AOS-W 8.5.0.5

Alcatel·Lucent
Enterprise

Release Notes

Copyright Information

Alcatel-Lucent and the Alcatel-Lucent Enterprise logo are trademarks of Alcatel-Lucent. To view other trademarks used by affiliated companies of ALE Holding, visit:

https://www.al-enterprise.com/en/legal/trademarks-copyright

All other trademarks are the property of their respective owners. The information presented is subject to change without notice. Neither ALE Holding nor any of its affiliates assumes any responsibility for inaccuracies contained herein. (2019)

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.

Chapter 1
Release Overview

This AOS-W release notes includes the following topics:

NOTE

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

- New Features and Enhancements on page 9
- Supported Platforms on page 10
- Regulatory Updates on page 13
- Resolved Issues on page 14
- Known Issues and Limitations on page 31
- Upgrade Procedure on page 45

For the list of terms, refer Glossary.

Important Points Before Upgrading to AOS-W 8.5.0.0

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 Migration 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	
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

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

Default Value of host-ageout-time Parameter

The default value of the Openflow switch's **host-ageout-time** parameter is changed from 300 seconds to 3600 seconds.

Execute the following command to view the value of the **ofc host-ageout-time** parameter:

```
(host) [mynode] #show openflow-controller

Openflow-controller
-------------------
Parameter                    Value
---------                    -----
ofc state                    Enabled
ofc host-ageout-time         3600 sec
ofc mode                     passive
ofc certificate-file         none
ofc key-file                 none
ofc ca-certificate-file      none
ofc tls                      Disabled
ofc port                     6633
ofc topology-discovery       Disabled
ofc auxiliary-channel-port   6633
```

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 8.5.0.5*

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 8.5.0.5*

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
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 8.5.0.5*

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
OAW-AP310 Series	OAW-AP314, OAW-AP315
OAW-AP318 Series	OAW-AP210AP-318
OAW-AP320 Series	OAW-APAP-324, OAW-AP325

Table 5: *Supported AP Platforms in AOS-W 8.5.0.5*

AP Family	AP Model
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_73310

Resolved Issues

This chapter describes the issues resolved 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.

Table 6: *Resolved Issues in AOS-W 8.5.0.5*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-125897 AOS-187598 AOS-189036 AOS-192082 AOS-192723 AOS-192731 AOS-192734 AOS-195746	151952	**Symptom:** When a managed device rebooted, APs and clients rebooted without IP addresses and other fields. The fix ensures that no fields are missing when clients come up after a reboot. **Scenario:** This issue was observed in managed devices running AOS-W 8.0.1.0 or later versions.	Monitoring	All platforms	AOS-W 8.0.1.0
AOS-144684 AOS-184346	176339	**Symptom:** Log files of few managed devices contained incorrect or garbled ESSID and BSSID values. The fix ensures that these incorrect messages are not generated. **Scenario:** This issue was observed in managed devices running AOS-W 8.2.1.0 or later versions.	Station Management	All platforms	AOS-W 8.2.1.0
AOS-146598 AOS-188589 AOS-192366 AOS-193748	178949	**Symptom:** The **Upload Sync Manager** process stopped responding in a Mobility Master. The log files listed the reason for the event as **PROCESS_ NOT_RESPONDING_CRITICAL**. The fix ensures that the Mobility Master works as expected. **Scenario:** This issue was observed in Mobility Masters running AOS-W 8.2.2.0 or later versions.	Captive Portal	All platforms	AOS-W 8.3.0.0

Table 6: *Resolved Issues in AOS-W 8.5.0.5*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-148529 AOS-191978	181872	**Symptom:** A few clients were unable to access Internet because the client traffic received incorrect Source NAT information. The fix ensures that the clients are able to access Internet seamlessly. **Scenario:** This issue occurred when IP NAT Inside feature was enabled on an Interface VLAN which was configured with PBR. This issue was observed in managed devices running AOS-W 8.0.0.0 or later versions in a Mobility Master-Managed Device topology.	switch-Datapath	All platforms	AOS-W 8.4.0.4
AOS-151541 AOS-185425	185851	**Symptom:** A few users were unable to access CLI by using SSH. The fix ensures that the SSH login session becomes inactive on the managed device and the users are able to access CLI by using SSH. **Scenario:** This issue occurred because the idle SSH login session to a managed device did not time out. This issue was observed in managed devices running AOS-W 8.2.0.0 or later versions.	Base OS Security	All platforms	AOS-W 8.2.1.1
AOS-152326 AOS-187297 AOS-187406 AOS-187549	186957	**Symptom:** The beacon displayed the country code information intermittently for 5 GHz non-DFS channel. The fix ensures to broadcast a country code after checking the status of the 802.11h Virtual AP to determine if the country code needs to be broadcast. **Scenario:** This issue occurred when 802.11h was enabled in the radio profile. This issue was observed in OAW-AP510 Series access points running AOS-W 8.3.0.0 or later versions.	AP-Wireless	OAW-AP510 Series access points	AOS-W 8.4.0.2
AOS-155632	191489	**Symptom:** A stand-alone switch crashed and rebooted unexpectedly. The log file listed the reason for this event as **Control Processor Kernel Panic**. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue occurred when IP options caused the **Datapath** process to crash. This issue was observed in OAW-4x50 Series switches running AOS-W 8.3.0.0 or later versions. **New Duplicates:** AOS-157337, AOS-157417, AOS-158610, AOS-158360, AOS-184786, AOS-186151, AOS-187156, AOS-187576, AOS-187752, AOS-187880, AOS-189198, AOS-189439, AOS-191458, AOS-191603, AOS-192748, AOS-193261, AOS-193272, AOS-193491, AOS-193997, AOS-194310, AOS-194588, AOS-194797, AOS-194817, AOS-196391 **Old Duplicates:** 193793, 193945, 195329, 195645	switch-Platform	OAW-4x50 Series switches	AOS-W 8.3.0.0

Table 6: *Resolved Issues in AOS-W 8.5.0.5*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-157008	193358	**Symptom:** The output of the **show ap bss table** command displayed incorrect MTU value for a OAW-RAP as the AP MTU report packet was single encrypted. The fix ensures that the MTU report packet is not dropped by the managed device and the output of the **show ap bss table** command displays the correct MTU value. **Scenario:** This issue occurred when the default value of the **rap-gre-mtu** parameter was changed to a new value using the **ap system-profile <profile_name>** command. This issue was observed in APs running AOS-W 8.2.0.0 or later versions.	AP-Platform	All platforms	AOS-W 8.3.0.0
AOS-157011 AOS-191292	193362	**Symptom:** The output of **show datapath papi counters** command displayed invalid tunnel endpoint information. The fix ensures that the **show datapath papi counters** command displays the correct information. **Scenario:** This issue was observed in Mobility Masters running AOS-W 8.2.2.0 or later versions.	switch-Datapath	All platforms	AOS-W 8.3.0.3
AOS-157544 AOS-191997 AOS-192527	194144	**Symptom:** Licenses were missing after the managed device was rebooted. The fix ensures that the licenses are not lost when a managed device is rebooted. **Scenario:** This issue occurred because of database corruption, which was caused by power outages. This issue was observed in managed devices running AOS-W 8.3.0.7 or later versions.	Database	All platforms	AOS-W 8.3.0.7
AOS-182008 AOS-192128 AOS-192459 AOS-192919 AOS-194219 AOS-196128 AOS-196849 AOS-196938	—	**Symptom:** A Mobility Master crashed and rebooted unexpectedly. The log file listed the reason for the event as **Reboot Cause: Kernel Panic (Intent:cause: 86:50)**. The fix ensures that the Mobility Master works as expected. **Scenario:** This issue was observed in Mobility Masters running AOS-W 8.4.0.0 or later versions.	switch-Platform	All platforms	AOS-W 8.5.0.5
AOS-183226 AOS-197435	—	**Symptom:** A few clients lost L3 connectivity though L2 connectivity was up. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue occurred when the client entered power saving mode and the AP queued packets. This issue was observed in OAW-AP200 Series access points running AOS-W 8.5.0.2 or later versions.	AP-Wireless	OAW-AP200 Series access points	AOS-W 8.5.0.2

Table 6: *Resolved Issues in AOS-W 8.5.0.5*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-183468 AOS-183550 AOS-183551 AOS-184610 AOS-186877 AOS-186916 AOS-194037 AOS-195185 AOS-196543	—	**Symptom:** A few managed devices crashed and rebooted unexpectedly. The log file listed the reason for the event as **datapath timeout (Fpapps Initiated) (Intent:cause:register 51:86:50:2).** This issue is resolved by ensuring that the unnecessary ARP traffic is not sent from a managed device to a Mobility Master. **Scenario:** This issue occurred because OpenFlow from the managed device sent all ARP packets to the Mobility Master. This issue was observed in Mobility Masters running AOS-W 8.2.2.0 or later versions.	switch-Datapath	All platforms	AOS-W 8.3.0.4
AOS-183883 AOS-183989 AOS-193747	—	**Symptom:** A few APs were marked as **Down** and were inactive. The fix ensures that the managed devices accept the messages from the APs and the APs are able to connect to the managed devices seamlessly. **Scenario:** This issue occurred because the managed devices dropped AP-READY message from the APs. This issue was observed in managed devices running AOS-W 8.3.0.0 or later versions.	switch-Datapath	All platforms	AOS-W 8.3.0.0
AOS-184474	—	**Symptom:** An AP crashed and rebooted unexpectedly. The log file listed the reason for this event as **kernel panic: Rebooting the AP because of FW ASSERT**. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue was observed in OAW-AP300 Series access points running AOS-W 8.2.2.0 or later versions. **Duplicates:** AOS-186793, AOS-186872, AOS-186971, AOS-189390, AOS-190362, AOS-192337, AOS-194239, AOS-194677, AOS-195037, AOS-195056, AOS-196028, AOS-196378, AOS-196861	AP-Wireless	OAW-AP300 Series access points	AOS-W 8.3.0.6
AOS-185103	—	**Symptom:** The **Outstanding Requests** parameter value was incremented unexpectedly in the output of the **show aaa authentication-server radius statistics** command in a managed device. The fix ensures that the managed device works as expected. **Scenario:** This issue was observed in managed devices running AOS-W 8.5.0.0 or later versions with EAP fragmentation enabled.	802.1x	All platforms	AOS-W 8.5.0.1

Table 6: *Resolved Issues in AOS-W 8.5.0.5*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-185696	—	**Symptom:** A few APs stopped responding to data frames and could not decode BA packets from the STAs, leading to packet drop. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue was observed in OAW-AP530 Series access points running AOS-W 8.5.0.0 or later versions.	AP-Wireless	OAW-AP530 Series access points	AOS-W 8.5.0.0
AOS-185812	—	**Symptom:** User traffic in tunneled node dropped when webcc was enabled. The fix ensures that the user traffic is not dropped. **Scenario:** This issue was observed in Mobility Masters running AOS-W 8.3.0.0 or later versions.	WebCC	All platforms	AOS-W 8.3.0.0
AOS-185920 AOS-185921	—	**Symptom:** A managed device rebooted unexpectedly. The log file listed the reason for this event as **Nanny Rebooted Machine – fpapps process died and crashed on pubsub, cfgm, syslogdwrap, aaa and nanny module**. The fix ensures that the managed device works as expected. **Scenario:** This issue occurred due to a memory leak. This issue was observed in managed devices running AOS-W 8.3.0.0 or later versions.	IPsec	All platforms	AOS-W 8.3.0.0
AOS-185977 AOS-190735	—	**Symptom:** Heartbeats were missed randomly on a managed device in a cluster setup. The fix ensures that the managed device works as expected. **Scenario:** This issue was observed in managed devices running AOS-W 8.3.0.7 or later versions.	switch-Datapath	All platforms	AOS-W 8.3.0.7
AOS-186179 AOS-194133	—	**Symptom:** A user was unable to add a custom site-to-site IPsec map to the nexthop list. The fix ensures that the user is able to add a custom site-to-site IPsec map to the nexthop list. **Scenario:** This issue was observed in managed devices running AOS-W 8.5.0.0.	switch-Datapath	All platforms	AOS-W 8.5.0.0
AOS-186303 AOS-187388 AOS-188301	—	**Symptom:** A few OAW-RAPs rebooted unexpectedly. The log file listed the reason for this event as **kernel panic: Fatal exception on PC is at netdev_run_todo+0x290/0x2b4**. The fix ensures that OAW-RAPs work as expected. **Scenario:** This issue was observed in OAW-AP305 access points running AOS-W 8.4.0.2 or later versions.	OAW-RAP	OAW-AP305 access points	AOS-W 8.4.0.2

Table 6: *Resolved Issues in AOS-W 8.5.0.5*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-186379	—	**Symptom:** IPv4 session table output was missing in tech support logs. The fix ensures that the IPv4 session table outputs are available in the tech support log. **Scenario:** This issue as observed in Mobility Masters running AOS-W 8.3.0.0 or later versions.	switch-Datapath	All platforms	AOS-W 8.3.0.0
AOS-186400 AOS-192691 AOS-194190 AOS-194399	—	**Symptom:** An SNMP walk failed on MIB objects. The fix ensures that the SNMP walk works as expected. **Scenario:** This issue was observed in Mobility Masters running AOS-W 8.5.0.0 or later versions.	SNMP	All platforms	AOS-W 8.5.0.0
AOS-186446	—	**Symptom:** RADIUS load balancing stopped responding because all the authentication requests were sent to only one RADIUS server. The fix ensures that load balancing between the two RADIUS authentication servers works as expected. **Scenario:** This issue was observed in stand-alone switches running AOS-W 8.2.0.0 or later versions.	RADIUS	All platforms	AOS-W 8.2.1.1
AOS-186558	—	**Symptom:** A few clients were unable to connect after reboot of a managed device. The fix ensures that the clients are able to connect to the managed device. **Scenario:** This issue occurred because the GRE tunnel was not established after the managed device was rebooted. This issue was observed in managed devices running AOS-W 8.2.0.0 or later versions.	switch-Datapath	All platforms	AOS-W 8.2.0.0
AOS-186735 AOS-194568	—	**Symptom:** An AP crashed and rebooted unexpectedly. The log file listed the reason for the event as **kernel panic: Rebooting the AP. NSS FW crashed**. The fix ensures that the AP works as expected. **Scenario:** This issue was observed in OAW-AP320 Series access points running AOS-W 8.3.0.0 or later versions.	AP Datapath	OAW-AP320 Series access points	AOS-W 8.5.0.5

Table 6: *Resolved Issues in AOS-W 8.5.0.5*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-187114	—	**Symptom:** The **Pending Changes** page displayed additional changes when the user configured a new policy rule under **Configuration > Roles & Policies > Policies** page in the WebUI. The fix ensures that unnecessary changes are not displayed in the **Pending Changes** page in the WebUI. **Scenario:** This issue was observed when the user configured a new rule for an existing policy under the **Policies** page and clicked the **Submit** button. This issue was observed in Mobility Masters running AOS-W 8.3.0.4.	WebUI	All platforms	AOS-W 8.3.0.4
AOS-187510	—	**Symptom:** A managed device crashed and rebooted unexpectedly. The fix ensures that the managed device works as expected. **Scenario:** This issue occured because the 802.1X processes crashed after a cluster live upgrade on the managed device. This issue was observed in managed devices running AOS-W 8.4.0.2 or later versions.	802.1X	All platforms	AOS-W 8.4.0.2
AOS-187726	—	**Symptom:** The output of the **show ap debug radio-stats** command displayed incorrect value for the Rx frames counter. The fix ensures that the correct number of Rx frames are displayed in the command output. **Scenario:** This issue was observed in OAW-AP325 access points running AOS-W 8.4.0.0 or later versions.	AP-Wireless	OAW-AP325 access points	AOS-W 8.4.0.0
AOS-187961	—	**Symptom:** AirGroup profile was not forwarded from master switch to standby switch during a failover. The fix ensures that the AirGroup configurations are synchronized between master switches and standby switches. **Scenario:** This issue was observed in OAW-4550 switches running AOS-W 8.2.0.0 or later versions.	AirGroup	OAW-4550 switches	AOS-W 8.2.2.5
AOS-188429	—	**Symptom:** A client was unable to login to the managed device after upgrading the AOS-W version to AOS-W 8.5.0.0. The fix ensures that the managed devices work as expected. **Scenario:** This issue was observed in managed devices running AOS-W 8.5.0.0 or later versions.	Base OS Security	All platforms	AOS-W 8.5.0.0

Table 6: *Resolved Issues in AOS-W 8.5.0.5*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-188470	—	**Symptom:** PPPoE did not work when a OAW-RAP was provisioned using ZTP and the **Either ping is disabled on AP's uplink router or there are issues with AP's uplink connectivity** error was displayed. The fix ensures that if the AP is a PPPoE AP, the AP does not reboot after checking for the IP address in the PPPoE server. **Scenario:** This issue was observed in OAW-AP203R access points running AOS-W 8.2.1.1 or later versions.	OAW-RAP	OAW-AP203R access points	AOS-W 8.2.1.1
AOS-188664 AOS-194339	—	**Symptom:** The output of the **show airmatch debug static-radios** command did not display AP related information. This issue is resolved by issuing the **show airmatch debug reporting-radio mac <MAC address>** command. **Scenario:** This issue was observed in Mobility Master Virtual Appliances running AOS-W 8.5.0.0.	AirMatch	All platforms	AOS-W 8.5.0.0
AOS-188943	—	**Symptom:** A user could not set the **denyall** role as the initial-role in a AAA profile. This issue is resolved by adding the **denyall** role as a system defined role irrespective of the PEFNG license bit value. **Scenario:** This issue occurred when the PEFNG license was disabled on a Mobility Master and the **denyall** role was not added in the system to be used by the user in AAA profile. This issue was observed in Mobility Masters running AOS-W 8.4.0.0 or later versions.	Role	All platforms	AOS-W 8.4.0.3
AOS-189152 AOS-191781	—	**Symptom:** A few APs appeared with standby tunnels on the switch though redundancy was disabled in the **lc-cluster profile**. As a result, the **show lc-cluster load distribution ap** command returned incorrect AP count. The fix ensures that APs do not get a standby switch assigned when redundancy is disabled. **Scenario:** This issue was observed in APs running AOS-W 8.2.0.0 or later versions.	Cluster-Manager	All platforms	AOS-W 8.4.0.4
AOS-189420	—	**Symptom:** A few clients declined the IP addresses and were unable to connect to the managed device. The fix ensures that the clients are able to connect to the managed device. **Scenario:** This issue occurred because the managed device sent an ARP request to the client's MAC address. This issue was observed in managed devices running AOS-W 8.3.0.0 or later versions.	SDN	All platforms	AOS-W 8.3.0.0

Table 6: *Resolved Issues in AOS-W 8.5.0.5*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-189450 AOS-192973	—	**Symptom:** An AP crashed and rebooted unexpectedly. The log file listed the reason for this event as **kernel panic - not syncing: subsys-restart: Resetting the SoC - q6v5-wcss crashed**. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue was observed in OAW-AP530 Series access points running AOS-W 8.5.0.0 or later versions.	AP-Wireless	OAW-AP530 Series access points	AOS-W 8.5.0.1
AOS-189471	—	**Symptom:** A few clients were unable to connect to APs that are configured with LACP and have allowed band of 5 GHz. The fix ensures that clients connect to the APs seamlessly. **Scenario:** This issue was observed in OAW-AP335 access points running AOS-W 8.5.0.0.	AP Datapath	OAW-AP335 access points	AOS-W 8.5.0.0
AOS-189721 AOS-197167	—	**Symptom:** The **Datapath** process crashed in a stand-alone switch. The log files listed the reason for the event as **Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:4)**. The fix ensures that the switch works as expected. **Scenario:** This issue was observed in OAW-4550 switches running AOS-W 8.4.0.2 or later versions.	switch-Datapath	OAW-4550 switches	AOS-W 8.4.0.2
AOS-189757	—	**Symptom:** The captive portal redirection did not work when the client's **http GET** packet contained files with .png or .gif format. The fix ensures that files with .png or .gif format are not included. **Scenario:** This issue was observed in managed devices running AOS-W 8.3.0.0 or later versions.	Captive Portal	All platforms	AOS-W 8.4.0.2
AOS-189768	—	**Symptom:** A few clients were unable to receive Route Advertisements from routers, which led to connectivity issues. The fix ensures that the clients are able to receive Route Advertisements. **Scenario:** This issue occurred when the user migrated the managed devices from AOS-W 6.x version to AOS-W 8.x version. This issue was observed in IPv6 clients connected to managed devices running AOS-W 8.2.1.0 or later versions.	switch-Datapath	All platforms	AOS-W 8.2.1.0
AOS-190057 AOS-192234	—	**Symptom:** An AP used the wrong PoE status. Enhancement to the wireless driver resolved this issue. **Scenario:** This issue occurred when the external switch granted greater power to the AP via LLDP negotiation, and the AP detected the power as invalid. This issue was observed in OAW-AP510 Series access points running AOS-W 8.5.0.0 or later versions.	AP-Platform	OAW-AP510 Series access points	AOS-W 8.5.0.0

Table 6: *Resolved Issues in AOS-W 8.5.0.5*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-190154 AOS-190628 AOS-192465 AOS-195358	—	**Symptom:** The status of an AP was displayed as **DOWN** in the Access Points table under **Dashboard > Infrastructure > Access Devices** page in the WebUI, but the status of the AP was displayed as **UP** when the **show ap database long** command was executed. The fix ensures that the AP count matches in both the WebUI and CLI. **Scenario:** This issue was observed in Mobility Masters and managed devices running AOS-W 8.3.0.0 or later versions.	DDS	All platforms	AOS-W 8.5.0.1
AOS-190236	—	**Symptom:** A few clients were not redirected to the captive portal login page. The fix ensures that the clients are redirected to the captive portal login page. **Scenario:** This issue occurred when PEFNG license was not installed in the stand-alone switch and domain name was configured in the captive portal page. This issue was observed in OAW-4550 switches running AOS-W 8.2.0.0 or later versions.	Captive Portal	OAW-4550 switches	AOS-W 8.2.1.1
AOS-190458	—	**Symptom:** The system logs of a managed device did not display warning messages when the managed device disabled both the radios of an AP due to insufficient power. The fix ensures that the warning messages are displayed in the system log of the managed device. **Scenario:** This issue was observed in managed devices running AOS-W 8.5.0.0 or later versions.	AP-Platform	All platforms	AOS-W 8.5.0.0
AOS-190905	—	**Symptom:** An AP crashed and rebooted unexpectedly. The log file listed the reason for this event as **kernel panic: subsys-restart: Resetting the SoC - q6v5-wcss crashed**. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue was observed in OAW-AP550 Series access points running AOS-W 8.5.0.0 or later versions.	AP-Wireless	OAW-AP550 Series access points	AOS-W 8.5.0.1
AOS-190930	—	**Symptom:** Multiple APs crashed unexpectedly. The fix ensures that the APs work as expected. **Scenario:** This issue occurred when the users disabled a cluster to add a new managed device and the APs failed over to the other cluster. This issue was observed in managed devices running AOS-W 8.4.0.4 or later versions in a Mobility Master-Managed Device topology.	AP Datapath	All platforms	AOS-W 8.4.0.4

Table 6: *Resolved Issues in AOS-W 8.5.0.5*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-191035	—	**Symptom:** When the user enabled redundancy, an error message was displayed - **VRRP IP or VLAN cannot be changed when cluster group-membership is enabled. Disable cluster groupmembership on all nodes and try again**. The fix ensures that the error message does not appear. **Scenario:** This issue was observed in managed devices running AOS-W 8.4.0.4.	Cluster-Manager	All platforms	AOS-W 8.4.0.4
AOS-191106	—	**Symptom:** A few managed device sent OSPF LSA logs with error message **BAD LSA TYPE** in LSA checksum causing the OSPF neighbour to go down. With the fix, Aruba controllers do not send bad LSA checksums. **Scenario:** This issue occurred when the managed device established OSPF neighbour relationship with routers other than Alcatel-Lucent routers. This issue was observed in managed devices running AOS-W 8.4.0.0 or later versions.	OSPF	All platforms	AOS-W 8.4.0.0
AOS-191214	—	**Symptom:** A few managed devices crashed and rebooted unexpectedly. The log files listed the reason for the event as **Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2)**. The fix ensures that the managed devices work as expected. **Scenario:** This issue was observed in managed devices running AOS-W 8.2.1.0 or later versions.	switch-Datapath	All platforms	AOS-W 8.2.1.0
AOS-191261	—	**Symptom:** A few wireless clients were unable to connect to the network due to mac-user entries leak. The fix ensures that the clients are able to connect to the network. **Scenario:** This issue was observed in managed devices running AOS-W 8.3.0.5 or later versions.	Base OS Security	All platforms	AOS-W 8.3.0.5
AOS-191496 AOS-195338	—	**Symptom:** A few clients were unable to connect to APs. This fix ensures that the clients are able to connect to the APs. **Scenario:** This issue occurred when the status of the APs was **Down** though the SSIDs of the APs were available. This issue was observed in OAW-AP340 Series access points running AOS-W 8.3.0.0 or later versions.	AP-Platform	OAW-AP340 Series access points	AOS-W 8.4.0.2

Table 6: *Resolved Issues in AOS-W 8.5.0.5*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-191675	—	**Symptom:** Some clients experienced packet loss, when they attempted to reach the destination with route-cache entry marked as inactive. The fix ensures that inactive route-cache entry is not created and a bandwidth contract is used for IP packets with errors, to avoid flooding the Captive Portal. **Scenario:** This issue was observed in managed devices running AOS-W 8.3.0.3 or later versions.	switch-Datapath	All platforms	AOS-W 8.3.0.3
AOS-191962	—	**Symptom:** An AP that terminated on a managed device did not come up when CPsec was enabled with auto certification. The fix ensures that the AP works as expected. **Scenario:** This issue occurred when CPsec auto cert provisioning was enabled in a Virtual OmniAccess Mobility Controller. This issue was observed in APs running AOS-W 8.4.0.4 or later versions.	AP-Platform	All platforms	AOS-W 8.4.0.4
AOS-192044	—	**Symptom:** A managed device crashed and rebooted unexpectedly. The log files listed the reason for the event as **Hardware Watchdog Reset (Intent:cause:register 53:86:50:8)**. The fix ensures that the managed device works as expected. **Scenario:** This issue was observed in managed devices running AOS-W 8.5.0.0 in a Mobility Master-Managed Device topology.	switch-Datapath	All platforms	AOS-W 8.5.0.2
AOS-192542	—	**Symptom:** The BSSID MTU value in data zone reverted to the previous value after the AP was rebooted. The fix ensures that the BSSID MTU value is changed successfully using the **ap system-profile** command. **Scenario:** This issue was observed in APs running AOS-W 8.2.2.0 or later versions.	AP-Platform	All platforms	AOS-W 8.5.0.1
AOS-192680	—	**Symptom:** The RADIUS attributes configured using RADIUS modifier profile were not sent in the RADIUS request for clients during 802.1x authentication. The fix ensures that the attributes from RADIUS modifier profile are sent in RADIUS request for 802.1x clients. **Scenario:** This issue was observed in managed devices running AOS-W 8.4.0.0 or later versions.	Base OS Security	All platforms	AOS-W 8.5.0.1

Table 6: *Resolved Issues in AOS-W 8.5.0.5*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-192711	—	**Symptom:** The load balancing between two RADIUS servers failed on a managed device. The fix ensures that load balancing between the two RADIUS authentication servers works as expected. **Scenario:** This issue occurred because the authentication requests were not distributed equally between both the RADIUS servers. This issue was observed in managed devices running AOS-W 8.4.0.0 or later versions in a Mobility Master-Managed Device topology.	RADIUS	All platforms	AOS-W 8.5.0.1
AOS-192745	—	**Symptom:** The **STM** process crashed unexpectedly in a managed device. This issue is resolved by increasing the buffer size of the mesh AP. **Scenario:** This issue occurred because the buffer size for mesh AP was small. This issue was observed in managed devices running AOS-W 8.4.0.0 or later versions.	Station Management	All platforms	AOS-W 8.4.0.0
AOS-192746 AOS-193755 AOS-196642	—	**Symptom:** Multiple APs were marked as **Down** and were inactive during upgrade of DHCPv6 server. The fix ensures that the APs work as expected. **Scenario:** This issue occurred when a DHCPv6 server was migrated from physical to virtual machines, and the IPv6 address of the DHCPv6 server was changed during the migration. This issue was observed in APs running AOS-W 8.3.0.0 or later versions in a Mobility Master-Managed Device topology.	DHCP	All platforms	AOS-W 8.3.0.8
AOS-193103	—	**Symptom:** Incorrect captive portal redirect URL was observed because of corrupt **apgroup** field name. The fix ensures that the correct **apgroup** field name is used in the captive portal redirect URL. **Scenario:** This issue was observed in managed devices running AOS-W 8.4.0.4 or later versions.	Captive Portal	All platforms	AOS-W 8.4.0.4
AOS-193559	—	**Symptom:** The **crypto-local ipsec-map <ipsec-map-name> <ipsec-map-number>** command did not accept IP addresses of the peer gateway that ended with 0 or 255 in a Mobility Master. As a result, the output of the **peer-ip <ipaddr>** command displayed the **Peer address cannot be a subnet or broadcast address** error message. The fix ensures that the Mobility Master allows peer IP addresses that ends with 0 or 255 except the following IP addresses: 255.255.255.255, 0.0.0.0, and 127.0.0.1 **Scenario:** This issue was observed in Mobility Masters running AOS-W 8.3.0.0 or later versions.	IPsec	All platforms	AOS-W 8.4.0.0

Table 6: *Resolved Issues in AOS-W 8.5.0.5*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-193660	—	**Symptom:** Some APs did not respond to the probe request for a hidden BSSID when two SSIDs were configured. The fix ensures that the APs respond to the probe request. **Scenario:** This issue was not limited to any specific AP model or AOS-W release version.	AP-Wireless	All platforms	AOS-W 8.3.0.8
AOS-193661 AOS-193696	—	**Symptom:** The output of several AP commands displayed **Module AM is busy. Please try later.** or **Module AP STM is busy. Please try later.** messages. The fix ensures that the error messages are not displayed for the commands. **Scenario:** This issue was observed in OAW-AP535 access points running AOS-W 8.3.0.0 or later versions in a Mobility Master-Managed Device topology.	AP Datapath	OAW-AP535 access points	AOS-W 8.5.0.2
AOS-193960	—	**Symptom:** The **show ap debug radio-stats** command did not display the channel utilization value. The fix ensures that the command works as expected. **Scenario:** This issue was observed in Mobility Masters running AOS-W 8.3.0.5 or later versions.	AP-Wireless	All platforms	AOS-W 8.3.0.5
AOS-194088	—	**Symptom:** A managed device failed to add RADIUS accounting session ID in the RADIUS access-request sent by clients. The issue is resolved by adding the missing flags containing RADIUS accounting session ID. **Scenario:** This issue was observed in managed devices running AOS-W 8.3.0.0 or later versions.	Base OS Security	All platforms	AOS-W 8.5.0.1
AOS-194157	—	**Symptom:** A client that failed wired Secure Jack 802.1X authentication was able to obtain an IP address on the post-auth VLAN in a managed device. The fix ensures that the managed device works as expected. **Scenario:** This issue was observed in managed devices running AOS-W 8.3.0.0 or later versions in a master-local topology.	Base OS Security	All platforms	AOS-W 8.3.0.0

Table 6: *Resolved Issues in AOS-W 8.5.0.5*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-194396 AOS-194397	—	**Symptom:** An AP crashed and rebooted unexpectedly. The log files listed the reason for the event as **kernel panic: Fatal exception in interrupt**. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue was observed in OAW-AP530 Series access points running AOS-W 8.5.0.0 or later versions in a Mobility Master-Managed Device topology.	AP-Wireless	OAW-AP530 Series access points	AOS-W 8.5.0.2
AOS-194519 AOS-196024	—	**Symptom:** A few 802.11r clients were unable to connect to APs during 802.1X authentication that led to packet drops in client traffic. The fix ensures that the clients are able to connect to the APs seamlessly. **Scenario:** This issue occurred when the APs were connected to Mobility Controller Virtual Appliances. This issue was observed in APs running AOS-W 8.4.0.0 or later versions.	802.1X	All platforms	AOS-W 8.5.0.0
AOS-194586 AOS-197002	—	**Symptom:** An 802.11ax client reconnected to an AP but did not send or receive traffic. This issue is resolved by: ■ Setting or clearing some HE capabilities from the configured values. ■ Sending some HE operation fields to AP station manager. ■ Adjusting the configured MCS rates for the current stream count. ■ Avoiding corruption of an HE capability information element when saving the MCS rates. **Scenario:** This issue occurred when the SSID used SAE WAP3 with HE and a client reconnected to the AP. This issue was observed in OAW-AP510 Series, OAW-AP530 Series, and OAW-AP550 Series access points running AOS-W 8.5.0.0.	Station Management	OAW-AP510 Series, OAW-AP530 Series, and OAW-AP550 Series access points	AOS-W 8.5.0.0
AOS-194591	—	**Symptom:** A few managed devices were unable to form clusters between cluster nodes. The fix ensures that the managed devices work as expected. **Scenario:** This issue occurred when the traffic for port numbers 9190 and 9199 was blocked, due to which the **DDS** process in the managed devices was unable to synchronize and form clusters. This issue was observed in managed devices running AOS-W 8.2.0.0 or later versions.	DDS	All platforms	AOS-W 8.5.0.2

Table 6: *Resolved Issues in AOS-W 8.5.0.5*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-195084 AOS-195001	—	**Symptom:** An AP crashed and rebooted unexpectedly. The log file listed the reason for the event as **kernel panic: Take care of the TARGET ASSERT first**. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue was observed in OAW-AP535 and OAW-AP555 access points running AOS-W 8.5.0.0 or later versions.	AP-Wireless	OAW-AP535 and OAW-AP555 access points	AOS-W 8.5.0.1
AOS-195180	—	**Symptom:** A few clients were unable to connect to a Virtual AP that had 802.11r enabled, and the clients were deauthenticated. The fix ensures that the clients are able to connect to the Virtual AP. **Scenario:** This issue occurred after a High Availability failover. This issue was observed in APs running AOS-W 8.3.0.0 or later versions in a Mobility Master-Managed Device topology.	Station Management	All platforms	AOS-W 8.3.0.8
AOS-195266 AOS-196392	—	**Symptom:** The **dpagent** process in a managed device crashed unexpectedly. The fix ensures that the managed device works as expected. **Scenario:** This issue was observed in managed devices running AOS-W 8.5.0.0 or later versions in a Mobility Master-Managed Device topology.	switch-Datapath	All platforms	AOS-W 8.5.0.3
AOS-195784 AOS-197083	—	**Symptom:** A mesh point failed to establish connection with the mesh portal. The fix ensures that mesh point comes up on the Mobility Master. **Scenario:** This issue occurred when the mesh portal was assigned a new channel. This issue was observed in OAW-AP210 Series, OAW-AP 220 Series, and OAW-AP270 Series access points running AOS-W 8.3.0.0 or later versions.	Mesh	OAW-AP210 Series, OAW-AP 220 Series, and OAW-AP270 Series access points	AOS-W 8.3.0.10
AOS-196103	—	**Symptom:** Heartbeat failures were observed between Mobility Masters and managed devices during ZTP. The fix ensures that the switch-IP address has the correct VLAN interface and the heartbeat packets from the Mobility Master are distributed across the managed devices. **Scenario:** This issue occured when VLAN 1 was set as the switch-IP address instead of VLAN 4094. This issue was observed in managed devices running AOS-W 8.5.0.0 or later versions.	Interface	All platforms	AOS-W 8.5.0.3

Table 6: *Resolved Issues in AOS-W 8.5.0.5*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-196594	—	**Symptom:** A few 802.1X clients were deauthenticated and lost connectivity to an AP. The fix ensures that the clients are able to connect to the AP. **Scenario:** This issue occurred when the PMK ID sent by the clients was not renewed. This issue was observed in APs running AOS-W 8.4.0.0 or later versions.	802.1X	All platforms	AOS-W 8.5.0.3
AOS-196937	—	**Symptom:** A stand-alone switch sent Network Advertisement using destination Layer 2 MAC address. The fix ensures that the stand-alone switch sends the Network Advertisement to the MAC address available in **Source Link-Layer Address** option. **Scenario:** This issue was observed in OAW-4750XM switches running AOS-W 8.2.0.0 or later versions.	IPv6	OAW-4750XM switches	AOS-W 8.5.0.1
AOS-197440	—	**Symptom:** A few clients were deauthenticated unexpectedly by an AP. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue occurred when AP impersonation event was triggered based on the number of beacon frames sent by the wireless driver to Air Monitor. This issue was observed in OAW-AP535 access points running AOS-W 8.5.0.0 or later versions.	AP-Wireless	OAW-AP535 access points	AOS-W 8.5.0.4

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.

Known Issues

Following are the known issues observed in this release.

Table 7: *Known Issues in AOS-W 8.5.0.5*

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 following 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

Table 7: *Known Issues in AOS-W 8.5.0.5*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
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
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-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-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
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

Table 7: *Known Issues in AOS-W 8.5.0.5*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-156742 AOS-156977	193031 193319	**Symptom:** A user is unable to make any change to IP Probe configuration, after forwarding a complete configuration by 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-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** string 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
AOS-182073 AOS-183743	—	**Symptom:** An AP crashes and reboots unexpectedly. The log files lists the reason for the event as **Reboot caused by kernel panic: Rebooting the AP because of FW ASSERT**. **Scenario:** This issue is observed in OAW-AP315 access points running AOS-W 8.3.0.5. **Workaround:** None.	IPsec	OAW-AP315 access points	AOS-W 8.3.0.5
AOS-183669 AOS-190457 AOS-192089 AOS-194012	—	**Symptom:** The system LED blinks with a green light after a OAW-RAP connects to the managed device and boots up. **Scenario:** : This issue is observed in OAW-RAPs running AOS-W 8.5.0.0 or later versions. **Workaround:** None.	Air Management - IDS	All platforms	AOS-W 8.4.0.0
AOS-183998 AOS-183999	—	**Symptom:** A few users are unable to configure the PPPoE password when they provision a OAW-RAP in the **Configuration > Access Points > Remote APs** page of the WebUI. **Scenario:** This issue occurs because the **Retype password** field for PPPoE is missing from the **Uplink** option in the provisioning page of the WebUI. This issue is observed in OAW-RAPs running AOS-W 8.2.2.0 or later versions. **Workaround:** None.	WebUI	All platforms	AOS-W 8.3.0.6

Table 7: *Known Issues in AOS-W 8.5.0.5*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-184135	—	**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-184977 AOS-188242 AOS-188378	—	**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
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

Table 7: *Known Issues in AOS-W 8.5.0.5*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
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-186860	—	**Symptom:** RADIUS authentication requests are sent in IP address of the managed device though they are configured to go through the loopback IP. **Scenario:** This issue is observed in managed devices running AOS-W 8.4.0.0 or later versions. **Workaround:** None.	IPsec	All platforms	AOS-W 8.4.0.1
AOS-187268 AOS-196356	—	**Symptom:** A few APs crash and reboot unexpectedly. The log files list the reason for the event as **Reboot caused by kernel panic: Fatal exception**. **Scenario:** This issue occurs when 802.11w standard is enabled in the APs. This issue is observed in APs running AOS-W 8.3.0.0 or later versions. **Workaround:** None.	AP-Wireless	All platforms	AOS-W 8.3.0.0
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. **Workaround:** None.	Configuration	All platforms	AOS-W 8.3.0.5
AOS-187479 AOS-188428	—	**Symptom:** The authentication server configuration details are not forwarded from the primary Mobility Master to the secondary Mobility Master in Layer-3 redundancy configuration. **Scenario:** This issue is observed in a Mobility Master Virtual Appliance running AOS-W 8.4.0.0 or later versions. **Workaround:** None.	Configuration	All platforms	AOS-W 8.4.0.2
AOS-187820	—	**Symptom:** The output of the **show cpuload per-cpu** command displays the same CPU load statistics for each processor. **Scenario:** This issue occurs after reboot of the switch. This issue is observed in managed devices running AOS-W 8.4.0.0 or later versions. **Workaround:** None.	switch-Platform	All platforms	AOS-W 8.4.0.0

Table 7: *Known Issues in AOS-W 8.5.0.5*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
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-188002 AOS-195453	—	**Symptom:** The OFA process crashes in a managed device unexpectedly. **Scenario:** This issue occurs due to a memory leak. This issue is observed in managed devices running AOS-W 8.2.2.0 or later versions. **Workaround:** None.	SDN	All platforms	AOS-W 8.4.0.3
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

Table 7: *Known Issues in AOS-W 8.5.0.5*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-188467	—	**Symptom:** The AMON messages from a peer cluster display **wrong value for cl_cluster_incompatible_reason**. **Scenario:** This issue occurs when the incompatible reason is not reset after an incompatibility with a peer cluster member is resolved and the cluster is re-formed. This issue is observed in managed devices running AOS-W 8.3.0.6 in a cluster topology. **Workaround:** None.	Cluster-Manager	All platforms	AOS-W 8.3.0.6
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-188485 AOS-193638	—	**Symptom:** The **<ofald 237504> <ERRS> |AP 32438@172.16.4.151 ofald| |sdn| ERRS ofald_datapath_msg_recv_cb:274 Invalid message type 126** error message is displayed every second in APs. **Scenario:** This issue is observed in APs running AOS-W 8.4.0.0-FIPS in a Mobility Master-Managed Device topology. **Workaround:** None.	SDN	All platforms	AOS-W 8.4.0.0
AOS-188490 AOS-189847 AOS-192747 AOS-197045	—	**Symptom:** A Mobility Master crashes and reboots unexpectedly. The log file lists the reason for the event as **Datapath timeout (SOS Assert) (Intent:cause:register 54:86:0:20)**. **Scenario:** This issue is observed in Mobility Masters running AOS-W 8.3.0.0 or later versions. **Workaround:** None.	switch-Datapath	All platforms	AOS-W 8.3.0.0
AOS-188897	—	**Symptom:** An AP crashes unexpectedly. The log files list the reason for the event as **Internal error: Oops: 96000004 [#1] SMP**. **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

Table 7: *Known Issues in AOS-W 8.5.0.5*

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-189913 AOS-193777	—	**Symptom:** A stand-alone switch fails to establish communication with the Activate server during ZTP. **Scenario:** This issue occurs when the database synchronization fails between the stand-alone switches in L2 redundancy. As a result, the output of the **show database synchronize** command displays the **Standby switch did not acknowledge the WMS database restore request** message. This issue is observed in OAW-4850 switches running AOS-W 8.5.0.0 or later versions. **Workaround:** None.	switch-Platform	OAW-4850 switches	AOS-W 8.5.0.2
AOS-189977	—	**Symptom:** A managed device crashes and reboots unexpectedly. The log file lists the reason for the event as **Reboot Cause: Datapath timeout (Fpapps Initiated) (Intent:cause:register 51:86:50:2)**. **Scenario:** This issue is observed in managed devices running AOS-W 8.3.0.0 or later versions. **Workaround:** None.	switch-Datapath	All platforms	AOS-W 8.3.0.7
AOS-190071 AOS-190372	—	**Symptom:** A few users are unable to access the 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:** ■ 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

Table 7: *Known Issues in AOS-W 8.5.0.5*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-190230 AOS-194760	—	**Symptom:** A few OAW-RAPs fail to come up on the managed device after reboot of the APs, and get the same inner IP address which has already been assigned to other OAW-RAPs. **Scenario:** This issue occurs because most of the OAW-RAP whitelist database entries are removed from the Mobility Master. This issue is observed in APs running AOS-W 8.4.0.0 or later versions. **Workaround:** Purge the OAW-RAP whitelist database entries on the Mobility Master and managed device, and add them again.	CPsec	All platforms	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-190380 AOS-196361	—	**Symptom:** A few users are unable to connect to VIA server from the guest account. **Scenario:** This issue occurs because PBR is not applied to data packets from UDP 4500 port. As a result, the client traffic is not forwarded correctly. This issue is observed in managed devices running AOS-W 8.0.0.0 or later versions. **Workaround:** None.	switch-Datapath	All platforms	AOS-W 8.0.1.0
AOS-190836	—	**Symptom:** The output of the **show interface gigabitethernet 0/0/0 transceiver** command displays the **Error reading Transceiver ID Prom on 0/0/0** message when the Small Form-factor Pluggable transceiver (SFP module) is connected to the Mobility Master. **Scenario:** This issue is observed in Mobility Masters running AOS-W 8.5.0.0 or later versions. **Workaround:** None.	switch-Platform	All platforms	AOS-W 8.5.0.1
AOS-191539	—	**Symptom:** The configuration synchronization fails and the status of the synchronization displays as **CONFIG Failure** 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 tunnel number 2048 is set for the interface tunnel. 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

Table 7: *Known Issues in AOS-W 8.5.0.5*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-191565	—	**Symptom:** A Mobility Master Virtual Appliance displays high memory utilization. **Scenario:** This issue is observed in Mobility Master Virtual Appliances running AOS-W 8.4.0.0 or later versions. **Workaround:** None.	Firewall Visibility	All platforms	AOS-W 8.4.0.0
AOS-191579 AOS-195733	—	**Symptom:** A few users are unable to connect to the wireless network. **Scenario:** This issue occurs when the **authentication** process crashes unexpectedly in a managed device. This issue is observed in managed devices running AOS-W 8.3.0.0 or later versions. **Workaround:** None.	Base OS Security	All platforms	AOS-W 8.3.0.0
AOS-191820	—	**Symptom:** The output of the **show datapath dns-cache counter** command does not display any information. **Scenario:** This issue is observed in managed devices running AOS-W 8.5.0.1 or later versions. **Workaround:** None.	switch-Datapath	All platforms	AOS-W 8.5.0.1
AOS-192568 AOS-192736	—	**Symptom:** A few clients are unable to connect to APs even though High Efficiency was disabled on all the SSID profiles of the APs. **Scenario:** This issue is observed in OAW-AP515 access points running AOS-W 8.5.0.0 or later versions. **Workaround:** None.	DDS	OAW-AP515 access points	AOS-W 8.5.0.1
AOS-192841	—	**Symptom:** The **STM** process crashes on a managed device and the APs are unable to communicate with the managed device. **Scenario:** This issue is observed in managed devices running AOS-W 8.3.0.1 or later versions. **Workaround:** None.	AP-Platform	All platforms	AOS-W 8.0.0.0
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

Table 7: *Known Issues in AOS-W 8.5.0.5*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-193188	—	**Symptom:** The **Reclassify Detected Radios** pop-up window displays action commands for a specific SSID in the **Dashboard > Security > Detected Radios** page of the WebUI. **Scenario:** This issue occurs when apostrophe and quotation are added to the ESSID of a stand-alone switch. This issue is observed in OAW-4550 switches running AOS-W 8.4.0.0 or later versions. **Workaround:** None.	WebUI	OAW-4550 switches	AOS-W 8.5.0.1
AOS-193775 AOS-194581	—	**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-194052	—	**Symptom:** A few clients are unable to obtain IP addresses. **Scenario:** This issue occurs when High Efficiency is enabled on the WPA2-PSK SSID profile of the APs. This issue is observed in Mobility Controller Virtual Appliances running AOS-W 8.5.0.0 or later versions. **Workaround:** Disable High Efficiency on the WPA2-PSK SSID profile of the APs.	switch-Platform	All platforms	AOS-W 8.5.0.2
AOS-194146	—	**Symptom:** A managed device does not display any warning message when the cluster profile name contains more than 32 characters. **Scenario:** This issue is observed in managed devices running AOS-W 8.5.0.2 or later versions in a cluster setup. **Workaround:** None.	Cluster-Manager	All platforms	AOS-W 8.5.0.2
AOS-194325 AOS-194579	—	**Symptom:** The **datapath** process in a managed device crashes multiple times. **Scenario:** This issue is observed in managed devices running AOS-W 8.3.0.0 or later versions in a Mobility Master-Managed Device topology. **Workaround:** None.	switch-Datapath	All platforms	AOS-W 8.3.0.7
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

Table 7: *Known Issues in AOS-W 8.5.0.5*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-194390	—	**Symptom:** The **SAPD** process crashes in a managed device unexpectedly. The log files lists the reason for this event as **RF Client failed: No such file or directory Message Code 1005 Sequence Num is 18119 Aug 29 10:35:21 sapd[2905]: RF Client failed: No such file or directory Message Code 1003 Sequence Num is 18112**. **Scenario:** This issue is observed in managed devices running AOS-W 8.3.0.0 or later versions. **Workaround:** None.	AP-Platform	All platforms	AOS-W 8.3.0.8
AOS-194706	—	**Symptom:** A managed device crashes and reboots unexpectedly. The log files list 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 8.3.0.7 or later versions in a Mobility Master-Managed Device topology. **Workaround:** None.	switch-Datapath	All platforms	AOS-W 8.5.0.2
AOS-194727	—	**Symptom:** An AP sends RTS requests continuously to one client only and this results in delay or packet drop to other clients. **Scenario:** This issue is observed in OAW-AP340 Series access points running AOS-W 8.3.0.7 or later versions. **Workaround:** None.	AP-Wireless	OAW-AP340 Series access points	AOS-W 8.3.0.7
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-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.	Configuration	All platforms	AOS-W 8.5.0.2

Table 7: *Known Issues in AOS-W 8.5.0.5*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-195000	—	**Symptom:** A few APs crash unexpectedly. The log files list the reason for the event as **Kernel panic: softlockup - hung tasks**. **Scenario:** This issue is observed in OAW-AP515 access points running AOS-W 8.5.0.1 or later versions. **Workaround:** None.	AP-Wireless	OAW-AP515 access points	AOS-W 8.5.0.1
AOS-195036	—	**Symptom:** The **authentication** process in a managed device crashes unexpectedly. **Scenario:** This issue is observed in managed devices running AOS-W 8.3.0.0 or later versions. **Workaround:** None.	802.1X	All platforms	AOS-W 8.3.0.6
AOS-195162	—	**Symptom:** The WebUI is unresponsive and the licenses are not visible in the **Mobility Master > Configuration > Licenses** page in the WebUI. **Scenario:** This issue occurs when 29 non-default pools are configured and enabled. This issue is observed in Mobility Masters running AOS-W 8.5.0.1 or later versions. **Workaround:** None.	Licensing	All platforms	AOS-W 8.5.0.1
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-195265	—	**Symptom:** A managed device crashes and reboots unexpectedly. The log files list the reason for the event as **Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2)**. **Scenario:** This issue occurs due to ACL corruption. This issue is observed in managed devices running AOS-W 8.5.0.0 or later versions. **Workaround:** None.	SDN	All platforms	AOS-W 8.5.0.3

Table 7: *Known Issues in AOS-W 8.5.0.5*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
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-195677 AOS-196311	—	**Symptom:** The **airmatch_recv** process crashes unexpectedly in a Mobility Master. **Scenario:** This issue is observed in Mobility Masters running AOS-W 8.3.0.0 or later versions in a Mobility Master-Managed Device topology. **Workaround:** None.	AirMatch	All platforms	AOS-W 8.3.0.7
AOS-196729	—	**Symptom:** An AP crashes and reboots unexpectedly. The log files list the reason for the event as **Unable to set up IPSec tunnel, Error:RC_ ERROR_IKEV2_TIMEOUT**. **Scenario:** This issue is observed in OAW-AP340 Series access points running AOS-W 8.5.0.3 or later versions. **Workaround:** None.	AP-Wireless	OAW-AP340 Series access points	AOS-W 8.5.0.3

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:

Migrating from AOS-W 6.x to AOS-W 8.x

Use the interactive migration tool provided on the customer support site to migrate any AOS-W 6.x deployments to one of the following AOS-W 8.x deployments:

- Master-Local setup to Mobility Master
- All-Master setup to Mobility Master
- Master-Local setup to Master switch Mode in AOS-W 8.x
- Stand-alone switch running AOS-W 8.x

For more information, refer to the *AOS-W 8.x Migration Guide*.

NOTE

Licenses are not migrated by the migration tool from any of the devices to Mobility Master. However, the licenses are preserved when migrating to AOS-W 8.x Master switch Mode or stand-alone switches. For more information on License migration, refer to *Alcatel-Lucent Mobility Master Licensing Guide*.

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.