AOS-W 8.8.0.2 Release Notes

Contents

Chapter 1
Revision History

The following table lists the revision numbers and the corresponding changes that were made in this release:

Table 1: *Revision History*

Revision	Change Description
Revision 02	The bug, **AOS-125897** was added as a known issue.
Revision 01	Initial release.

Chapter 2
Release Overview

This AOS-W release notes includes the following topics:

- New Features and Enhancements
- Supported Platforms
- Regulatory Updates
- Resolved Issues
- Known Issues and Limitations
- Upgrade Procedure

Related Documents

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

- *AOS-W Getting Started Guide*
- *AOS-W User Guide*
- *AOS-W CLI Reference Guide*
- *AOS-W API Guide*
- *Alcatel-Lucent Mobility Conductor Licensing Guide*
- *Alcatel-Lucent Virtual Appliance Installation Guide*
- *Alcatel-Lucent AP Software Quick Start Guide*

Supported Browsers

The following browsers are officially supported for use with the AOS-W 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 48 or later on Windows 7, Windows 8, Windows 10, and macOS
- Apple Safari 9.0 or later on macOS
- Google Chrome 67 on Windows 7, Windows 8, Windows 10, and macOS

Terminology Change

As part of advancing Alcatel-Lucent Enterprise's commitment to racial justice, we are taking a much-needed step in overhauling ALE engineering terminology to reflect our belief system of diversity and inclusion. Some legacy products and publications may continue to include terminology that seemingly evokes bias against specific groups of people. Such content is not representative of our ALE culture and moving forward, ALE will replace racially insensitive terms and instead use the following new language:

Usage	Old Language	New Language
Campus Access Points + Controllers	Master-Slave	Conductor-Member
Instant Access Points	Master-Slave	Conductor-Member
Switch Stack	Master-Slave	Conductor-Member
Wireless LAN Controller	Mobility Master	Mobility Conductor
Firewall Configuration	Blacklist, Whitelist	Denylist, Allowlist
Types of Hackers	Black Hat, White Hat	Unethical, Ethical

Contacting Support

Table 2: *Contact Information*

Contact Center Online	
Main Site	https://www.al-enterprise.com
Support Site	https://businessportal.al-enterprise.com
Email	ebg_global_supportcenter@al-enterprise.com
Service & Support Contact Center Telephone	
North America	1-800-995-2696
Latin America	1-877-919-9526
EMEA	+800 00200100 (Toll Free) or +1(650)385-2193
Asia Pacific	+65 6240 8484
Worldwide	1-818-878-4507

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

Automatic BIOS Upgrade in 9012 switches

The automatic BIOS upgrade feature ensures that the 9012 switches have the latest version of the BIOS. When a firmware upgrade is initiated on the switch, this feature compares the running (current) BIOS version with the available (new) BIOS version. The automatic BIOS upgrade happens if the running BIOS version is less than the available BIOS version.

The firmware upgrade on the 9012 switches takes longer than usual when the automatic BIOS upgrade happens as the complete process is estimated to take up to 15 minutes. Do not shutdown or interrupt the upgrade. Power failures and interruptions during the upgrade may make the switch unusable.

CLI

show stm perf-history command

Starting from ArubaOS 8.8.0.2, the **show stm perf-history** command displays the number of association requests received by the switch for the past 24 hours.

```
(host) #show stm perf-history
Association Rate History
------------------------
Day  Hour  Min  Total  Peak rate/s  Peak time
---  ----  ---  -----  -----------  ---------
10   14    45   5725   40.0         14:47:34
10   14    50   9850   40.0         14:50:26
10   14    55   10040  40.0         14:55:05
10   15    0    9860   40.0         15:01:30
10   15    5    9900   40.0         15:05:18
10   15    10   9900   40.0         15:10:33
10   15    15   9900   40.0         15:15:16
10   15    20   10075  40.0         15:20:05
```

The output displays the association rate history for every five minute of the past 24 hours.

Chapter 4
Supported Platforms in AOS-W 8.8.0.2

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 AOS-W 8.8.0.2*

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

OmniAccess Mobility Controller Platforms

The following table displays the OmniAccess Mobility Controller platforms that are supported in this release:

Table 4: *Supported OmniAccess Mobility Controller Platforms in AOS-W 8.8.0.2*

OmniAccess Mobility Controller Family	OmniAccess Mobility Controller Model
OAW-40xx Series Hardware OmniAccess Mobility Controllers	OAW-4005, OAW-4008, OAW-4010, OAW-4024, OAW-4030
OAW-4x50 Series Hardware OmniAccess Mobility Controllers	OAW-4450, OAW-4550, OAW-4650, OAW-4750, OAW-4750XM, OAW-4850
OAW-41xx Series Hardware OmniAccess Mobility Controllers	OAW-4104, 9012
MC-VA-xxx Virtual OmniAccess Mobility Controllers	MC-VA-10, MC-VA-50, MC-VA-250, MC-VA-1K

AP Platforms

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

Table 5: *Supported AP Platforms in AOS-W 8.8.0.2*

AP Family	AP Model
OAW-AP200 Series	OAW-AP204, OAW-AP205
OAW-AP203H Series	OAW-AP203H
OAW-AP203R Series	OAW-AP203R, OAW-AP203RP

Table 5: *Supported AP Platforms in AOS-W 8.8.0.2*

AP Family	AP Model
OAW-AP205H Series	OAW-AP205H
OAW-AP207 Series	OAW-AP207
OAW-AP210 Series	OAW-AP214, OAW-AP215
OAW-AP 220 Series	OAW-AP224, OAW-AP225
OAW-AP228 Series	OAW-AP228
OAW-AP270 Series	OAW-AP274, OAW-AP275, OAW-AP277
OAW-AP300 Series	OAW-AP304, OAW-AP305
OAW-AP303 Series	OAW-AP303, OAW-AP303P
OAW-AP303H Series	OAW-AP303H, AP-303HR
OAW-AP310 Series	OAW-AP314, OAW-AP315
OAW-AP318 Series	OAW-AP210AP-318
OAW-AP320 Series	OAW-APAP-324, OAW-AP325
OAW-AP330 Series	OAW-AP334, OAW-AP335
OAW-AP340 Series	OAW-AP344, OAW-AP345
OAW-AP360 Series	OAW-AP365, OAW-AP367
OAW-AP370 Series	OAW-AP374, OAW-AP375, OAW-AP377
370EX Series	AP-375EX, AP-377EX, AP-375ATEX
OAW-AP387	OAW-AP387
500 Series	OAW-AP504, OAW-AP505
500H Series	AP-503H, AP-505H
510 Series	OAW-AP514, OAW-AP515, AP-518
530 Series	OAW-AP534, OAW-AP535
550 Series	OAW-AP555
560 Series	AP-565, AP-567
570 Series	AP-574, AP-575, AP-577

Chapter 5
Regulatory Updates in AOS-W 8.8.0.2

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 switch 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 businessportal2.alcatel-lucent.com.

The following DRT file version is part of this release:

- DRT-1.0_81660

Chapter 6
Resolved Issues in AOS-W 8.8.0.2

This chapter describes the resolved issues in this release.

Table 6: *Resolved Issues in AOS-W 8.8.0.2*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-225808 AOS-226249	—	The APs crashed unexpectedly after a cluster split. This issue occurred when there were seven or more managed devices in a dual stack deployment. This issue was observed in managed devices running AOS-W 8.7.0.0 or later versions in a cluster setup.	AOS-W 8.7.1.3
AOS-213507	—	Some managed devices crashed unexpectedly. The log files listed the reason for the event as, **Reboot Cause: Soft Watchdog reset**. Some users also experienced decreased network performance in high density deployments. The fix ensures that the managed devices work as expected. This issue was observed in OAW-4550, OAW-4650, OAW-4750, and OAW-4750XM switches running AOS-W 8.3.0.14 or later versions. **Duplicates:** AOS-210240, AOS-214964, AOS-215393, AOS-215421, AOS-215628, AOS-215765, AOS-215827, AOS-216087, AOS-216315, AOS-216420, AOS-216888, AOS-217041, AOS-218007, AOS-218021, AOS-218907, AOS-219588, AOS-219597, AOS-216315, AOS-216420, AOS-216888, AOS-220471, AOS-220981, AOS-221390, AOS-221642, AOS-222036, AOS-223402, AOS-224238, AOS-225375, AOS-226268, AOS-226517, AOS-223254, and AOS-224552	AOS-W 8.5.0.10
AOS-201428 AOS-204928 AOS-217626 AOS-216968	—	The **show log all** command did not display output in a chronological order. The fix ensures that the output is displayed correctly. This issue was observed in Mobility Masters running ArubaOS 8.3.0.0 or later versions.	ArubaOS 8.3.0.0
AOS-209093 AOS-210452	—	Some managed devices running AOS-W 8.7.0.0 or later versions generated multiple AMON receiver errors. The fix ensures that the managed devices work as expected.	AOS-W 8.7.0.0
AOS-210198	—	The **Dashboard > Security > Detected Radio** page of the WebUI displayed incorrect number of **Clients**. The fix ensures that the WebUI displays correct number of **Clients**. This issue was observed in Mobility Masters running AOS-W 8.6.0.5 or later versions.	AOS-W 8.6.0.5
AOS-212936	—	Some users experienced network outage. The fix ensures that the users do not experience network outage. This issue was observed in managed devices running AOS-W 8.6.0.6 or later versions.	AOS-W 8.6.0.6

Table 6: *Resolved Issues in AOS-W 8.8.0.2*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-213011 AOS-219946	—	Packet loss was observed for a few clients during a cluster failover. This issue was observed in managed devices running AOS-W 8.0.0.0 or later versions. The fix ensures that the managed devices work as expected.	AOS-W 8.5.0.10
AOS-213337	—	A few AP-325 access points running AOS-W 8.5.0.10 or later versions crashed unexpectedly. The log files listed the reason for the event as **Reboot caused by kernel panic: Fatal exception in interrupt**. The fix ensures that the APs work as expected.	AOS-W 8.5.0.10
AOS-213924 AOS-217233	—	Mobility Controller Virtual Appliances running AOS-W 8.7.0.0 or later versions displayed incorrect VLAN ID details for some wired users. The fix ensures that the Mobility Controller Virtual Appliances display correct VLAN IDs.	AOS-W 8.7.0.0
AOS-214510 AOS-219139	—	A few clients were disconnected from the network. The log files listed the reason for the event as **Wlan driver excessive tx fail quick kickout**. The fix ensures seamless connectivity. This issue was observed in managed devices running AOS-W 8.6.0.5 or later versions.	AOS-W 8.6.0.5
AOS-214963	—	Some APs running AOS-W 8.5.0.11 or later versions detected false radar. The fix ensures that the APs work as expected.	AOS-W 8.5.0.11
AOS-214977 AOS-220420	—	Memory leak was observed in **arci-cli-helper** process. This issue occurred while running an API script. The fix ensures that the APs work as expected. This issue was observed in APs running AOS-W 8.5.0.8 or later versions.	AOS-W 8.5.0.8
AOS-215498	—	Some OAW-AP535 access points running AOS-W 8.5.0.11 or later versions detected false radar. The fix ensures that the APs work as expected.	AOS-W 8.5.0.11
AOS-216512	—	The DHCP client / station related AMON message sent the mask, server IP address, and client IP address in the reverse order to the AirWave server. The fix ensures that the Mobility Masters work as expected. This issue was observed in Mobility Masters running AOS-W 8.6.0.6 or later versions.	AOS-W 8.6.0.6
AOS-216764	—	Users were not redirected to the captive portal page. The fix ensures that the captive portal works as expected. This issue was observed in managed devices running AOS-W 8.7.1.0 or later versions in a cluster setup.	AOS-W 8.7.1.0

Table 6: *Resolved Issues in AOS-W 8.8.0.2*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-216766	—	Some APs generated sapd coredump. The fix ensures that the APs work as expected. This issue was observed in APs running AOS-W 8.5.0.11 or later versions.	AOS-W 8.5.0.11
AOS-216874 AOS-219841	—	The virtual MAC address of a VLAN got deleted from the bridge table and hence, resulted in a network outage. The fix ensures that the managed devices work as expected. This issue was observed in managed devices running AOS-W 8.5.0.11 or later versions.	AOS-W 8.5.0.11
AOS-216972	—	Some managed devices running AOS-W 8.6.0.7 or later versions forwarded data frames that are larger than the configured IPsec tunnel MTU value. The fix ensures that the managed devices do not forward data frames that are larger than the configured IPsec tunnel MTU value.	AOS-W 8.6.0.7
AOS-217104 AOS-219159	—	ESI redirect failed and traffic was forwarded to the default gateway. The fix ensures that the managed devices work as expected. This issue was observed in managed devices running AOS-W 8.6.0.6 or later versions.	AOS-W 8.6.0.6
AOS-217106	—	The **no valid** parameter of the **ap regulatory-domain-profile** command did not work while creating a new regulatory profile. The fix ensures that the **no valid** parameter of the **ap regulatory-domain-profile** command works as expected. This issue was observed in controllers running AOS-W 8.0.0.0 or later versions.	AOS-W 8.6.0.7
AOS-217807	—	Some OAW-RAPs took a long time to come up on a managed device. This issue occurred due to a delay in whitelist-db synchronization between the Mobility Master and managed devices and when external authentication was enabled for OAW-RAPs. The fix ensures that the OAW-RAPs do not take a long time to come up on a managed device. This issue was observed in managed devices running AOS-W 8.6.0.5 or later versions in a cluster setup.	AOS-W 8.6.0.5
AOS-218012	—	The **Maintenance** tab of the WebUI displayed a list of clusters that were not configured for that particular node. The fix ensures that the WebUI displays the correct information. This issue was observed in Mobility Masters running AOS-W 8.5.0.9 or later versions.	AOS-W 8.5.0.9
AOS-218070	—	The **auth** process crashed on managed devices running AOS-W 8.6.0.0 or later versions. The fix ensures that the managed devices work as expected.	AOS-W 8.6.0.0

Table 6: *Resolved Issues in AOS-W 8.8.0.2*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-218328 AOS-220026 AOS-223535	—	VRRP flapping was observed on managed devices running AOS-W 8.6.0.4 or later versions and hence, clients faced connectivity issues. The fix ensures that the managed devices work as expected.	AOS-W 8.6.0.4
AOS-218404 AOS-212330	—	Some APs were unable to ping a few clients. The fix ensures that the APs are able to ping the clients. This issue was observed in APs running AOS-W 8.5.0.11 or later versions.	AOS-W 8.5.0.11
AOS-218488 AOS-219694	—	The management VLAN address of the Mobility Master was pointing to the OAW-RAP tunnel. The fix ensures that the management VLAN address is not available in the OAW-RAP tunnel. This issue was observed in Mobility Masters running AOS-W 8.3.0.0 or later versions.	AOS-W 8.3.0.0
AOS-218518 AOS-218880 AOS-222186 AOS-222204	—	Some managed devices running AOS-W 8.7.1.0 or later versions crashed unexpectedly. The log files listed the reason for the event as **Reboot reason Datapath timeout (SOS Assert).** The fix ensures that the managed devices work as expected.	AOS-W 8.7.1.0
AOS-218622	—	Some APs running AOS-W 8.6.0.6 or later versions crashed unexpectedly. The log files listed the reason for the event as **PC:aruba_wlc_ratesel_ getcurrate+0x24/0xd0 [wl_v6] Warm-reset**. The fix ensures that the APs work as expected.	AOS-W 8.7.1.1
AOS-218642	—	Some iPads and other clients were unable to access the internet. This issue occurred when client entries were not removed by the managed devices even when CoA disconnect was triggered for the clients. The fix ensures seamless connectivity. This issue was observed in managed devices running ArubaOS 8.5.0.11 or later versions.	ArubaOS 8.5.0.11
AOS-218646	—	Ascom i63 phones connected to OAW-AP515 access points running AOS-W 8.6.0.7 or later versions experienced degraded audio quality. The fix ensures that the clients do not experience degraded audio quality.	AOS-W 8.6.0.7
AOS-218822	—	High flash memory utilization was observed in Mobility Masters running AOS-W 8.5.0.10 or later versions. The fix ensures that the Mobility Masters work as expected.	AOS-W 8.5.0.10
AOS-219034	—	Clients that were connected to HT-enabled SSIDs connected as non-HT clients. The fix ensures that the APs work as expected. This issue was observed in APs running AOS-W 8.6.0.6 or later versions.	AOS-W 8.6.0.6

Table 6: *Resolved Issues in AOS-W 8.8.0.2*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-219098 AOS-219914	—	Some devices were unable to connect to the network. The fix ensures seamless connectivity. This issue was observed in APs running AOS-W 8.7.1.1 or later versions.	AOS-W 8.7.1.1
AOS-219178	—	A few clients connected to the anchor controller were unable to receive IP addresses. The fix ensures that the clients are able to receive IP addresses. This issue is observed in managed devices running AOS-W 8.3.0.7 or later versions.	AOS-W 8.3.0.7
AOS-219214	—	The validuser acl list was reordered in stand-alone controllers running AOS-W 8.6.0.8 or later versions. The fix ensures that the validuser acl list is not reordered.	AOS-W 8.6.0.8
AOS-219328	—	SNMP configurations failed and the error message, **Error: User (itam_net) should be created before adding to the trap host** was displayed. This issue occurred when the SNMP server v3 trap host which had the engine-id same as the engine-id of the switch was removed and added again. The fix ensures that the SNMP configurations do not fail. This issue was observed in managed devices running AOS-W 8.5.0.11 or later versions.	AOS-W 8.5.0.11
AOS-219355 AOS-223755 AOS-224270	—	Some OAW-AP515 access points running ArubaOS 8.7.1.3 or later versions crashed unexpectedly. The log file listed the reason for the event as, **Reboot reason: BadAddr:ffffffc139724881 PC:memcpy+0x7c/0x180 Warm-reset**. The fix ensures that the APs work as expected.	ArubaOS 8.7.1.3
AOS-219365	—	Some APs running AOS-W 8.7.0.0 or later versions rebooted sporadically. This issue occurred when the smart antenna feature was enabled. The fix ensures that the APs work as expected.	AOS-W 8.7.1.1
AOS-219384	—	Some APs running AOS-W 8.7.1.1 or later versions crashed unexpectedly. The log files listed the reason for the event as **PC is at wlc_nar_dotxstatus+0x450**. The fix ensures that the APs work as expected.	AOS-W 8.7.1.1
AOS-219390	—	The **datapath** process crashed on stand-alone controllers running AOS-W 8.7.1.1 or later versions. The log files listed the reason for the event as **Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2)**. This issue occurred when the op mode of the SSID profile was changed from WPA3-AES-CCM-128 to WPA3-CNSA. The fix ensures that the stand-alone controllers work as expected.	AOS-W 8.7.1.1

Table 6: *Resolved Issues in AOS-W 8.8.0.2*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-219423	—	Honeywell Handheld 60SL0 devices were unable to connect to 802.1X SSIDs. The fix ensures seamless connectivity. This issue was observed in managed devices running AOS-W 8.6.0.8 or later versions.	AOS-W 8.6.0.8
AOS-219594	—	The **Logon-Webcc** process crashed on Mobility Masters running AOS-W 8.7.1.2 or later versions. The fix ensures that the Mobility Masters work as expected.	AOS-W 8.7.1.2
AOS-219627 AOS-218851	—	A few clients were unable to connect to the 2.4 GHz SSID of some APs. This issue occurred when the MAC address of the Radio 1 was incorrect. The fix ensures seamless connectivity. This issue was observed in APs running AOS-W 8.7.1.1 or later versions.	AOS-W 8.7.1.1
AOS-219725	—	Some APs running AOS-W 8.7.1.1 or later versions crashed unexpectedly. The log files listed the reason for the event as **PC is at wlc_nar_detach+0x8c**. The fix ensures that the APs work as expected.	AOS-W 8.7.1.1
AOS-219894 AOS-220122	—	The BLE server displayed an incorrect **Last Sync Time**. The fix ensures that the BLE server displays the correct **Last Sync Time**. This issue was observed in managed devices running ArubaOS 8.7.1.1 or later versions.	ArubaOS 8.7.1.1
AOS-219978 AOS-220568	—	iPhone 12 Pro users experienced poor upstream network performance. This issue occurred when APs operated in tunnel mode. The fix ensures optimal network performance. This issue was observed in APs running AOS-W 8.6.0.9 or later versions in tunnel mode.	AOS-W 8.7.1.2
AOS-220179	—	A few clients were unable to complete the SAE handshake. This issue occurred when the password of an SSID profile was modified to a length greater than the existing password. The fix ensures that the SAE handshake is not interrupted. This issue was observed in APs running ArubaOS 8.8.0.0.	ArubaOS 8.8.0.0
AOS-220251	—	Some users experienced connectivity issue. This issue occurred when APs did not respond to the authentication frames in MultiZone networks that have non-cluster zones and dot11r enabled Virtual APs. The fix ensures seamless connectivity. This issue was observed in stand-alone switches running ArubaOS 8.5.0.4 or later versions.	ArubaOS 8.5.0.4
AOS-220398	—	A few clients in bridge mode were unable to connect to WPA2-PSK SSIDs. The fix ensures that the clients in bridge mode are able to connect to WPA2-PSK SSIDs. This issue was observed in stand-alone switches running AOS-W 8.6.0.8 or later versions.	AOS-W 8.6.0.8

Table 6: *Resolved Issues in AOS-W 8.8.0.2*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-220996	—	The **switch_daemon** process crashed on Mobility Masters running AOS-W 8.7.1.3 or later versions. The fix ensures that the Mobility Masters work as expected.	AOS-W 8.7.1.3
AOS-221018 AOS-220919	—	Some users were unable to connect to SSIDs. This issue occurred in 802.11r and MultiZone enabled configurations. The fix ensures seamless connectivity. This issue was observed in APs running AOS-W 8.5.0.11 or later versions.	AOS-W 8.5.0.11
AOS-221047 AOS-221813 AOS-223756	—	Some OAW-AP515 access points running ArubaOS 8.7.1.3 or later versions crashed unexpectedly. The log files listed the reason for the event as, **AP Reboot reason: Panic:Ktrace core monitor: cpu2 hung for 36893488 seconds, hung cpu count: 3 Warm-reset.** The fix ensures that the APs work as expected.	ArubaOS 8.7.1.3
AOS-221064	—	Some OAW-AP515 access points running ArubaOS 8.7.1.3 or later versions crashed unexpectedly. The log files listed the reason for the event as, **AP Reboot reason: InternalError: : 96000210 1 SMP PC:phy_utils_write_phyreg_nopi+0x70/0x130 [wl_v6] Warm-reset.** The fix ensures that the APs work as expected.	ArubaOS 8.7.1.3
AOS-221222	—	Some APs came up with IDe flag and the **show ap database** command displayed **e** flag even when EST was not configured. This issue occurred when external whitelist authentication was configured on the managed devices and CPsec enabled APs were brought up on the managed devices. The fix ensures that the APs work as expected. This issue was observed in managed devices running AOS-W 8.8.0.0.	ArubaOS 8.8.0.0
AOS-221225	—	Some OAW-AP387 access points running AOS-W 8.7.1.1 or later versions rebooted unexpectedly. The log files listed the reason for the event as **Reboot caused by kernel panic: Fatal exception**. The fix ensures that the APs work as expected.	AOS-W 8.7.1.1
AOS-221352	—	Some mesh links reported incorrect RSSI values. The fix ensures that the mesh links report correct RSSI values. This issue was observed in APs running AOS-W 8.7.0.0 or later versions.	AOS-W 8.7.0.0
AOS-221478 AOS-221569 AOS-221572	—	The **auth** process crashed on managed devices running AOS-W 8.5.0.9 or later versions. This issue occurred when the **show auth-tracebuf mac** command was executed. The fix ensures that the managed devices work as expected.	AOS-W 8.5.0.9

Table 6: *Resolved Issues in AOS-W 8.8.0.2*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-222540	—	Some APs dropped EAPOL packets from the bridge mode wired port. The fix ensures that the APs do not drop the EAPOL packets. This issue was observed in APs running ArubaOS 8.6.0.9 or later versions.	ArubaOS 8.6.0.9
AOS-224090 AOS-225043	—	Some managed devices running AOS-W 8.6.0.10 or later versions were stuck in the **Last Snapshot** state. This issue occurred when tunnel MTU was set to a value lesser than 1500. The fix ensures that the managed devices work as expected.	AOS-W 8.6.0.10
AOS-224296	—	A few clusters got disconnected from the network. The fix ensures that the managed devices work as expected. This issue was observed in managed devices running ArubaOS 8.7.1.3 or later versions.	ArubaOS 8.7.1.3
AOS-225590	—	Some users experienced connectivity issues while roaming. This issue occurred when heavy load was encountered on the **STM** process due to the roaming of clients. The **STM** process was impacted due to the fix introduced for AOS-125897 to improve the synchronization of client visibility between the Mobility Master and managed devices. This issue was observed in managed devices running AOS-W 8.5.0.10 or later versions in a cluster setup. The fix ensures that the managed devices work as expected.	AOS-W 8.5.0.10
AOS-225614	—	Some AP-505H access points running ArubaOS 8.9.0.0 experienced poor network bandwidth issues. The fix ensures that the APs work as expected.	ArubaOS 8.9.0.0
AOS-225808	—	A few APs crashed after a cluster split. This issue occurred when there are seven or more managed devices in a dual stack deployment. The fix ensures that the APs work as expected. This issue was observed in managed devices running AOS-W 8.7.0.0 or later versions in a cluster setup.	ArubaOS 8.7.1.3
AOS-226324 AOS-225655	—	AirMatch stopped working on Mobility Masters running ArubaOS 8.7.1.1 or later versions. This issue occurred when the network had multiple 802.1ax APs. The fix ensures that the AirMatch feature works as expected.	ArubaOS 8.7.1.1
AOS-226516 AOS-226552	—	Some AP-505H mesh access points running ArubaOS 8.7.1.5 changed its wired MAC address every time after a reboot. The fix ensures that the APs do not change its MAC address every time after a reboot.	ArubaOS 8.7.1.5
AOS-226410	—	Cluster heartbeats were dropped in OAW-4850 switches running ArubaOS 8.7.1.5 in a cluster setup. The fix ensures that the cluster heartbeats are not dropped.	ArubaOS 8.7.1.5

Table 6: *Resolved Issues in AOS-W 8.8.0.2*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-226008	—	Cluster heartbeats were delayed and ping latency was also observed. This issue occurred due to continuous irregular traffic like ARP flooding. The fix ensures that the managed devices work as expected. This issue was observed in managed devices running ArubaOS 8.7.1.4 or later versions in a cluster setup.	ArubaOS 8.7.1.4
AOS-222895	—	The **STM** process was stuck on managed devices running AOS-W 8.6.0.0 or later versions. The fix ensures that the managed devices work as expected.	AOS-W 8.6.0.9

Chapter 7
Known Issues in AOS-W 8.8.0.2

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

Limitations

Following are the limitations observed in this release.

Port-Channel Limitation in OAW-4850 switches

On OAW-4850 switches with all the member ports of each port-channel configured from the same NAE (Network Acceleration Engine), if one of the member ports experiences link flap either due to a network event or a user-driven action, the rest of the port-channels also observe the link flap for less than a second.

Custom Certificate

When AOS-W is downgraded from 8.8.0.0 to 8.7.0.0, APs retain the custom certificate that was synchronized in AOS-W 8.8.0.0. In AOS-W 8.8.0.0, an AP downloads the custom certificate from a managed device and saves it in its flash memory, when a bridge mode SSID is configured. If the managed device is downgraded to AOS-W 8.7.0.0, the AP is also downgraded. The AP that is running AOS-W 8.7.0.0 checks if any custom certificate is saved in its flash memory. If the AP finds a custom certificate saved in its flash memory, it uses the custom certificate. If the AP does not find a custom certificate saved in its flash memory, it generates a new default certificate. If you do not want to use the custom certificate, issue the following command to erase the flash sector:

```
apfcutil -i RAP
```

The AP reboots and generates new default certificate.

Known Issues

Following are the known issues observed in this release.

Table 7: *Known Issues in AOS-W 8.8.0.2*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-125897 AOS-187598 AOS-189036 AOS-192082 AOS-192723 AOS-192731 AOS-192734 AOS-195746 AOS-198423 AOS-204676	151952	When a managed device reboots, APs and clients boot without IP addresses and other fields. This issue is observed in managed devices running AOS-W 8.0.1.0 or later versions.	AOS-W 8.0.1.0

Table 7: *Known Issues in AOS-W 8.8.0.2*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-151022 AOS-188417	185176	The output of the **show datapath uplink** command displays incorrect session count. This issue is observed in managed devices running AOS-W 8.1.0.0 or later versions.	AOS-W 8.1.0.0
AOS-151355	185602	A few managed devices are unable to pass traffic to the nexthop VPN concentrator (VPNC) using policy-based routing. This issue is observed in managed devices running AOS-W 8.0.1.0 or later versions.	AOS-W 8.0.1.0
AOS-153742 AOS-194948	188871	A stand-alone switch crashes and reboots unexpectedly. The log files list the reason for the event as **Hardware Watchdog Reset (Intent:cause:register 51:86:0:8)**. This issue is observed in OAW-4010 switches running AOS-W 8.5.0.1 or later versions in a Mobility Master-Managed Device topology.	AOS-W 8.5.0.1
AOS-190071 AOS-190372	—	A few users are unable to access websites when WebCC is enabled on the user role. This issue occurs in a Per User Tunnel Node (PUTN) setup when the VLAN of user role is in trunk mode. This issue is observed in OAW-4005 switches running AOS-W 8.4.0.0. **Workaround:** Perform the following steps to resolve the issue: 1.Remove web category from the ACL rules and apply **any any any permit** policy. 2. Disable WebCC on the user role. 3. Change the VLAN of user role from trunk mode to access mode.	AOS-W 8.4.0.0
AOS-193231 AOS-200101 AOS-207456	—	The **Dashboard > Infrastructure > Access Devices** page of the WebUI displays an error message, **Error retrieving information**. This issue is observed in Mobility Masters running ArubaOS 8.5.0.3 or later versions.	ArubaOS 8.5.0.3
AOS-200515 AOS-219987	—	The **DDS** process crashes on managed devices running ArubaOS 8.3.0.10 or later versions.	ArubaOS 8.3.0.10
AOS-208102 AOS-214040	—	APs running AOS-W 8.7.0.0 or later versions crash unexpectedly. The log files list the reason for the event as **Process /aruba/bin/sapd has too many open files (771)**.	AOS-W 8.7.0.0
AOS-209276	—	The **show datapath crypto counters** command displays the same output parameter, **AESCCM Decryption Invalid Replay Co** twice. This issue is observed in Mobility Masters running AOS-W 8.5.0.0 or later versions.	AOS-W 8.5.0.10

Table 7: *Known Issues in AOS-W 8.8.0.2*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-210416 AOS-210480	—	The **show ap client trail-info** command displays incorrect **VLAN(s)** values. This issue is observed in Mobility Masters running AOS-W 8.5.0.8 or later versions.	AOS-W 8.5.0.8
AOS-210490	—	Some managed devices running AOS-W 8.5.0.8 or later versions display the error message, **Error: Tunnel is part of a tunnel-group** while deleting a L2 GRE tunnel which is not a part of any tunnel group.	AOS-W 8.5.0.8
AOS-211720	—	The **STM** process crashes on managed devices running AOS-W 8.5.0.5 or later versions and hence, APs failover to another cluster.	AOS-W 8.5.0.5
AOS-212605 AOS-218721	—	Some APs running AOS-W 8.6.0.9 or later versions crashes unexpectedly. The log files list the reason for the event as **wlc_key_get_info+0x4/0x60 [wl_v6]**.	AOS-W 8.7.1.1
AOS-212861 AOS-215350 AOS-215522 AOS-216305	—	Some OAW-AP535 and OAW-AP555 access points running AOS-W 8.6.0.6 or later versions crash and reboot unexpectedly. The log file lists the reason for the reboot as **kernel panic: Take care of the TARGET ASSERT first.**	AOS-W 8.6.0.6
AOS-215303	—	Users are unable to view file names in the **Diagnostic > Technical Support > Copy Files** page of the WebUI. This issue occurs when **Flash file system** is selected as the source file. This issue is observed in managed devices running AOS-W 8.5.0.11 or later versions.	AOS-W 8.5.0.11
AOS-215669	—	Some managed devices running ArubaOS 8.6.0.7 or later versions crash and reboot unexpectedly. The log file lists the reason for the event as **Datapath timeout (Heartbeat Initiated) (Intent:cause:register 53:86:50:4)**.	ArubaOS 8.6.0.7
AOS-215712	—	Mobility Masters running ArubaOS 8.7.0.0 or later versions forward all syslog messages with severity level marked as debug. This issue occurs when CEF format is enabled on the Mobility Master.	ArubaOS 8.7.0.0
AOS-215852	—	Mobility Masters running AOS-W 8.6.0.6 or later versions log the error message, **ofa: 07765|ofproto|INFO|Aruba-SDN: 1 flow_mods 28 s ago (1 modifications).** This issue occurs when the UCC session idle timeout value is set to 35 seconds	AOS-W 8.6.0.6
AOS-215857 AOS-216162	—	Some OAW-AP514 and OAW-AP515 access points running AOS-W 8.4.0.0 or later versions crash and reboot unexpectedly. The log file lists the reason for reboot as, **AP Reboot reason: Warm-reset**. This issue occurs due to a beacon inactivity loop condition in the 5 GHz radio.	AOS-W 8.7.1.1

Table 7: *Known Issues in AOS-W 8.8.0.2*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-216145	—	Mobility Masters running ArubaOS 8.5.0.8 or later versions send continuous DNS requests to the managed devices. This issue occurs when a folder that is not available on the /mm node is trying to get synchronized on the managed devices. **Workaround:** 1. Issue the **show memory debug | include rsync** command to identify the name of the folder that is trying to get synchronized on the managed devices. 2. Ensure that the folder is not present in the /flash/upload/custom/ path of the Mobility Master and the issue the **no sync files <folder name>** command to stop synchronization.	ArubaOS 8.5.0.8
AOS-216536 AOS-220630	—	Some managed devices running ArubaOS 8.5.0.11 or later versions are unable to come up on the Mobility Master. This issue occurs when the managed devices get the branch IP address as the switch IP address in a VPNC deployment.	ArubaOS 8.5.0.11
AOS-216622	—	A few APs incorrectly display the restricted flag, **p = Restriction mode in POE-AF/AT** in the AP database even if the Ethernet port is disabled. This issue is observed in APs running AOS-W 8.7.0.0 or later versions.	AOS-W 8.7.0.0
AOS-217184 AOS-218026 AOS-220562 AOS-220985	—	Some OAW-4750XM switches running ArubaOS 8.7.1.1 or later versions crash and reboot unexpectedly. The log files list the reason for the events as, **Kernel Panic (Intent:cause:register 12:86:b0:4)**. This issue occurs due to socket buffer corruption.	ArubaOS 8.7.1.1
AOS-217890	—	Some managed devices running ArubaOS 8.5.0.10 or later versions crash and reboot unexpectedly. The log file lists the reason for the event as, **Datapath timeout (SOS Assert)**.	ArubaOS 8.5.0.10
AOS-218075 AOS-219316	—	Some managed devices running AOS-W 8.5.0.11 or later versions log multiple error message, **Trying to obtain mac address**.	AOS-W 8.5.0.11
AOS-218162	—	The wired Ethernet port does not form GRE tunnel with the managed device. This issue is observed in managed devices running AOS-W 8.7.1.1 or later versions.	AOS-W 8.7.1.1
AOS-218231 AOS-216177	—	Wireless users are unable to find a few wired clients. This issue is observed in controllers running AOS-W 8.7.1.1 or later versions.	AOS-W 8.7.1.1

Table 7: *Known Issues in AOS-W 8.8.0.2*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-218254 AOS-218875	—	Some managed devices running AOS-W 8.7.1.0 or later versions crashes unexpectedly. The log files list the reason for the event as **Reboot Cause: Kernel Panic (Intent:cause:register 12:86:e0:2).**	AOS-W 8.7.1.0
AOS-218621	—	Some APs running AOS-W 8.7.1.1 or later versions crashes unexpectedly. The log files list the reason for the event as **AP Reboot reason: BadAddr:6c0094119461 PC:wlc_ampdu_recv_ addba_resp+0x240/0x838 [wl_v6] Warm-reset**.	AOS-W 8.7.1.1
AOS-218795	—	Downloadable user roles are not downloaded and hence, user roles are not assigned to the tunnel-node users. This issue is observed in managed devices running AOS-W 8.7.1.2 or later versions.	AOS-W 8.7.1.2
AOS-219112	—	Some UBT clients hop between VLANs. This issue is observed in managed devices running AOS-W 8.7.1.1 or later versions.	AOS-W 8.7.1.1
AOS-219307 AOS-223234	—	Some managed devices running AOS-W 8.5.0.12 or later versions crash unexpectedly. The log files list the reason for the event as, **Reboot cause: Kernel Panic (Intent:cause:register 12:86:f0:2)**.	AOS-W 8.5.0.12
AOS-219376	—	Some users are unable to add VIA server details if the domain name exceeds 32 characters. This issue is observed in Mobility Masters running ArubaOS 8.7.1.2 or later versions.	ArubaOS 8.7.1.2
AOS-219383	—	The **Configuration > License > License Usage** tab does not display the license related details. This issue is observed in stand-alone controllers running AOS-W 8.5.0.12 or later versions.	AOS-W 8.5.0.12
AOS-219385	—	Some APs take a long time to come up on the backup data center after primary data center failover. This issue is observed in APs running ArubaOS 8.5.0.10 or later versions.	ArubaOS 8.5.0.10
AOS-219936	—	The stand-alone controller displays the error message, **Module Profile Manager is busy. Please try later** while configuring netdestination. This issue is observed in stand-alone controllers running AOS-W 8.7.1.1 or later versions.	AOS-W 8.7.1.1
AOS-220053	—	Some OAW-RAPs went down on managed devices running ArubaOS 8.6.0.5 or later versions. This issue occurs after a failover.	ArubaOS 8.6.0.5
AOS-220108	—	The **OFA** process crashes on Mobility Master Virtual Appliances running AOS-W 8.6.0.6 or later versions. This issue occurs when the **show openflow debug ports** command is executed.	AOS-W 8.6.0.6

Table 7: *Known Issues in AOS-W 8.8.0.2*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-220293	—	Some APs running AOS-W 8.7.1.1 or later versions crashes unexpectedly. The log files list the reason for the event as **aruba_wlc_ratesel_getmaxrate+0x34**.	AOS-W 8.7.1.1
AOS-220515	—	Some managed devices running AOS-W 8.0.0.0 or later versions display the error message, **|fpapps| filling up the default gateway configuration.**	AOS-W 8.5.0.12
AOS-220552	—	The **Configuration > Services > Clusters** page of the WebUI does not display the status of live upgrade. This issue occurs when the cluster profile name has blank spaces. This issue is observed in Mobility Masters running AOS-W 8.6.0.9 or later versions.	AOS-W 8.6.0.9
AOS-220704	—	Some APs are incorrectly displayed under different clusters. This issue is observed in managed devices running ArubaOS 8.5.0.11 or later versions.	ArubaOS 8.5.0.11
AOS-220903	—	The **s** flag indicating LACP striping is not displayed in the output of the **show ap database long** command even if LLDP is enabled on two uplinks. This issue is observed in APs running ArubaOS 8.6.0.8 or later versions.	ArubaOS 8.6.0.8
AOS-221005	—	Some stand-alone switches running AOS-W 8.7.1.2 or later versions are stuck in reboot loop. The log files list the reason for the event as **Nanny rebooted machine - fpapps process died (Intent:cause:register 34:86:50:2)**.	AOS-W 8.7.1.2
AOS-221429	—	Downloadable user role is not applied correctly to the first user connecting in the split tunnel mode. This issue is observed in stand-alone switches running ArubaOS 8.6.0.9 or later versions.	ArubaOS 8.6.0.9
AOS-221507	—	Some OAW-AP515 access points running AOS-W 8.7.1.3 or later versions crashes unexpectedly. The log files list the reason for the event as **BadAddr:ffffffc12c30ca80 PC:__alloc_ skb+0x110/0x1c8 Warm-reset**.	AOS-W 8.7.1.3
AOS-221666 AOS-222708	—	Some OAW-RAPs running ArubaOS 8.6.0.9 or later versions crash and reboot unexpectedly. The log file lists the reason for the event as, **Kernel panic - not syncing**.	ArubaOS 8.6.0.9
AOS-221726	—	Some managed devices running ArubaOS 8.7.1.1 or later versions are unable to form L2 clusters with its peers.	ArubaOS 8.7.1.1
AOS-221743 AOS-212229	—	Some APs running ArubaOS 8.5.0.10 or later versions reboot unexpectedly. The log files list the reason for the events as, **skb_release_data+0xa0/0xc8/neigh_ flush_dev+0x60**.	ArubaOS 8.5.0.10

Table 7: *Known Issues in AOS-W 8.8.0.2*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-222754	—	The SNMP walk to managed devices fails when the SNMP requets have the IPv6 address of the switch. This issue occurs when the primary managed device has VRRP IPv6 address configured. This issue is observed in managed devices running ArubaOS8.4.0.1 or later versions.	ArubaOS 8.4.0.1
AOS-222771	—	Some managed devices running ArubaOS 8.5.0.12 or later versions do not send SNMPv3 information to the OmniVista 3600 Air Manager server.	ArubaOS 8.5.0.12
AOS-222787	—	Some AP-335 access points running ArubaOS 8.7.1.3 or later versions reboot unexpectedly. The log file lists the reason for the event as, **kernel panic: Fatal exception**. This issue occurs due to a race condition.	ArubaOS 8.7.1.3
AOS-222931	—	Some APs do not form active tunnels with the AAC. This issue is observed in managed devices running ArubaOS 8.7.1.4 or later versions.	ArubaOS 8.7.1.4
AOS-223839	—	The output of the **show ap active** command does not display any value for **Outer IP**. This issue is observed in Mobility Masters running ArubaOS 8.6.0.9 or later versions.	ArubaOS 8.6.0.9
AOS-223848	—	The **+** symbol in the **Configuration > Services > AirGroup > Service-Based Policy** page of the WebUI does not allow users to create an AirGroup profile. Users can create an AirGroup profile only by navigating to the **Configuration > System > Profiles > AirGroup** page of the WebUI. This issue is observed in Mobility Masters running ArubaOS 8.0.0.0 or later versions.	ArubaOS 8.7.1.4
AOS-221144	—	ARP packets are not forwarded to the uplink switch when bcmc-optimization is enabled on the switches. This issue is observed in Mobility Masters and managed devices running AOS-W 8.5.0.9 or later versions.	AOS-W 8.5.0.9

Chapter 8
Upgrade Procedure

This chapter details software upgrade procedures. It is recommended that you schedule a maintenance window for the upgrade.

Read all the information in this chapter before upgrading your Mobility Conductor, managed device, or stand-alone switch.

Important Points to Remember

To upgrade your managed device or Mobility Conductor:

- 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 AOS-W runs on your managed device?
  - Are all managed devices running the same version of AOS-W?
  - What services are used on your managed device (employee wireless, guest access, OAW-RAP, wireless voice)?
- Resolve any existing issues (consistent or intermittent) before you upgrade.
- If possible, use FTP to load AOS-W 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 AOS-W, 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 the *Alcatel-Lucent Mobility Conductor Licensing Guide*.
- Multiversion is supported in a topology where the managed devices are running the same version as the Mobility Conductor, or two versions lower. For example multiversion is supported if a Mobility Conductor is running AOS-W 8.5.0.0 and the managed devices are running AOS-W 8.5.0.0, AOS-W 8.4.0.0, or AOS-W 8.3.0.0.

Memory Requirements

All Alcatel-Lucent 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 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 the minimum flash space inis 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 files, crash data, or flash backups from your the 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 flash memory. 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 CLI.

In the WebUI

From the Mobility Conductor, navigate to **Diagnostic > Technical Support > Delete Files** and remove any aging log files or redundant backups.

In the CLI

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

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 Conductor 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 flash memory, 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 back up 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 either of 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 AOS-W

Upgrade AOS-W using the WebUI or CLI.

CAUTION

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

NOTE

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 is displayed ccurs 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 AOS-W from a TFTP server, FTP server, or local file.

1. Download the AOS-W image from the customer support site.
2. Upload the AOS-W image to a PC or workstation on your network.
3. Validate the SHA hash for the AOS-W image:
   a. Download the **Alcatel.sha256** file from the download directory.
   b. Load the AOS-W 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.

NOTE

The AOS-W image file is digitally signed and is verified using RSA2048 certificates preloaded at the factory. The Mobility Conductor or managed device will not load a corrupted AOS-W image.

4. Log in to the AOS-W WebUI from the Mobility Conductor.
5. Navigate to the **Maintenance > Software Management > Upgrade** page.
   a. Select the **Local File** option 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.

NOTE

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

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

In the CLI

The following steps describe how to upgrade AOS-W from a TFTP server, FTP server, or local file.

1. Download the AOS-W image from the customer support site.

2. Open an SSH session to your Mobility Conductor.

3. Execute the **ping** command to verify the network connection between the Mobility Conductor 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 AOS-W image is loaded on the flash partition. 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 Conductor.

```
(host)#reload
```

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

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

Verifying the AOS-W Upgrade

Verify the AOS-W upgrade in the WebUI or CLI.

In the WebUI

The following steps describe how to verify that the Mobility Conductor is functioning as expected:

1. Log in to the WebUI and navigate to the **Dashboard > WLANs** page to verify the AOS-W image version.
2. Verify if all the managed devices are up after the reboot.
3. Navigate to the **Dashboard > Access Points** page to determine if your APs are up and ready to accept clients.
4. Verify that the number of APs and clients are as expected.
5. Test a different type of client in different locations, for each access method used.
6. 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

The following steps describe how to verify that the Mobility Conductor is functioning as expected:

1. Log in to the CLI to verify that all your managed devices are up after the reboot.
2. Execute the **show version** command to verify the AOS-W image version.
3. Execute the **show ap active** command to determine if your APs are up and ready to accept clients.
4. Execute the **show ap database** command to verify that the number of APs and clients are as expected.
5. Test a different type of client in different locations, for each access method used.
6. 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 AOS-W

A Mobility Conductor or managed device has two partitions, 0 and 1. If the upgrade fails on one of the partitions, you can reboot the Mobility Conductor or managed device from the other partition.

Pre-requisites

Before you reboot the Mobility Conductor or managed device with the pre-upgrade AOS-W version, perform the following steps:

1. Back up your Mobility Conductor 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 Conductor or managed device to boot with the previously saved configuration file.
4. Set the Mobility Conductor or managed device to boot from the partition that contains the pre-upgrade AOS-W version.

   When you specify a boot partition or copy an image file to a system partition, Mobility Conductor or managed device checks if the AOS-W version is compatible with the configuration file. An error message is displayed if the boot parameters are incompatible with the AOS-W version and configuration files.
5. After switching the boot partition, perform the following steps:

- Restore the pre-upgrade flash backup from the file stored on the Mobility Conductor or managed device. Do not restore the AOS-W flash backup file.
- Do not import the WMS database.
- If the RF plan is unchanged, do not import it. If the RF plan was changed before switching the boot partition, the changed RF plan does not appear in the downgraded AOS-W version.
- If any new certificates were added in the upgraded AOS-W version, reinstall these certificates in the downgraded AOS-W version.

Downgrade AOS-W version using the WebUI or CLI.

In the WebUI

The following steps describe how to downgrade the AOS-W version:

1. If the saved pre-upgrade configuration file is on an external FTP or TFTP server, copy the file to the Mobility Conductor 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, select **Flash file system**, and enter a file name (other than default.cfg).
   c. Click **Copy**.
2. Determine the partition on which your pre-upgrade AOS-W version is stored by navigating to the **Maintenance > Software Management > Upgrade** page. If a pre-upgrade AOS-W 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 or 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**, and click **Reboot**.

The Mobility Conductor or managed device reboots after the countdown period.

4. When the boot process is complete, verify that the Mobility Conductor or managed device is using the correct AOS-W version by navigating to the **Maintenance > Software Management > About** page.

In the CLI

The following steps describe how to downgrade the AOS-W version:

1. If the saved pre-upgrade configuration file is on an external FTP or TFTP server, use the following command to copy it to the Mobility Conductor 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 Conductor 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 AOS-W version is stored.

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

You cannot load a new image into the active system partition.

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

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

5. Reboot the Mobility Conductor or managed device.

```
(host) # reload
```

6. When the boot process is complete, verify that the Mobility Conductor or managed device is using the correct AOS-W version.

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

Before Calling Technical Support

Provide the following information when you call the 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 and 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 first 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.