy any log file, crash data, or flash backups from your managed device to a desired location. Delete the following files from the managed device to free some memory:
  - **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 29 to copy the **crash.tar** file to an external server. Execute the **tar clean crash** command to delete the file from the managed device.
  - **Flash backups:** Use the procedures described in Backing up Critical Data on page 29 to back up the flash directory to a file named **flash.tar.gz**. Execute the **tar clean flash** command to delete the file from the managed device.
  - **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 29 to copy the **logs.tar** file to an external server. Execute the **tar clean logs** command to delete the file from the managed device.

In certain situations, a reboot or a shutdown could cause the managed device 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.

Deleting a File

You can delete a file using the WebUI or the CLI.

In the WebUI

From the Mobility Master, navigate to **Diagnostic** > **Technical Support** > **Delete Files** and remove any aging log files or redundant backups which may have been created by administrator.

In the CLI

```
(host) #delete filename <filename>
```

MIB Files

To access ArubaOS MIB files:

1. Log in to the Aruba Support site.
2. Navigate to **Download Software > ArubaOS**.
3. Navigate to the desired release folder.
4. Download the MIB file corresponding to the release.
5. Uncompress the MIB file to a local directory.

Syslog Files

To generate syslog file:

1. Log in to CLI of Mobility Master.
2. Switch to config mode.
3. Configure the logging command. Example: `logging <ipv4addr> facility local0`. For additional information, see ArubaOS 8.4.0.0 Command-Line Interface Reference Guide.
4. Execute the `show logging` command. For additional information, see ArubaOS 8.4.0.0 Command-Line Interface Reference Guide.

Backing up Critical Data

It is important to frequently back up all critical configuration data and files on the flash memory to an external server or mass storage device. You should include the following files in these frequent backups:

- Configuration data
- WMS database
- Local user database
- Licensing database
- Custom captive portal pages

- x.509 certificates
- Log files
- Flash backup

Backing up and Restoring Flash Memory

You can backup and restore the flash memory using the WebUI or CLI.

In the WebUI

The following steps describe how to back up and restore the flash memory:

1. In the Mobility Master node hierarchy, navigate to the **Maintenance** > **Configuration Management** > **Backup** page.
2. Click **Create Backup** to backup the contents of the flash memory to the **flashbackup.tar.gz** file.
3. Click **Copy Backup** to copy the file to an external server.

   You can copy the backup file from the external server to the flash memory using the file utility in the **Diagnostics** > **Technical Support** > **Copy Files** page.
4. To restore the backup file to the Compact Flash file system, navigate to the **Maintenance** > **Configuration Management** > **Restore** page and click **Restore**.

In the CLI

The following steps describe how to back up and restore the flash memory:

1. Execute the following command in the **enable** mode.

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

   ```
   (host) # backup flash
   Please wait while we take the flash backup.......
   File flashbackup.tar.gz created successfully on flash.
   Please copy it out of the controller and delete it when done.
   ```
3. Execute either of the following command to transfer the flash backup 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 transfer the flash backup file from the external server or storage device to the flash memory by executing the following command.

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

   ```
   (host) # restore flash
   Please wait while we restore the flash backup........
   ```

```
Flash restored successfully.
Please reload (reboot) the controller for the new files to take effect.
```

Upgrading ArubaOS

Upgrade ArubaOS using WebUI or CLI. Follow the below recommendations while upgrading:

- ArubaOS 8.4.0.0 supports only a maximum of 3 network adapters for Mobility Master and 4 network adapters for Mobility Master Virtual Appliance. If you have 4 network adapters on your ArubaOS 8.0.0.0 Mobility Master Virtual Appliance, you must remove one before upgrading to ArubaOS 8.4.0.0 to avoid upgrade failure. To remove a network adapter from ArubaOS 8.0.0.0 Mobility Master Virtual Appliance:

Before you remove the additional network adapter from the Mobility Master Virtual Appliance, ensure that you copy the ArubaOS 8.0.0.0 image on the system partition of Mobility Master Virtual Appliance.

  1. Log in to the vSphere client.
  2. Select the Mobility Master VM instance and click **Shut down the virtual machine**.
  3. Click **Edit Virtual machine settings**.
  4. From the **Hardware** tab, select and remove a network adapter that is not active.
- Before upgrading to ArubaOS 8.4.0.0 from ArubaOS 8.0.0.0, ensure that you configure the MAC address of the management interface as the peer MAC address, if the peer is a Mobility Master Virtual Appliance or Mobility Master. Before reloading the new image on Mobility Master, alter the peer MAC address using the following procedure in the WebUI:
  1. From the **Managed Network** node hierarchy, select the managed device.
  2. Navigate to **Configuration > Controllers** and enter the management interface MAC address in the **Peer MAC address of master** field.
  3. Click **Submit**, and then click **Continue** in the reload popup.
  4. Click **Pending Changes**.
  5. In the **Pending Changes** window, select the check box and click **Deploy changes**.

  Alternatively, you can execute the following CLI command on the Mobility Master at the device level:

  ```
  (host) [<device-mac-address>] (config) #masterip <ipaddr> ipsec <key> peer-mac-1 <mgmt-interface-mac> peer-mac-2 <mgmt-interface-mac> interface vlan <id>
  ```
- Before upgrading to ArubaOS 8.4.0.0, you must share the licenses within the global licensing pool by executing the **license-pool-profile-root** command:

  ```
  (host) [mm](config) #license-pool-profile-root
  (host) [mm](License root(/) pool profile) #acr-license-enable
  ```

Ensure that there is enough free memory and flash space on your Mobility Master or managed device. For details, see Memory Requirements on page 28.

When you navigate to the **Configuration** tab in the WebUI, the managed device might display the **Error getting information: command is not supported on this platform** message. This message occurs when you upgrade using the WebUI and navigate to the **Configuration** tab after the managed device reboots. This message disappears after clearing the Web browser cache.

In the WebUI

The following steps describe how to upgrade ArubaOS a TFTP server, FTP server, or local file:

1. Download the ArubaOS image from the customer support site.
2. Upload the new software image to a PC or workstation on your network.
3. Validate the SHA hash for the ArubaOS image:
   a. Download the **Aruba.sha256** file from the download directory.
   b. Load the ArubaOS image to a Linux system and execute the **sha256sum <filename>** command. Alternatively, 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 customer support site.

The ArubaOS image file is digitally signed, and is verified using RSA2048 certificates preloaded at the factory. The Mobility Master or managed device will not load a corrupted ArubaOS image.

4. Log in to the ArubaOS WebUI from the Mobility Master.
5. Navigate to the **Maintenance** > **Software Management** > **Upgrade** page.
   a. Select the **Local File** from the **Upgrade using** drop-down list.
   b. Click **Browse** from the **Image file name** to navigate to the saved image file on your PC or workstation.
6. Select the downloaded image file.
7. Choose the partition from the **Partition to Upgrade** option.
8. Enable the **Reboot Controller After Upgrade** toggle switch to automatically reboot after upgrading. If you do not want to reboot immediately, disable this option.

The upgrade does not take effect until reboot. If you chose to reboot after upgrade, the Mobility Master or Managed device reboots automatically.

9. Select the **Save Current Configuration**.
10. Click **Upgrade**.
11. Click **OK**, when **Changes were written to flash successfully** message is displayed.

In the CLI

The following steps describe how to upgrade ArubaOS from a TFTP server, FTP server, or local file:

1. Download the ArubaOS image from the customer support site.
2. Open an SSH session to your Mobility Master.
3. Execute the **ping** command to verify the network connection between the Mobility Master and the SCP server, FTP server, or 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 image is loaded on the 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 to the non-boot 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>
   ```

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

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

7. Reboot the Mobility Master.

   ```
   (host)# reload
   ```

Verifying the ArubaOS Upgrade

Verify the upgrade using the WebUI or CLI.

In the WebUI

Log in to the WebUI and navigate to the **Dashboard** > **WLANs** page to verify the ArubaOS image version. The following steps describe how to verify that the Mobility Master is functioning as expected:

1. Log in to the WebUI to verify all the managed devices are up after the reboot.
2. Navigate to the **Dashboard > Access Points** page to determine if your APs are up and ready to accept clients.

3. Verify that the number of access points and clients are as expected.
4. Test a different type of client in different locations, for each access method used.
5. Complete a backup of all critical configuration data and files on the flash memory, to an external server or mass storage facility. See Backing up Critical Data on page 29 for information on creating a backup.

In the CLI

Execute the **show version** command to verify the ArubaOS image version. The following steps describe how to verify that the Mobility Master is functioning as expected:

1. Log in to the CLI and verify that all your managed devices 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 APs and clients are as expected.
4. Test a different type of client in different locations, for each access method used.
5. Complete a backup of all critical configuration data and files on the flash memory to an external server or mass storage facility. See Backing up Critical Data on page 29 for information on creating a backup.

Downgrading ArubaOS

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

Pre-requisites

A Mobility Master or a managed device has two partitions, 0 and 1. If the upgrade fails on one of the partitions, you can reboot the Mobility Master or the managed device from the other partition. Before you reboot the Mobility Master or with the pre-upgrade ArubaOS version, you must perform the following steps:

1. Back up your Mobility Master or managed device. For details, see Backing up Critical Data on page 29.
2. Verify that the control plane security is disabled.
3. Set the Mobility Master or managed device to boot with the previously saved configuration file.
4. Set the Mobility Master or managed device to boot from the partition that contains the pre-upgrade ArubaOS version.

   When you specify a boot partition or copy an image file to a system partition, Mobility Master or managed device checks if the ArubaOS version is compatible with the configuration file . An error message is displayed if the boot parameters are incompatible with ArubaOS version and configuration files.
5. After switching the boot partition, perform the following steps:
   - Pre-upgrade flash backup from the file stored on the Mobility Master or managed device. Do not restore the ArubaOS flash backup file.
   - Do not import the WMS database.

- If the RF plan was changed before switching the boot partition, the changed RF plan does not appear in the downgraded ArubaOS version.
- If any new certificates were added in the upgraded ArubaOS version, reinstall these certificates in the downgraded ArubaOS version.

Downgrade ArubaOS version using the WebUI or CLI.

In the WebUI

The following steps describe how to downgrade the ArubaOS version:

1. If the saved pre-upgrade configuration file is on an external FTP/TFTP server, copy the file to the Mobility Master or managed device by navigating to the **Diagnostics > Technical Support > Copy Files** page.
   a. From **Select source file** drop-down list, select FTP or TFTP server, and enter the IP address of the FTP or TFTP server and the name of the pre-upgrade configuration file.
   b. From **Select destination file** drop-down list, enter a file name (other than default.cfg).
   c. Click **Copy.**
2. Determine the partition on which your previous ArubaOS version stored by navigating to the **Maintenance > Software Management > Upgrade** page. If a pre-upgrade ArubaOS version is not stored on your system partition, load it into the backup system partition by performing the following steps:

You cannot load a new image into the active system partition

   a. Enter the FTP/TFTP server address and image file name.
   b. Select the backup system partition.
   c. Enable **Reboot controller after upgrade**.
   d. Click **Upgrade**.
3. Navigate to the **Maintenance > Software Management > Reboot** page. Select **Save configuration before reboot** option and click **Reboot**. The Mobility Master or managed device reboots after the countdown period.
4. When the boot process is complete, verify that the Mobility Master or managed device is using the correct ArubaOS version by navigating to the **Maintenance > Software Management > About** page.

In the CLI

The following steps describe how to downgrade the ArubaOS version:

1. If the saved pre-upgrade configuration file is on an external FTP/TFTP server, use the following command to copy it to the Mobility Master or managed device:

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

   or

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

2. Set the Mobility Master or managed device to boot with your pre-upgrade configuration file.

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

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

```
#show image version
```

4. Set the backup system partition as the new boot partition.

```
(host) # boot system partition 1
```

5. Reboot the Mobility Master or managed device.

```
(host) # reload
```

6. When the boot process is complete, verify that the Mobility Master or managed device is using the correct ArubaOS version.

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

Before Calling Technical Support

Provide the following information when you call Technical Support:

- The status of installation (new or existing) and recent changes to network, device, or AP configuration. If there was a configuration change, list the exact configuration steps and commands used.
- A detailed network topology including all the devices in the network with IP addresses Interface numbers.
- The make and model number of the wireless device and NIC, driver date, version, and configuration of the NIC, and the OS version including any service packs or patches.
- The logs and output of the **show tech-support** command.
- The syslog file at the time of the problem.
- The date and time when the problem occurred. If the problem is reproducible, list the exact steps taken to re-create the problem.
- Any wired or wireless sniffer traces taken during the time of the problem.
- The device site access information, if possible.