AOS-W 8.5.0.9

Alcatel·Lucent Enterprise

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.

Revision History

The following table provides the revision history of this document.

Table 1: *Revision History*

Revision	Change Description
Revision 01	Initial release.

This AOS-W release notes includes the following topics:

NOTE

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

Important Points Before Upgrading to AOS-W 8.5.0.0

Starting from AOS-W 8.5.0.0, your CPU should support version SSE4.2. For deployments on versions prior to AOS-W 8.5.0.0, SSSE3 is the minimum supported version. Additionally the CPU should also support Intel VT.

DPI Classification

DPI classification is not initialized after a switch is upgraded from AOS-W 8.4.0.0, 8.4.0.1, or 8.4.0.2 to AOS-W 8.5.0.0. The affected platforms are OAW-4x50 Series switches.

An additional reboot of the affected platform is required to initialize DPI classification.

To check the status of DPI classification after upgrading an affected platform from AOS-W 8.4.0.0, 8.4.0.1, or 8.4.0.2 to AOS-W, 8.5.0.0, issue the **show firewall | include dpi** command. In the following example, DPI classification is disabled:

```
(host) #show firewall | include dpi
DPI Classification      Disabled [Cfg: enabled, PEF license: installed]
```

If DPI classification is enabled, further action is not needed. However, if DP classification is disabled, issue the **show datapath utilization** and check if the DPI classification CPUs are initialized. In the following example, the DPI classification CPUs are disabled:

```
(host) #show datapath utilization

Datapath CPU Allocation Summary
Slow Path (SP) : 1,  Slow Path Gateway (SPGW) : 1
Fast Path (FP) : 17,  Fast Path Gateway (FPGW) : 1
DPI : 0, Crypto (CRYP) : 0
Slow Path Spare (SPSPARE) : 0
```

If the DPI classification CPUs are not initialized, reboot the affected platform by:

- Issuing the **reload** command.
- Power cycling the switch.

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 Master Licensing Guide*
- *Alcatel-Lucent Virtual Appliance Installation Guide*
- *Alcatel-Lucent Mobility Master Hardware Appliance Installation 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 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 8, Windows 10, and macOS

Contacting Support

Table 2: *Contact Information*

Contact Center Online	
Main Site	https://www.al-enterprise.com
Support Site	https://businessportal2.alcatel-lucent.com
Email	ebg_global_supportcenter@al-enterprise.com
Service & Support Contact Center Telephone	

Contact Center Online	
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

Chapter 2
New Features and Enhancements

There are no features or enhancements introduced in this release.

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 8.5.0.9*

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 8.5.0.9*

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
MC-VA-xxx Virtual OmniAccess Mobility Controllers	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 8.5.0.9*

AP Family	AP Model
OAW-AP100 Series	OAW-AP104, OAW-AP105
OAW-AP103 Series	OAW-AP103
OAW-AP110 Series	OAW-AP114, OAW-AP115
OAW-AP130 Series	OAW-AP134, OAW-AP135
OAW-AP 170 Series	OAW-AP175AC, OAW-AP175AC-F1, OAW-AP175DC, OAW-AP175DC-F1, OAW-AP175P, OAW-AP175P-F1
OAW-AP200 Series	OAW-AP204, OAW-AP205
OAW-AP203H Series	OAW-AP203H
OAW-AP205H Series	OAW-AP205H
OAW-AP207 Series	OAW-AP207
OAW-AP203R Series	OAW-AP203R, OAW-AP203RP
OAW-AP210 Series	OAW-AP214, OAW-AP215
OAW-AP 220 Series	OAW-AP224, OAW-AP225
228 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-AP303H Series	OAW-AP303H

Table 5: *Supported AP Platforms in AOS-W 8.5.0.9*

AP Family	AP Model
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
OAW-AP387	OAW-AP387
OAW-AP510 Series	OAW-AP514, OAW-AP515
OAW-AP530 Series	OAW-AP534, OAW-AP535
OAW-AP550 Series	OAW-AP555
OAW-RAP3 Series	OAW-RAP3WN, OAW-RAP3WNP
OAW-RAP100 Series	OAW-RAP108, OAW-RAP109
OAW-RAP155 Series	OAW-RAP155, OAW-RAP155P

Regulatory Updates

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_75272

Resolved Issues

After upgrading to AOS-W 8.5.0.9, it is recommended to re-store flash backup of data in OAW-4850 switches, that were earlier upgraded from AOS-W 8.3.0.x to AOS-W 8.5.0.8 (or prior versions). This ensures that internal user database entries are not lost. For more details, see AOS-203656.

Also, the following issues are resolved in this release.

NOTE

We have migrated to a new defect tracking tool. All the bugs are listed with the new bug ID, which is prefixed by AOS.

Table 6: *Resolved Issues in AOS-W 8.5.0.9*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-197326 AOS-203063	—	**Symptom:** Mobility Master did not generate AirMatch optimization. The fix ensures that the Mobility Master works as expected. **Scenario:** This issue occurred when APs received large number of events. This issue was observed in Mobility Masters running AOS-W 8.6.0.3 or later versions.	AirMatch	All platforms	AOS-W 8.5.0.3
AOS-200277 AOS-204071	—	**Symptom:** Managed devices logged the error message, **There is only 996 MB left on the flash. At least 1000 MB of free flash space is recommended to keep the system stable**. The fix ensures that the error message is not displayed. **Scenario:** This issue was observed in managed devices running AOS-W 8.5.0.8 or later versions.	switch-Platform	All platforms	AOS-W 8.5.0.8
AOS-200568 AOS-202762 AOS-203588	—	**Symptom:** GSM channel entries were not replicated from managed device to Mobility Master. The fix ensures that the GSM channel entries are replicated to the Mobility Master. **Scenario:** This issue was observed in managed devices running AOS-W 8.5.0.5 or later versions.	GSM	All platforms	AOS-W 8.5.0.5

Table 6: *Resolved Issues in AOS-W 8.5.0.9*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-200595 AOS-203897	—	**Symptom:** WebUI displayed the error message, **Internal Server Error** when users copied files to SCP server using the **Diagnostics > Technical Support > Copy Files** page. The fix ensures that the WebUI does not display the error message. **Scenario:** This issue was observed in OAW-4850 switches running AOS-W 8.5.0.3 or later versions.	Web Server	OAW-4850 switches	AOS-W 8.5.0.3
AOS-202577 AOS-204027 AOS-204410 AOS-204811	—	**Symptom:** AirGroup stopped working on managed devices. The fix ensures that AirGroup works as expected. **Scenario:** This issue was observed in managed devices running AOS-W 8.6.0.3 or later versions in a cluster setup.	Base OS Security	All platforms	AOS-W 8.6.0.3
AOS-202743 AOS-203498 AOS-203507 AOS-204322	—	**Symptom:** The **Configuration > Interfaces > VLANs** tab did not display the IP addresses of Mobility Master and managed devices. The fix ensures that WebUI displays the IP addresses. **Scenario:** This issue was observed in Mobility Master and managed devices running AOS-W 8.5.0.7 or later versions.	WebUI	All platforms	AOS-W 8.5.0.7
AOS-203168	—	**Symptom:** Managed devices were disconnecting from the cluster frequently. Also, the cluster heartbeats were randomly missed on managed devices which led to packet loss. The fix ensures that the managed devices work as expected. **Scenario:** This issue was observed in managed devices running AOS-W 8.6.0.3 or later versions in a cluster setup.	Cluster-Manager	All platforms	AOS-W 8.6.0.3
AOS-203656 AOS-204128	—	**Symptom:** A managed device displayed an error message, **Please wait while we take the flash backup...Error backing up DBs**, when taking a flash backup. The fix ensures that the database files are migrated in compatible format. **Scenario:** This issue occurred due to incompatible database files. This issue was observed when OAW-4850 switches were upgraded from AOS-W 8.3.0.x version to AOS-W 8.5.0.x version.	Database	OAW-4850 switches	AOS-W 8.5.0.8
AOS-203702 AOS-204024 AOS-204423 AOS-204544	—	**Symptom:** Managed devices crashed and rebooted unexpectedly. The log files listed the reason for the event as **Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:4)** . The fix ensures that the managed devices work as expected. **Scenario:** This issue was observed in OAW-40xx Series, OAW-4450, OAW-4550, OAW-4650, OAW-4750, OAW-4750XM switches running AOS-W 8.5.0.8 or later versions.	switch-Datapath	OAW-40xx Series, OAW-4450, OAW-4550, OAW-4650, OAW-4750, OAW-4750XM switches	AOS-W 8.5.0.8

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

NOTE

We have migrated to a new defect tracking tool. Some bugs are listed with the new bug ID, which is prefixed by AOS.

Limitation

Zero Touch Provisioning and multi-version support for OAW-4104 switches are currently not supported.

NOTE

It is recommended to have the Mobility Master and managed device running the same AOS-W version.

Known Issues

Following are the known issues observed in this release.

Table 7: *Known Issues in AOS-W 8.5.0.9*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-131325 AOS-146748	159222 179137	**Symptom:** The number of clients displayed in the active-standby IP field under **Wireless Clients** table on the **Dashboard > Overview > Clients** page in the WebUI is incorrect. **Scenario:** This issue occurs due to a cluster failover causing race condition. This issue is observed in Mobility Masters running AOS-W 8.1.0.0 or later versions. **Workaround:** None.	Base OS Security	All platforms	AOS-W 8.1.0.0
AOS-145410 AOS-146962	177352 179430	**Symptom:** A managed device crashes and reboots with the error message, **Atleast 2000 MB free flash is recommended to keep system stable. Please clean up your flash file.** **Scenario:** This issue occurs when a managed device receives IP packets larger than one segment. This issue is observed in managed devices running AOS-W 8.2.0.2 or later versions. **Workaround:** None.	switch-Platform	All platforms	AOS-W 8.2.0.2
AOS-145566	177559	**Symptom:** A Mobility Master is unable to forward the traffic that is sourced from an IP interface in the gateway. **Scenario:** This issue occurs when netdestinations are used in the routing ACL rule. This issue is observed in Mobility Masters running AOS-W 8.0.1.0 or later versions. **Workaround:** None.	Policy-Based Routing	All platforms	AOS-W 8.0.1.0
AOS-148643 AOS-150529	—	**Symptom:** Clients are unable to connect to the 802.1x SSID when UAC and AAC are different. **Scenario:** This issue is observed in managed devices running AOS-W 8.3.0.0 or later versions. **Workaround:** None.	Station Management	All platforms	AOS-W 8.3.0.0
AOS-151022 AOS-188417	185176	**Symptom:** The output of the **show datapath uplink** command displays incorrect session count. **Scenario:** This issue is observed in managed devices running AOS-W 8.1.0.0 or later versions. **Workaround:** None.	switch-Datapath	All platforms	AOS-W 8.1.0.0

Table 7: *Known Issues in AOS-W 8.5.0.9*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-151355	185602	**Symptom:** A few 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 AOS-W 8.0.1.0 or later versions. **Workaround:** None.	Policy-Based Routing	All platforms	AOS-W 8.0.1.0
AOS-151557	185873	**Symptom:** The hotspot-shield application is not classified for some Android clients. **Scenario:** This issue occurs as the Android client does not provide support for this application. This issue is observed in OAW-4750 switches running ArubaOS 8.3.0.2 or later versions. **Workaround:** None.	DPI	OAW-4750 switches	AOS-W 8.3.0.2
AOS-153185	188148	**Symptom:** The **Dashboard > Security > Active rogue > Locate** option does not function in the WebUI. **Scenario:** This issue is observed in Mobility Masters running AOS-W 8.3.0.1 or later versions. **Workaround:** None.	WebUI	All platforms	AOS-W 8.3.0.1
AOS-153742 AOS-194948	188871	**Symptom:** 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)**. **Scenario:** 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. **Workaround:** None.	switch- Datapath	OAW-4010 switches	AOS-W 8.5.0.1
AOS-155037	190571	**Symptom:** A OAW-RAP fails to boot up. **Scenario:** This issue occurs in a OAW-RAP with EST key type, **X9.62/SECG curve**. This issue is observed in OAW-AP303H access points running AOS-W 8.3.0.3 or later versions. **Workaround:** None.	CPsec	OAW-AP303H access points	AOS-W 8.3.0.3
AOS-155801	191726	**Symptom:** The SNMP walk performed from OmniVista 3600 Air Manager does not produce correct results. **Scenario:** This issue is observed in managed devices running AOS-W 8.3.0.3. **Workaround:** None.	SNMP	All platforms	AOS-W 8.3.0.3

Table 7: *Known Issues in AOS-W 8.5.0.9*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-156068	192100	**Symptom:** The **DDS** process in a managed device crashes unexpectedly. **Scenario:** This issue is observed in managed devices running AOS-W 8.2.1.1 or later versions. **Workaround:** None.	Base OS Security	All platforms	AOS-W 8.2.1.1
AOS-156085 AOS-157704	192119 194393	**Symptom:** A few managed devices are unable to obtain the switch-IP address during boot up after an upgrade. **Scenario:** This issue is observed in managed devices running AOS-W 8.1.0.0 or later versions. **Workaround:** None.	Configuration	All platforms	AOS-W 8.1.0.0
AOS-156742 AOS-156977	193031 193319	**Symptom:** A user is unable to make any change to IP Probe configuration, after forwarding a complete configuration using API. **Scenario:** This issue is observed in managed devices running AOS-W 8.0.1.0. **Workaround:** None.	Configuration	All platforms	AOS-W 8.0.1.0
AOS-157462 AOS-202579	—	**Symptom:** The web_cc process crashes on a managed device. **Scenario:** This issue is observed in managed devices running AOS-W 8.2.2.6 or later versions. **Workaround:** None.	WebCC	All platforms	AOS-W 8.2.2.6
AOS-157492	194064	**Symptom:** VRRP authentication fails in a managed device. **Scenario:** This issue is observed in managed devices running AOS-W 8.2.1.0. **Workaround:** None.	VRRP	All platforms	AOS-W 8.2.1.0
AOS-157795	194516	**Symptom:** A few managed devices are unable to process two **APN usb-init** strings using the **uplink cellular apn** command with Huawei E3372 modem. **Scenario:** This issue is observed in managed devices running AOS-W 8.3.0.0 or later versions. **Workaround:** None.	switch-Platform	All platforms	AOS-W 8.3.0.6

Table 7: *Known Issues in AOS-W 8.5.0.9*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-182847	—	**Symptom:** A few users are unable to copy the **WPA Passphrase** field and **High-throughput** profile to a new SSID profile in the **Configuration > System > Profiles > Wireless LAN > SSID > <SSID_Profile>** option of the WebUI. **Scenario:** This issue occurs when a new SSID profile is created from an existing SSID profile in the WebUI. This issue is observed in managed devices running AOS-W 8.4.0.0 in a Mobility Master-Managed Device topology. **Workaround:** None.	WebUI	All platforms	AOS-W 8.4.0.0
AOS-184135 AOS-195866	—	**Symptom:** A few users are unable to download applications from Google Play Store. **Scenario:** This issue occurs when the YouTube application is blocked. This issue is observed in stand-alone switches running AOS-W 8.4.0.0 or later versions. **Workaround:** None.	switch-Datapath	All platforms	AOS-W 8.4.0.0
AOS-184801	—	**Symptom:** A few managed devices crash and reboot unexpectedly. The log files list the reason for the event as **Datapath exception**. **Scenario:** This issue is observed in managed devices running AOS-W 8.4.0.0. **Workaround:** None.	switch -Datapath	All platforms	AOS-W 8.4.0.0
AOS-184947 AOS-192737	—	**Symptom:** The jitter and health score data are missing from the **Dashboard > Infrastructure > Uplink > Health** page in the WebUI. **Scenario:** This issue is observed in Mobility Master running AOS-W 8.4.0.4 or later versions. **Workaround:** None.	WebUI	All platforms	AOS-W 8.4.0.4
AOS-184977 AOS-188242 AOS-188378 AOS-197491	—	**Symptom:** The output of basic commands such as **show version**, **show clock**, and **show image version** are unable to display any information and the default gateway details are missing in a managed device. **Scenario:** This issue occurs when the **/tmp** directory runs out of memory because of too many logs from the Policy Manager. This issue is observed in managed devices running AOS-W 8.4.0.0 or later versions. **Workaround:** None.	Routing	All platforms	AOS-W 8.4.0.0

Table 7: *Known Issues in AOS-W 8.5.0.9*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-185538	—	**Symptom:** High number of EAP-TLS timeouts are observed in a managed device. **Scenario:** This issue occurs because multiple IP addresses are assigned to each client. This issue is observed in managed devices running AOS-W 8.3.0.8 or later versions.	Base OS Security	All platforms	AOS-W 8.3.0.8
AOS-186133	—	**Symptom:** A few managed devices display abnormally high multicast traffic in **Performance Summary > All Radios** monitoring page. **Scenario:** This issue is observed in OAW-AP320 Series access points running AOS-W 8.3.0.6. **Workaround:** None.	AP-Wireless	OAW-AP320 Series access points	AOS-W 8.3.0.6
AOS-186411	—	**Symptom:** A few users are unable to remove a VLAN from port channel trunk. **Scenario:** This issue is observed in Mobility Masters running AOS-W 8.3.0.0 or later versions. **Workaround:** Execute the **switchport trunk allowed vlan 1-4094** command to add the allowed VLAN range (1-4094). Then, execute the **switchport trunk allowed vlan remove 259** command to remove the VLAN from the port channel trunk.	Interface	All platforms	AOS-W 8.3.0.0
AOS-186774	—	**Symptom:** When the **show memory cfgm** command is executed, a large memory allocation is displayed in the output of the command. **Scenario:** This issue is observed in managed devices running AOS-W 8.3.0.0 or later versions. **Workaround:** None.	Configuration	All platforms	AOS-W 8.3.0.6
AOS-187115	—	**Symptom:** Application name in the policy configuration is incorrect in the **Configuration > Roles & Policies > Policies > <Policy name>** WebUI page. **Scenario:** This issue occurs when the WebUI is accessed for the first time. This issue is observed in Mobility Masters running AOS-W 8.2.2.0 or later versions. **Workaround:** None.	WebUI	All platforms	AOS-W 8.2.2.0

Table 7: *Known Issues in AOS-W 8.5.0.9*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-187422 AOS-189258	—	**Symptom:** The output of **show log all** and **show audit-trail** commands displays the unencrypted password entered for non-profile commands such as **aaa test-server** command. **Scenario:** This issue is observed in a Mobility Master Virtual Appliance running AOS-W 8.3.0.5 or later versions. **Workaround:** None.	Configuration	All platforms	AOS-W 8.3.0.5
AOS-187834	—	**Symptom:** A few APs do not send Port VLAN IDs in an LLDP packet although the **native-vlan-id** parameter is set using the **ap system-profile** command. **Scenario:** This issue is observed in APs running AOS-W 8.2.2.0 or later versions. **Workaround:** None.	AP-Platform	All platforms	AOS-W 8.2.2.5
AOS-187911	—	**Symptom:** The **Wireless Clients** section of the **Dashboard > Overview** page in the WebUI displays incorrect client usage values. **Scenario:** This issue is observed in Mobility Masters running AOS-W 8.4.0.0 or later versions. **Workaround:** Add a tooltip over the usage tab to mention that the current client usage value accounts for the last 15 min.	WebUI	All platforms	AOS-W 8.4.0.0
AOS-188090 AOS-196004 AOS-199152	—	**Symptom:** The **Dashboard > Overview > Clients** page of the WebUI displays incorrect usage values intermittently. **Scenario:** This issue is observed in Mobility Master Virtual Appliances running AOS-W 8.4.0.0 or later versions. **Workaround:** None.	Monitoring	All platforms	AOS-W 8.4.0.0
AOS-188271 AOS-196680 AOS-201542 AOS-201956 AOS-202569 AOS-202570	—	**Symptom:** APs crash and reboot unexpectedly. The log file lists the reason for the event as **BadAddr:20000002d PC:crypto_authenc_ ahash+0x2c/0x90 Warm-reset.** **Scenario:** This issue is observed in OAW-AP515 access points running AOS-W 8.5.0.0 or later versions. **Workaround:** None.	AP-Wireless	OAW-AP515 access points	AOS-W 8.5.0.0

Table 7: *Known Issues in AOS-W 8.5.0.9*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-188285	—	**Symptom:** A mesh portal reboots continuously because the **wpa_hex_key** value exceeds more than 132 bytes string in **the ap mesh-recovery-profile cluster <cluster_id> wpa-hexkey <wpa_hex_key>** command. The log files list the reason for the event as **AP rebooted Tue Jun 11 10:40:01 CDT 2019; Critical process /aruba/bin/meshd [pid 2450] DIED, process marked as RESTART**. **Scenario:** This issue is observed in APs running AOS-W 8.3.0.7 as a mesh portal. **Workaround:** ■ Modify **mesh-recovery-profile** by using **mesh-recovery-generate** command. ■ Reboot the mesh portal and issue the **setenv mesh_role 0** command on apboot in the console port of the AP. ■ Reprovision the AP to mesh portal.	Mesh	All platforms	AOS-W 8.3.0.7
AOS-188478	—	**Symptom:** The OAW-RAP whitelist file does not contain the first MAC address entry. **Scenario:** This issue occurs when the user executes the **show whitelist-db rap export-css <filename>** command to export the OAW-RAP whitelist file to the switch directory. This issue is observed in stand-alone switches running AOS-W 8.3.0.5 or later versions. **Workaround:** None.	Local Database	All platforms	AOS-W 8.3.0.5
AOS-188898 AOS-198730 AOS-200227	—	**Symptom:** The **postgres** process crashes on a managed device. **Scenario:** This issue is observed in managed devices running AOS-W 8.2.1.0 or later versions. **Workaround:** None.	Database	All platforms	AOS-W 8.2.2.6
AOS-188979 AOS-201731	—	**Symptom:** LEAP authenticated wireless clients are unable to connect to OAW-AP535 access points. **Scenario:** This issue is observed in OAW-AP535 access points running AOS-W 8.5.0.5 or later versions.	AP-Wireless	OAW-AP535 access points	AOS-W 8.5.0.5

Table 7: *Known Issues in AOS-W 8.5.0.9*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-189194	—	**Symptom:** The 5 GHz and 2.4 GHz antenna values are swapped after AP provisioning rules configuration is committed in the **Configuration > Access Points > Provisioning Rules** page of the WebUI. **Scenario:** This issue occurs when the user selects the **Set Antenna Gain for Dual Band mode** option from the **Actions** drop-down list in the **Configuration > Access Points > Provisioning Rules** page, and enters the **5 GHz** and **2.4 GHz** field values in the WebUI. This issue is observed in Mobility Master Virtual Appliances running AOS-W 8.4.0.3 or later versions. **Workaround:** None.	WebUI	All platforms	AOS-W 8.5.0.0
AOS-190071 AOS-190372	—	**Symptom:** A few users are unable to access websites when WebCC is enabled on the user role. **Scenario:** 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 to resolve the issue: ■ Remove web category from the ACL rules and apply **any any any permit** policy. ■ Disable WebCC on the user role. ■ Change the VLAN of user role from trunk mode to access mode.	WebCC	OAW-4005 switches	AOS-W 8.4.0.0
AOS-190240 AOS-192168	—	**Symptom:** The SNMP OIDs provide incorrect result in a cluster setup. **Scenario:** This issue is observed in managed devices running AOS-W 8.3.0.0 or later versions. **Workaround:** None.	SNMP	All platforms	AOS-W 8.3.0.0
AOS-191216 AOS-196523 AOS-199160	—	**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:e0:2)** **Scenario:** This issue is observed in managed devices running AOS-W 8.5.0.4 or later versions. **Workaround:** None.	switch-Platform	All platforms	AOS-W 8.5.0.4

Table 7: *Known Issues in AOS-W 8.5.0.9*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-191446 AOS-201647	—	**Symptom:** Users are unable to change the password of PSK authenticated SSID profiles from lower node levels. **Scenario:** This issue occurs when the AP group is mapped to an IoT profile. This issue is observed in managed devices running AOS-W 8.5.0.6 or later versions.	IoT	All platforms	AOS-W 8.5.0.6
AOS-191539	—	**Symptom:** The configuration synchronization fails and **CONFIG Failure** is displayed as the status of the synchronization displays in a managed device. The log files list the **Error: Tunnel is an L2 GRE Tunnel, Delete the Vlans, before changing the mode." executing "tunnel mode gre 2048** error message. **Scenario:** This issue occurs when the interface tunnel is set as 2048. This issue is observed in managed devices running AOS-W 8.4.0.0 or later versions in a Mobility Master-Managed Device topology. **Workaround:** None.	Interface	All platforms	AOS-W 8.4.0.1
AOS-191612	—	**Symptom:** The MAC address of users connected using VIA is not sent to ClearPass Policy Manager for authentication. **Scenario:** This issue occurs when IKE V2 with EAP-FTC is used for VIA authentication. This issue is observed in Mobility Masters running AOS-W 8.5.0.1 or later versions. **Workaround:** None.	IPsec	All platforms	AOS-W 8.5.0.1
AOS-192725 AOS-190476 AOS-196004	—	**Symptom:** The **Dashboard > Overview** page of the WebUI displays incorrect number of users intermittently. **Scenario:** This issue is observed in Mobility Masters running AOS-W 8.3.0.8 or later versions. **Workaround:** None.	Monitoring	All platforms	AOS-W 8.3.0.8
AOS-192738 AOS-197047	—	**Symptom:** The Mobility Master list in the WebUI incorrectly displays the mac address of the primary Mobility Master for the secondary Mobility Master. **Scenario:** This issue is observed in Mobility Masters running AOS-W 8.3.0.10 or later versions. **Workaround:** None.	WebUI	All platforms	AOS-W 8.3.0.10

Table 7: *Known Issues in AOS-W 8.5.0.9*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-193033 AOS-198921 AOS-198953	—	**Symptom:** Some clients are not redirected to the captive portal page. **Scenario:** This issue occurs because the **Nginx** process fails due to a race condition. This issue is observed in managed devices running AOS-W 8.4.0.2 or later versions. **Workaround:** None.	Captive Portal	All platforms	AOS-W 8.4.0.2
AOS-193083	—	**Symptom:** The cluster upgrade fails on a 2 node cluster because the AP platform capacity of the managed device is only 4 and the hash table size is calculated as zero. **Scenario:** This issue is observed in Mobility Controller Virtual Appliances running AOS-W 8.5.0.0 or later versions. **Workaround:** None.	Cluster-Manager	All platforms	AOS-W 8.5.0.0
AOS-193184	—	**Symptom:** L2 connected managed devices in a cluster move to L3 connected state after an upgrade. **Scenario:** This issue is observed in managed devices running AOS-W 8.5.0.2 or later versions. **Workaround:** None.	Cluster-Manager	All platforms	AOS-W 8.5.0.2
AOS-193560 AOS-198565 AOS-200262 AOS-204794	—	**Symptom:** The number of APs that are DOWN are incorrectly displayed in the WebUI. However, CLI displays the correct status of APs. **Scenario:** This issue is observed in Mobility Masters running AOS-W 8.4.0.4 or later versions. **Workaround:** None.	WebUI	All platforms	AOS-W 8.4.0.4
AOS-193775 AOS-194581 AOS-197372	—	**Symptom:** A mismatch of AP count and client count is observed between the Mobility Master and the managed device. **Scenario:** This issue is observed in Mobility Masters running AOS-W 8.3.0.0 or later versions. **Workaround:** None.	Monitoring	All platforms	AOS-W 8.5.0.2
AOS-193840	—	**Symptom:** The managed device loses connectivity to IPv6 gateway intermittently. **Scenario:** This issue is observed in managed devices running AOS-W 8.3.0.6 or later versions. **Workaround:** None.	switch- Datapath	All platforms	AOS-W 8.3.0.6

Table 7: *Known Issues in AOS-W 8.5.0.9*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-193883 AOS-197756	—	**Symptom:** A few APs are unable to use DHCP IPv6 addresses and option 52 for master discovery. **Scenario:** This issue occurs when the APs do not clear the previous LMS entries after the upgrade. This issue is observed in access points running AOS-W 8.3.0.8 or later versions. **Workaround:** Delete the IPv4 addresses from ap system profile using the command, **ap system-profile** and from high availability profiles using the command, **ha.**	AP Platform	All platforms	AOS-W 8.3.0.8
AOS-194082 AOS-196092	—	**Symptom:** A few APs crash and reboot unexpectedly. The log files lists the reason for the event as **BadPtr:00000006 PC:wlc_keymgmt_ wsec+0x28/0xa4 [wl_v6] Warm-reset.** **Scenario:** This issue is observed in access points running AOS-W 8.6.0.0 or later versions. **Workaround:** None.	AP-Wireless	All platforms	AOS-W 8.6.0.0
AOS-194370	—	**Symptom:** High memory utilization is observed in the **cluster manager** process of managed devices. **Scenario:** This issue is observed in managed devices running AOS-W 8.4.0.2 or later versions in a cluster setup. **Workaround:** None.	Cluster-Manager	All platforms	AOS-W 8.4.0.2
AOS-194381	—	**Symptom:** Some managed devices loose the route-cache entries and drop the VRRP IP addresses sporadically. **Scenario:** This issue is observed in managed devices running AOS-W 8.3.0.7 or later versions. **Workaround:** None.	switch-Datapath	All platforms	AOS-W 8.3.0.7
AOS-194846	—	**Symptom:** The commands **show ap arm history** and **show airmatch debug optimization** do not display any output. **Scenario:** This issue is observed in Mobility Masters running AOS-W 8.3.0.7 or later versions.	Airmatch	All platforms	AOS-W 8.3.0.7

Table 7: *Known Issues in AOS-W 8.5.0.9*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-194911	—	**Symptom:** Incorrect flag output is displayed for APs configured with 802.1X authentication when the **show ap database** command is executed. **Scenario:** This issue is observed in APs running AOS-W 8.5.0.2 or later versions. **Workaround:** None.	AP-Platform	All platforms	AOS-W 8.5.0.2
AOS-194925 AOS-195413	—	**Symptom:** A Branch office managed device is unable to failover to a secondary VPNC managed device. **Scenario:** This issue occurs because the secondary VPNC's MAC address is not updated on the running configuration of the managed device. This issue is observed in Mobility Master Virtual Appliances and Branch office managed devices running AOS-W 8.5.0.2 or later versions. **Workaround:** None.	Configuration	All platforms	AOS-W 8.5.0.2
AOS-194930	—	**Symptom:** The **Auth Sub-type** column under **Managed Network > Dashboard > Overview > Clients** table displays **None** though the authentication sub-type is **EAP-PEAP.** **Scenario:** This issue occurs in some 802.1X authenticated users after a failed station reauthentication attempt. This issue is observed in managed devices running AOS-W 8.3.0.7 or later versions. **Workaround:** None.	Base OS Security	All platforms	AOS-W 8.3.0.7
AOS-194964	—	**Symptom:** A few users are unable to clone the configuration from an existing group to a new group in a Mobility Master. **Scenario:** This issue is observed in Mobility Masters running AOS-W 8.4.0.1 or later versions. **Workaround:** Change the operating mode of the AP from am-mode to ap-mode using the **ap spectrum local-override** command.	Configuration	All platforms	AOS-W 8.5.0.2
AOS-195089	—	**Symptom:** The DNS traffic is incorrectly getting classified as Thunder and is getting blocked. **Scenario:** This issue occurs when the DNS traffic is blocked and peer-peer ACL is denied for users. This issue is observed in managed devices running AOS-W 8.3.0.7 or later versions. **Workaround:** None.	switch-Datapath	All platforms	AOS-W 8.3.0.7

Table 7: *Known Issues in AOS-W 8.5.0.9*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-195100 AOS-198302	—	**Symptom:** The health status of a managed device is incorrectly displayed as **Poor** in the **Dashboard > Infrastructure** page of the Mobility Master WebUI. **Scenario:** This issue is observed in Mobility Masters running AOS-W 8.3.0.7 or later versions. **Workaround:** None.	WebUI	All platforms	AOS-W 8.3.0.7
AOS-195177	—	**Symptom:** Managed devices frequently generate internal system error logs. **Scenario:** This issue occurs when the **sapd** process reads a non-existent interface. This issue is observed in OAW-4650 switches running AOS-W 8.3.0.7 or later versions. **Workaround:** None.	AP-Wireless	OAW-4650 switches	AOS-W 8.3.0.7
AOS-195228	—	**Symptom:** The device status is always displayed as inactive when SNMP walk is performed. **Scenario:** This issue is observed in stand-alone switches running AOS-W 8.5.0.2 or later versions. **Workaround:** None.	SNMP	All platforms	AOS-W 8.5.0.2
AOS-195434	—	**Symptom:** An AP crashes and reboots unexpectedly. The log files list the reason for the event as **Reboot caused by kernel panic: Fatal exception**. **Scenario:** This issue is observed in APs running AOS-W 8.5.0.0 o or later versions in a Mobility Master-Managed Device topology. **Workaround:** None.	AP-Wireless	All platforms	AOS-W 8.5.0.2
AOS-195526	—	**Symptom:** Clients are unable to get the DHCP address. **Scenario:** This issue occurs because the ACE entries of the logon role ACL changes to **Deny all** when the PEFNG feature is disabled. This issue is observed in managed devices running AOS-W 8.3.0.8 or later versions. **Workaround:** None.	Base OS Security	All platforms	AOS-W 8.3.0.8

Table 7: *Known Issues in AOS-W 8.5.0.9*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-195939	—	**Symptom:** UBT users are assigned **logon** role when they receive the same IP addresses. **Scenario:** This issue is observed in managed devices running AOS-W 8.5.0.2 or later versions. **Workaround:** None.	Tunnel-Node-Manager	All platforms	AOS-W 8.5.0.2
AOS-196115	—	**Symptom:** Users are unable to configure untrusted VLAN in the **Configuration > Interfaces > Ports** page of the WebUI. **Scenario:** This issue is observed in Mobility Masters running AOS-W 8.5.0.0 or later versions. **Workaround:** None.	WebUI	All platforms	AOS-W 8.5.0.0
AOS-196541	—	**Symptom:** API on an AOS-W Mobility Master does not operate over port 443. **Scenario:** This issue occurs when there is no rule for login or token generation over port 443. This issue is observed in Mobility Masters running AOS-W 8.5.0.4 or later versions. **Workaround:** Use port 4343 in the API URL to login, subsequently port 443 will work.	Web Server	All platforms	AOS-W 8.5.0.4
AOS-196593	—	**Symptom:** APs crash and reboot unexpectedly. The log file lists the reason for the event as **reboot caused by Kernel panic - not syncing: Fatal exception in interrupt PC is at 0x000C7461**. **Scenario:** This issue is observed in OAW-AP335 access points running AOS-W 8.3.0.8 or later versions.	Station Management	OAW-AP335 access points	AOS-W 8.3.0.8
AOS-196864	—	**Symptom:** Although a new VLAN ID is successfully connected, the managed device displays that the VLAN ID fails with a different ID. **Scenario:** This issue is observed when new VLANs are added and the total number of VLANs are 100/101, 200/201, 300/301 and likewise. This issue is observed in managed devices running AOS-W 8.5.0.3 or later versions. **Workaround:** None.	Cluster-Manager	All platforms	AOS-W 8.5.0.3
AOS-196878 AOS-197216	—	**Symptom:** The **Datapath** process crashes on a managed device. The log file lists the reason for the event as **wlan-n09-nc1.gw.illinois.edu.** **Scenario:** This issue is observed in managed devices running AOS-W 8.5.0.2 or later versions. **Workaround:** None.	DPI	All platforms	AOS-W 8.5.0.2

Table 7: *Known Issues in AOS-W 8.5.0.9*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-197023	—	**Symptom:** Mobility Master sends incorrect AP regulatory-domain-profile channel changes to the managed device during the initial configuration propagation. **Scenario:** This issue is observed in Mobility Masters running AOS-W 8.0.0.0 or later versions. **Workaround:** The following are recommended: ■ In the CLI, execute the **ap regulatory-domain-profile** command to create an AP regulatory-domain-profile without any channel configuration, save the changes and later add or delete channels as desired. ■ In the WebUI, create an AP regulatory-domain-profile with default channel selected, save the changes and later add or delete channels as desired in the **Configuration > AP Groups** page.	WebUI	All platforms	AOS-W 8.5.0.4
AOS-197048	—	**Symptom:** Some clients face degraded Wi-Fi download speed after the managed device resumes function post standby mode. **Scenario:** This issue occurs when the AP does not setup an aggregation session. This issue is observed in managed devices running AOS-W 8.3.0.8 or later versions. **Workaround:** None.	AP-Wireless	All platforms	AOS-W 8.3.0.8
AOS-197127	—	**Symptom:** A managed device crashes and reboots unexpectedly. The log file lists the reason for this event as **Datapath timeout (Fpapps Initiated) (Intent:cause:register 51:86:50:2).** **Scenario:** This issue is observed in OAW-4x50 Series switches running AOS-W 8.3.0.7 or later versions in a cluster setup. **Workaround:** None. **Duplicates:** AOS-197060, AOS-197130, AOS-197137, AOS-197161, AOS-197163, AOS-198720, AOS-201821	switch-Datapath	OAW-4x50 Series switches	AOS-W 8.3.0.7
AOS-197215	—	**Symptom:** Users are unable to delete the **Weekend** entry under **Start Day** of **Time range** field in the WebUI. **Scenario:** This issue occurs when the users create a new policy rule in the **Configuration > Roles & Policies > Policies > <policy_name> > <new_policy_rule>** page, and select **Access control** radio button in the **Rule type** field of the WebUI. This issue is observed in Mobility Masters running AOS-W 8.2.2.6 or later versions. **Workaround:** None.	Configuration	All platforms	AOS-W 8.2.2.6

Table 7: *Known Issues in AOS-W 8.5.0.9*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-197309	—	**Symptom:** Clients are unable to obtain the user role from ClearPass Policy Manager. **Scenario:** This issue is observed in managed devices running AOS-W 8.5.0.3 or later versions. **Workaround:** None.	RADIUS	All platforms	AOS-W 8.5.0.3
AOS-197565	—	**Symptom:** APs crash and reboot unexpectedly. The log file lists the reason for the event as **Dump capture kernel:AP rebooted caused by cold HW reset(power loss).** **Scenario:** This issue is observed in access points running AOS-W 8.5.0.0 or later versions. **Workaround:** None.	AP - Platform	All platforms	AOS-W 8.5.0.2
AOS-197912	—	**Symptom:** Multicast traffic is not forwarded to the clients when UAC and AAC are different. **Scenario:** This issue is observed in managed devices running AOS-W 8.3.0.7 or later versions. **Workaround:** None.	Station Management	All platforms	AOS-W 8.3.0.7
AOS-197945	—	**Symptom:** Access points crash and reboot unexpectedly. The log file lists the reason for the events as, **BadAddr:ffff00000010 PC:wlc_dump_ aggfifo+0x1160/0x12b0 [wl_v6] Warm-reset.** **Scenario:** This issue occurs due to memory corruption. This issue is observed in OAW-AP514 and OAW-AP515 access points running AOS-W 8.5.0.3 or later versions. **Workaround:** None.	AP - Wireless	OAW-AP514 and OAW-AP515 access points	AOS-W 8.5.0.3
AOS-198007	—	**Symptom:** Some APs are unable to ping managed devices and the APs keep switching between clusters. **Scenario:** This issue is observed in APs running AOS-W 8.3.0.8 or later versions. **Workaround:** None.	UCC	All platforms	AOS-W 8.3.0.8
AOS-198218	—	**Symptom:** After reboot, the status of the GRE tunnel of a standby switch is UP instead of DOWN in a VRRP instance and this results in network loop. **Scenario:** This issue is observed in managed devices running AOS-W 8.5.0.3 or later versions. **Workaround:** Re-enable the VRRP instance and the correct status of the GRE tunnel will be displayed.	GRE	All platforms	AOS-W 8.5.0.3

Table 7: *Known Issues in AOS-W 8.5.0.9*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-198266	—	**Symptom:** MAC authenticated clients are unable to reauthenticate even after enabling reauthentication. **Scenario:** This issue is observed in stand-alone switches running AOS-W 8.5.0.5 or later versions. **Workaround:** None.	Authentication	All platforms	AOS-W 8.5.0.5
AOS-198281	—	**Symptom:** The details of the **Up** time under **Managed network > Dashboard > Access Points > Access Points** table does not get updated correctly. **Scenario:** This issue is observed in Mobility Masters running AOS-W 8.2.2.6 or later versions. **Workaround:** None.	WebUI	All platforms	AOS-W 8.2.2.6
AOS-198475	—	**Symptom:** A user cannot upgrade a Mobility Master Virtual Appliance to AOS-W 8.5.0.0 or a later version. **Scenario:** This issue is observed in Mobility Master Virtual Appliances running AOS-W 8.5.0.0 or later versions. **Workaround:** None.	switch-Datapath	All platforms	AOS-W 8.5.0.5
AOS-198483	—	**Symptom:** WebUI does not have an option to map the **rf dot11-60GHz-radio-profile** to an AP group. **Scenario:** This issue is observed in Mobility Masters running AOS-W 8.5.0.4 or later versions. **Workaround:** None.	WebUI	All platforms	AOS-W 8.5.0.4
AOS-198488	—	**Symptom:** An AP reboots unexpectedly and sets an **F** flag. **Scenario:** This issue occurs when an 801.1X client is connected to the AP in bridge mode or tunnel mode for wired 802.1X authentication. This issue is observed in OAW-AP205H and OAW-AP303H access points running AOS-W 8.5.0.3 or later versions. **Workaround:** None.	AP-Platform	OAW-AP205H and OAW-AP303H access points	AOS-W 8.5.0.3

Table 7: *Known Issues in AOS-W 8.5.0.9*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-198511	—	**Symptom:** A few managed devices display an error, **Similar name certificate already exists on the same or different path. upload with a different name** when a new certificate is uploaded. **Scenario:** This issue occurs when the same new certificate is uploaded with its old name because the certificate manager receives the **crypto pki-import** command twice for a single certificate addition. This issue is observed in managed devices running AOS-W 8.4.0.5 or later versions. **Workaround:** None.	Certificate Manager	All platforms	AOS-W 8.4.0.5
AOS-198605	—	**Symptom:** A few APs fail to transition to a standby managed device during a datacenter failover. **Scenario:** This issue is observed in managed devices running AOS-W 8.3.0.10 or later versions. **Workaround:** None.	Cluster-Manager	All platforms	AOS-W 8.3.0.10
AOS-198787 AOS-198929	—	**Symptom:** A OAW-RAP does not come up on a managed device when Verizon U730L modem is used. **Scenario:** This issue is observed in managed devices running AOS-W 8.6.0.0 or later versions. **Workaround:** None.	OAW-RAP	All platforms	AOS-W 8.6.0.0
AOS-198822 AOS-203559 AOS-203959	—	**Symptom:** The **show iap table, show user-table internal** and **show global-user-table list** command do not display entries in the output. **Scenario:** This issue occurs after upgrading to AOS-W 8.4.0.4. This issue is observed in managed devices running AOS-W 8.4.0.4 or later versions. **Workaround:** None.	Web Server	All platforms	AOS-W 8.4.0.4
AOS-198834 AOS-200088 AOS-200555 AOS-201312	—	**Symptom:** A managed device crashes and reboots unexpectedly. The log file lists the reason for the event as **rebooted due to Soft Watchdog reset (Intent:cause:register de:86:70:4).** **Scenario:** This issue is observed in OAW-4750XM switches running AOS-W 8.3.0.10 or later versions. **Workaround:** None.	switch Platform	OAW-4750XM switches	AOS-W 8.3.0.10

Table 7: *Known Issues in AOS-W 8.5.0.9*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-198849 AOS-198850	—	**Symptom:** Users are unable to configure 2.4 GHz radio profile in the **Configuration > System > Profiles > 2.4 GHz radio profile** page and the WebUI displays the error message, **Feature is not enabled in the license.** **Scenario:** This issue is observed in stand-alone switches running AOS-W 8.5.0.3 or later versions. **Workaround:** None.	WebUI	All platforms	AOS-W 8.5.0.3
AOS-199012 AOS-198865	—	**Symptom:** A managed device crashes and reboots unexpectedly. The log file lists the reason for the event as **Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:4)**. **Scenario:** This issue is observed in managed devices running AOS-W 8.4.0.4 or later versions. **Workaround:** None.	switch-Datapath	All platforms	AOS-W 8.4.0.4
AOS-199306 AOS-201623	—	**Symptom:** APs crash and reboot unexpectedly. The log file lists the reason for the event as **Reboot caused by kernel panic: Fatal exception in interrupt [packet_lookup_frame+0x30/0x68].** **Scenario:** This issue is observed in APs running AOS-W 8.3.0.6 or later versions. **Workaround:** None.	AP-Wireless	All platforms	AOS-W 8.3.0.6
AOS-199420	—	**Symptom:** Clients roam between APs that are deployed in different clusters. **Scenario:** This issue is observed in access points running AOS-W 8.2.2.2 or later versions. **Workaround:** None.	ClientMatch	All platforms	AOS-W 8.2.2.2
AOS-199423	—	**Symptom:** Some L3 redundant Mobility Masters witness **profmgr** error logs. **Scenario:** This issue occurs when the Mobility Master is upgraded to a later version of AOS-W. This issue is observed in Mobility Masters running AOS-W 8.5.0.5-FIPS. **Workaround:** None.	Interface	All platforms	AOS-W 8.5.0.5

Table 7: *Known Issues in AOS-W 8.5.0.9*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-199539	—	**Symptom:** All the profiles listed under an AP group get marked as default except the VAP profile. **Scenario:** This issue is observed in managed devices running AOS-W 8.5.0.4 or later versions. **Workaround:** Run **ccm-debug full-config-sync** command on the effected managed device.	AP-Platform	All platforms	AOS-W 8.5.0.4
AOS-199663	—	**Symptom:** After reboot of mesh auto APs, the configuration changes and mesh auto setting were reset. The fix ensures that the APs work as expected. **Scenario:** This issue was observed in APs running AOS-W 8.5.0.4 or later versions.	Mesh	All platforms	AOS-W 8.5.0.5
AOS-199878 AOS-198897 AOS-200006 AOS-200080	—	**Symptom:** An AP crashes and reboots unexpectedly. The log file lists the reason for this event as **Reboot caused by kernel panic: CPU stall**. **Scenario:** This issue is observed in OAW-AP303H access points running AOS-W 8.5.0.4 or later versions. **Workaround:** None.	AP-Wireless	OAW-AP303H access points	AOS-W 8.5.0.4
AOS-199884	—	**Symptom:** Mobility Master logs the following error messages, **PAPI_Free: This buffer 0x4f6c48 may already be freed** and **PAPI_Free: Bad state index 0 state 0x1.** **Scenario:** This issue is observed in Mobility Masters running AOS-W 8.5.0.5 or later versions. **Workaround:** None.	VRRP	All platforms	AOS-W 8.5.0.5
AOS-199947	—	**Symptom:** The **Lic. FeatureBit** parameter under the License Client Table changes to enabled for Mobility Master Virtual Appliance and Mobility Controller Virtual Appliance. **Scenario:** This issue occurs when EVAL license is deleted and the licenses are displayed as 0. This issue is observed in stand-alone switches running AOS-W 8.3.0.11 or later versions. **Workaround:** None.	Licensing	All platforms	AOS-W 8.3.0.11

Table 7: *Known Issues in AOS-W 8.5.0.9*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-200071 AOS-201068	—	**Symptom:** Some clients are getting **U-APSD disabled in association** response though they are able to connect to an SSID without any issues. This issue does not allow the client to enter power saving mode and reduces the talk time from 12 hours to 3 hours. **Scenario:** This issue is observed in APs running AOS-W 8.3.0.0 or later versions. **Workaround:** Disable the 802.11r profile in the configurations using the **no dot11r** command.	Station Management	All platforms	AOS-W 8.6.0.2
AOS-200187	—	**Symptom:** Mobility Master is assigning duplicate IP addresses to Branch office switches from the VLAN pool. **Scenario:** This issue is observed in Mobility Masters running AOS-W 8.5.0.5 or later versions. **Workaround:** None.	BOC	All platforms	AOS-W 8.5.0.5
AOS-200275	—	**Symptom:** When the **interface gigabitethernet no description** command is executed, the GE0/0/0 value is sent by default. **Scenario:** This issue is observed in managed devices running AOS-W 8.2.2.6 or later versions. **Workaround:** None.	switch- Platform	All platforms	AOS-W 8.2.2.6
AOS-200446	—	**Symptom:** Some users are unable to change the Cluster Profile under **Configuration > Services > Cluster** tab of the WebUI. **Scenario:** This issue occurs when there is no VRRP ID configured but the Cluster Profile requests for a VRRP passphrase. This issue is observed in Mobility Masters running AOS-W 8.5.0.5 or later versions. **Workaround:** None.	WebUI	All platforms	AOS-W 8.5.0.5

Table 7: *Known Issues in AOS-W 8.5.0.9*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-200462	—	**Symptom:** A few managed devices do not respond to the SNMP queries from Airwave regarding rogue information. **Scenario:** This issue occurs when: ■ there is a mismatch in the message length between **WMS** process and **AM** process. ■ the managed device is running a higher version of AOS-W than that of the AP. This issue is observed in managed devices running AOS-W 8.3.0.8 or later versions. **Workaround:** None.	Air Management-IDS	All platforms	AOS-W 8.3.0.8
AOS-200534 AOS-203370	—	**Symptom:** The output of the **show ap active** command displays **SA (AAC=0.0.0.0)**. **Scenario:** This issue is observed in managed devices running AOS-W 8.5.0.7 or later versions. **Workaround:** None.	Mesh	All platforms	AOS-W 8.5.0.7
AOS-200566	—	**Symptom:** An AP crahses and reboots unexpectedly. The log file lists the reason for this event as **wlc_txq_enq_spq+0x3c/0x158 crash**. **Scenario:** This issue is observed in OAW-AP515 access points running AOS-W 8.5.0.2 or later versions. **Workaround:** None.	AP-Wireless	OAW-AP515 access points	AOS-W 8.5.0.2
AOS-200699 AOS-200760	—	**Symptom:** Some users are unable to delete the configured SNMP V3 trap hosts. **Scenario:** This issue occurs when the IPv4 and IPv6 address type flags are missing. This issue is observed in managed devices running AOS-W 8.5.0.0 or later versions. **Workaround:** None.	SNMP	All platforms	AOS-W 8.5.0.0
AOS-200733	—	**Symptom:** APs crash and reboot unexpectedly. The log file list the reason for the event as **kernel page fault at virtual address 00005654, epc == c0bd7dd4, ra == c0bf95f8.** **Scenario:** This issue is observed in APs running AOS-W 8.5.0.3 or later versions. **Workaround:** None.	AP-Wireless	All platforms	AOS-W 8.5.0.3

Table 7: *Known Issues in AOS-W 8.5.0.9*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-200765	—	**Symptom:** Managed devices log the error message, **<199804> <4844> |authmgr| |cluster| gsm_auth.c, auth_gsm_publish_ip_user_local_section:1011: auth_gsm_publish_ip_user_local_section: ip_user_local_flags.** **Scenario:** This issue is observed in managed devices running AOS-W 8.3.0.7 or later versions in a cluster setup. **Workaround:** None.	Cluster-Manager	All platforms	AOS-W 8.3.0.7
AOS-201042	—	**Symptom:** A large number of packet drops are observed in a few APs. **Scenario:** This issue occurs when the AP SAP MTU datapath tunnel is set to 1514. This issue is observed in APs running AOS-W 8.3.0.6 or later versions. **Workaround:** None.	AP Datapath	All platforms	AOS-W 8.3.0.6
AOS-201150 AOS-201997 AOS-204328	—	**Symptom:** A few APs crash and reboot unexpectedly. The log file lists the reason for the event as **AP Reboot reason: External-WDT-reset.** **Scenario:** This issue is observed in OAW-AP510 Series access points running AOS-W 8.6.0.2 or later versions. **Workaround:** None.	AP-Platform	OAW-AP510 Series access points	AOS-W 8.6.0.2
AOS-201152	—	**Symptom:** APs crash and reboot unexpectedly. The log files list the reason for the event as **AP Reboot reason: BUGSoftLockup:CPU#1 stuck for 22s! [kworker/1:2:2288] PC:_udelay+0x30/0x48 Warm-reset.** **Scenario:** This issue is observed in OAW-AP515 access points running AOS-W 8.5.0.6 or later versions. **Workaround:** None.	AP-Wireless	OAW-AP515 access points	AOS-W 8.5.0.6
AOS-201200	—	**Symptom:** The **show license-pool-profile** command does not display the output when executed in the **/mm/my node** hierarchy. **Scenario:** This issue is observed in Mobility Masters running AOS-W 8.3.0.6 or later versions. **Workaround:** None.	Configuration	All platforms	AOS-W 8.5.0.5

Table 7: *Known Issues in AOS-W 8.5.0.9*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-201210	—	**Symptom:** When the **show aaa authentication-server radius statistics** command is executed, few RADIUS authentication servers always display the **expAuthTm** value as 0. **Scenario:** This issue is observed when the managed devices are upgraded to AOS-W 8.5.0.5 or later versions. **Workaround:** None.	RADIUS	All platforms	AOS-W 8.5.0.5
AOS-201250	—	**Symptom:** Some managed devices crash and reboot unexpectedly. The log file lists the reason for the event as **Nanny rebooted machine - low on free memory.** **Scenario:** This issue is not limited to any switch platform or AOS-W release version. **Workaround:** None.	Base OS Security	All platforms	AOS-W 8.5.0.5
AOS-201273 AOS-201395	—	**Symptom:** The **show switches** command does not display the IP address of the managed device and tunnel is not created between the Mobility Master and managed device. **Scenario:** This issue occurs when **masterip** is changed using the **masteripv6** command. This issue is observed in Mobility Masters running AOS-W 8.5.0.6 or later versions. **Workaround:** None.	Configuration	All platforms	AOS-W 8.5.0.6
AOS-201329	—	**Symptom:** CPsec toggling stops working after upgrading to AOS-W 8.5.0.8. **Scenario:** This issue occurs when CPsec is disabled at multiple node levels and re-enabled only at the higher node level. This results in an override of CPsec configurations at the lower node levels. This issue is observed in managed devices running AOS-W 8.0.0.0 or later versions. **Workaround:** Verify that there are no overridden CPsec configurations at lower node levels before the upgrade.	Configuration	All platforms	AOS-W 8.3.0.10
AOS-201439 AOS-201448	—	**Symptom:** APs crash and reboot unexpectedly. The log file lists the reason for the event as **PC is at skb_panic+0x5c/0x68**. **Scenario:** This issue is observed in OAW-AP303H access points running AOS-W 8.5.0.5 or later versions. **Workaround:** None.	AP-Wireless	OAW-AP303H access points	AOS-W 8.5.0.5

Table 7: *Known Issues in AOS-W 8.5.0.9*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-201612	—	**Symptom:** Role policies configured on a Mobility Master are displayed in a different order on the managed devices in the **Configuration > Roles & Policies > Roles** tab. **Scenario:** This issue occurrs when the default ACLs get deleted during the initial configuration synchronization after upgrade. This issue is observed in Mobility Masters running AOS-W 8.0.0.0 or later versions. **Workaround:** None.	Configuration	All platforms	AOS-W 8.3.0.8
AOS-202110	—	**Symptom:** The **Active Controller** field displays a hyphen (-) for some APs under **Dashboard > Infrastructure > Access Devices** page in the WebUI. **Scenario:** This issue is observed in Mobility Masters running AOS-W 8.2.0.0 or later versions. **Workaround:** None.	Monitoring	All platforms	AOS-W 8.5.0.6
AOS-202129 AOS-204127	—	**Symptom:** The **Configuration > AP groups** page does not have the **Split radio** toggle to enable the tri-radio feature. **Scenario:** This issue is observed in stand-alone switches running AOS-W 8.6.0.0 or later versions. **Workaround:** None.	WebUI	All platforms	AOS-W 8.6.0.0
AOS-202195	—	**Symptom:** A managed device crashes and reboots unexpectedly. The log file lists the reason for the event as **Nanny rebooted machine - isakmpd process died (Intent:cause:register 34:86:50:2).** **Scenario:** This issue is observed in managed devices running AOS-W 8.3.0.6 or later versions. **Workaround:** None.	IPsec	All platforms	AOS-W 8.3.0.6
AOS-202290	—	**Symptom:** The error message, **Cannot modify existing server-group from different node in config path** is displayed when users try to create or modify aaa server group. **Scenario:** This issue occurs when similar naming conventions are used for different folders under the same hierarchy. This issue is observed in Mobility Masters running AOS-W 8.5.0.6 or later versions. **Workaround:** None.	Configuration	All platforms	AOS-W 8.5.0.6

Table 7: *Known Issues in AOS-W 8.5.0.9*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-202341	—	**Symptom:** A managed device crashes and reboots unexpectedly. The log file lists the reason for the event as **Datapath timeout (SOS Assert) ((Intent:cause:register 54:86:0:2c).** **Scenario:** This issue is observed in managed devices running AOS-W 8.3.0.8 or later versions. **Workaround:** None.	switch-Datapath	All platforms	AOS-W 8.3.0.8
AOS-202370	—	**Symptom:** Some managed devices reset when the **activate sync** command is issued. **Scenario:** This issue occurs when the node paths that are configured for Activate and Mobility Master use different cases. This issue is observed in Mobility Masters running AOS-W 8.5.0.5 or later versions. **Workaround:** None.	Configuration	All platforms	AOS-W 8.5.0.5
AOS-202450	—	**Symptom:** OAW-RAPs reboot unexpectedly. **Scenario:** This issue occurs when Mobility Master modifies the existing whitelist database entries when the **activate whitelist download** command is executed. This issue is observed in OAW-RAPs running AOS-W 8.5.0.7 or later versions. **Workaround:** None.	Base OS Security	All platforms	AOS-W 8.5.0.7
AOS-202515 AOS-202658	—	**Symptom:** APs crash and reboot unexpectedly. The log file lists the reason for the event as **Panic:assert Warm-reset**. **Scenario:** This issue is observed in APs running AOS-W 8.5.0.2 or later versions. **Workaround:** None.	AP Datapath	All platforms	AOS-W 8.5.0.2
AOS-202551	—	**Symptom:** An AP logs the error message, **An internal system error has occurred at file parser.c function parse_mgmt line 656 error parse_mgmt Size mismatch on frame.** **Scenario:** This issue is observed in OAW-AP535 access points running AOS-W 8.5.0.7 or later versions. **Workaround:** None.	AP-Wireless	OAW-AP535 access points	AOS-W 8.5.0.7

Table 7: *Known Issues in AOS-W 8.5.0.9*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-202691	—	**Symptom:** The **Key Management** column in the **Configuration > WLANs** page of the WebUI displays multiple **wpa2-psk-tkip** entries. **Scenario:** This issue occurs when multiple wpa2-psk-tkip opmode SSIDs are created. This issue is observed in stand-alone switches running AOS-W 8.5.0.4 or later versions. **Workaround:** None.	WebUI	All platforms	AOS-W 8.5.0.4
AOS-202739	—	**Symptom:** APs generate the error message, **WPA Passphrase not configured for AP**. **Scenario:** This issue is observed in APs running AOS-W 8.3.0.9 or later versions. **Workaround:** None.	Base OS Security	All platforms	AOS-W 8.3.0.9
AOS-202803	—	**Symptom:** The error message, **cluster was fractured during the upgrade** is displayed during the cluster live upgrade process and therefore cluster live upgrade cannot be performed. **Scenario:** This issue is observed in Mobility Masters running AOS-W 8.5.07 or later versions. **Workaround:** None.	Cluster-Manager	All platforms	AOS-W 8.5.07
AOS-203097	—	**Symptom:** WebUI prompts that additional VLANs will be deleted when user tries to delete a VLAN. **Scenario:** This issue occurs in stand-alone switch running AOS-W 8.3.0.10 or later versions. **Workaround:** None.	WebUI	All platforms	AOS-W 8.3.0.10
AOS-203170	—	**Symptom:** Class attribute field is missing in accounting packets of the VIA connection profile. **Scenario:** This issue occurs when IKEv2 is enabled in VIA connection profile. This issue is observed in managed devices running AOS-W 8.4.0.1 or later versions. **Workaround:** None.	IPsec	All platforms	AOS-W 8.6.0.2

Table 7: *Known Issues in AOS-W 8.5.0.9*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-203201	—	**Symptom:** The managed device is unable to download configurations from the Mobility Master using VPNC. **Scenario:** This issue is observed in managed devices running AOS-W 8.2.2.6 or later versions. **Workaround:** None.	Configuration	All platforms	AOS-W 8.2.2.6
AOS-203698	—	**Symptom:** A mismatch is observed in the ACL positions between the Mobility Master and the managed devices. **Scenario:** This issue occurs when the ACLs of the user-role are changed. This issue is observed in Mobility Masters and managed devices running AOS-W 8.5.0.6 or later versions. **Workaround:** None.	Base OS Security	All platforms	AOS-W 8.5.0.6
AOS-203712	—	**Symptom:** Avaya Spectalink wireless phones reboot unexpectedly with the error message, **No AVPP response from 192.168.249.001.** **Scenario:** This issue occurs because of the IP packet size. This issue is observed in managed devices running AOS-W 8.5.0.7 or later versions. **Workaround:** None.	Base OS Security	All platforms	AOS-W 8.5.0.7
AOS-203859	—	**Symptom:** Windows clients are unable to get WINS server information from the Mobility Master. **Scenario:** This issue is observed in Mobility Masters running AOS-W 8.3.0.11 or later versions. **Workaround:** None.	IPsec	All platforms	AOS-W 8.3.0.11
AOS-204367	—	**Symptom:** Map name is not displayed in the output of the **show crypto ipsec sa** command. **Scenario:** This issue is observed in managed devices running AOS-W 8.5.0.8 or later versions. **Workaround:** None.	IPsec	All platforms	AOS-W 8.5.0.8
AOS-204390	—	**Symptom:** Radius source interface is not working on a managed device. **Scenario:** This issue occurs when Radsec is enabled. This issue is observed in managed devices running AOS-W 8.5.0.8 or later versions. **Workaround:** None.	Base OS Security	All platforms	AOS-W 8.5.0.8

Chapter 7 Upgrade Procedure

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

CAUTION

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

Topics in this chapter include:

Important Points to Remember and Best Practices

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** section of 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 the 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 *Alcatel-Lucent Mobility Master Licensing Guide*.

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 the best practices for memory requirement:

- 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 files, 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 47 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 47 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 file:** 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 47 to copy the **logs.tar** files to an external server. Execute the **tar clean logs** command to delete the file from the managed device.

CAUTION

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 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.

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
- Logs
- Flashbackup

Backing up and Restoring Flash Memory

You can backup and restore flash using the WebUI or the 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 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 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 backup flash file from the external server or storage device to the compact flash file system 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 compact flash file system.

```
(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 Master or managed device. For details, see Memory Requirements on page 46.

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 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 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 new software 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 Master or managed device will not load a corrupted AOS-W image.

4. Log in to the AOS-W 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 **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 Master 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 AOS-W 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 AOS-W 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 AOS-W 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 AOS-W 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 if 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 Memory Requirements on page 46 for information on creating a backup.

In the CLI

Execute the **show version** command to verify the AOS-W image version. The following steps describe how to verify that the Mobility Master 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 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 47 for information on creating a backup.

Downgrading AOS-W

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

Pre-requisites

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

1. Back up your Mobility Master or managed device. For details, see Backing up Critical Data on page 47.
2. Verify that the control plane security is disabled.
3. Set the Mobility Master or managed device to boot with the previously saved AOS-W configuration file.
4. Set the Mobility Master or managed device to boot from the system 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 Master 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 pre-upgrade flash backup from the file stored on the Mobility Master or managed device. Do not restore the AOS-W 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 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 Master or managed device by navigating to the **Diagnostics > Technical Support > Copy Files** page.
   a. From the **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 the **Select destination file** drop-down list, 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:

CAUTION

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** 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 AOS-W version by navigating to the **Maintenance > Software Management > About** page.

In the CLI

The following section describes how to downgrade the AOS-W 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 switch:

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

   or

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

2. Set the switch 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. 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 AOS-W 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 any recent network 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 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.