AOS-W 8.5.0.7

Alcatel·Lucent

Enterprise

Copyright Information

Open Source Code

Contents

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:

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

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

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

CLI

airgroupprofile commad

A new parameter, **network** is added to the **airgroupprofile** command. The **network default** is enabled whenever an **airgroupprofile** is configured in either distributed or centralized mode. This parameter allows the users to,

- Block or blacklist the client or server based on the MAC address or MAC OUI.
- Limit the number of maximum allowed IP addresses per server.
- Limit the number of maximum tokens allowed per server or client.

The following are the limitation of the **network default** parameter:

- User defined network profile is not supported.
- The default network profile is always enabled and cannot be disabled when any **airgroupprofile** is activated.
- The default network profile can be modified only from **/md** hierarchy node.
- In case of multiple islands, the network profile is activated only to the island where the **airgroupprofile** is activated.

```
(host) [md] (config) #airgroupprofile network default
(host) [md] (Network profile "default") #blacklist-mac <macaddr>
(host) [md] (Network profile "default") #max-ip-per-device <number of ip addresses>
(host) [md] (Network profile "default") #max-tokens-per-device <number of tokens>
```

datapath command

- A new parameter, **dns-cache periodic-flush** is introduced to the **datapath** command. The **dns-cache periodic-flush** parameter configures time period to check if the **dns iplist table** has reached the configured threshold level.

```
(host) [mynode] (config) #datapath dns-cache periodic-flush <interval> <threshold>
```

- A new counter, **DNS-Cache Clear Count** has been added to the **show datapath dns-cache counters** command output.

IPv6

Network Advertisement

Starting from AOS-W 8.5.0.7, a stand-alone switch sends the network advertisement to the MAC address available in Source Link-Layer Address option.

LLDP

Starting from AOS-W 8.5.0.7, when an AP is in active-standby mode, LLDP packets transmitted from eth1 interface will use eth1's hardware address as Layer-2 source MAC address.

WebUI

Enhancements to the Traffic Analysis Page

Users can now allow, deny, or block application traffic by hovering on the Application line in the **Dashboard > Traffic Analysis > Applications** page in the WebUI.

Support for Cluster Members

AOS-W displays a **Cluster Members** pop-up window under **Dashboard > Infrastructure > Clusters** page in the WebUI. The **Cluster Members** pop-up window displays a summary of each cluster member, includes the connection type - L2, L3, or both and the latency information of each selected cluster.

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 8.5.0.7*

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 8.5.0.7*

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 8.5.0.7*

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 8.5.0.7*

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

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_74492

This chapter describes the issues 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 8.5.0.7*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-137577 AOS-139523 AOS-145692 AOS-196723	167045 169550 177729	**Symptom:** The **authentication** process in a Mobility Master crashed and the WebUI of the Mobility Master was inaccessible. The fix ensures that the Mobility Master works as expected. **Scenario:** This issue occurred when the **show global-usertable** command was executed. This issue was observed in Mobility Masters running AOS-W 8.3.0.0 or later versions.	Base OS Security	All platforms	AOS-W 8.3.0.0
AOS-146689 AOS-184873	179064	**Symptom:** The status of the virtual AP was temporarily **DOWN**, which resulted in clients getting disconnected. The fix ensures that the APs work as expected. **Scenario:** This issue was observed in access points running AOS-W 8.2.0.0 or later versions.	AP - Wireless	All platforms	AOS-W 8.2.0.0
AOS-156424 AOS-156777 AOS-185158 AOS-193880 AOS-198034 AOS-198568	192581 193081	**Symptom:** Invalid SSIDs were displayed in the **Dashboard > WLAN** page in the WebUI. The fix ensures that the WebUI displays only the valid SSIDs. **Scenario:** This issue occurred when a few APs were broadcasting invalid SSIDs. This issue was observed in managed devices running AOS-W 8.2.2.0 or later versions.	Monitoring	All platforms	AOS-W 8.2.2.0
AOS-157356	193833	**Symptom:** The **firewall dns-name cache** command filled up and caused service interruptions. This issue is resolved by automatically clearing the IP address list entries every 24 hours. **Scenario:** This issue was observed in managed devices running AOS-W 8.0.0.0 or later versions.	switch-Datapath	All platforms	AOS-W 8.0.0.0
AOS-157882 AOS-200009	194655	**Symptom:** The **Dashboard > Overview > Clients** page displayed incorrect roles for wired clients connected to a OAW-RAP. The fix ensures that the WebUI displays the correct role for wired clients. **Scenario:** This issue was observed in stand-alone switches running AOS-W 8.4.0.0 or later versions.	WebUI	All platforms	AOS-W 8.4.0.0

Table 6: *Resolved Issues in AOS-W 8.5.0.7*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-182579 AOS-195790 AOS-196493 AOS-197868 AOS-197989	—	**Symptom:** APs and clients got disconnected frequently from the managed device. The fix ensures seamless connectivity. **Scenario:** This issue occurred when heartbeats were randomly missed on the managed device. This issue was observed in managed devices running AOS-W 8.3.0.2 or later versions in a cluster setup.	switch-Datapath	All platforms	AOS-W 8.3.0.2
AOS-182923	—	**Symptom:** Mobility Master's scheduled deployments did not occur at the time scheduled in the AirMatch profile. The fix ensures that the scheduled deployments occur at the time scheduled in the AirMatch profile. **Scenario:** This issue was observed in Mobility Masters running AOS-W 8.2.2.3 or later versions.	AirMatch	All platforms	AOS-W 8.2.2.3
AOS-183669 AOS-190457 AOS-192089 AOS-194012	—	**Symptom:** The system LED blinked with a green light after a OAW-RAP connected to the managed device and booted up. The fix ensures that the system LED blinks with red light when the OAW-RAP boots up. **Scenario:** This issue was observed in OAW-RAPs running AOS-W 8.5.0.0 or later versions.	Air Management - IDS	All platforms	AOS-W 8.4.0.0
AOS-183998 AOS-183999	—	**Symptom:** A few users were unable to configure the PPPoE password when they provisioned a OAW-RAP in the **Configuration > Access Points > Remote APs** page of the WebUI. The fix ensures that the users are able to configure PPPoE password. **Scenario:** This issue occurred because the **Retype password** field for PPPoE was missing from the **Uplink** option in the provisioning page of the WebUI. This issue was observed in OAW-RAPs running AOS-W 8.2.2.0 or later versions.	WebUI	All platforms	AOS-W 8.3.0.6

Table 6: *Resolved Issues in AOS-W 8.5.0.7*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-184268 AOS-197642 AOS-198392	—	**Symptom:** The command **show ap debug mgmt-frames** displayed an error message, **stm| |ap| Unexpected stm (Station management) runtime error at handle_assoc_req, 7314**. Enhancements to the wireless driver fixed the issue. **Scenario:** This issue occurred when the peer APs sent two reassociation requests simultaneously. This issue was observed in access points AOS-W 8.4.0.0 or later versions.	AP - Wireless	All platforms	AOS-W 8.4.0.2
AOS-184705 AOS-186108	—	**Symptom:** Some clients were unable to send and receive data traffic. The fix ensures that the clients send and receive data traffic. **Scenario:** This issue occurred when the client experienced inter-band roaming in both bridge and decrypt-tunnel forward modes. This issue was observed in managed devices running AOS-W 8.5.0.0 or later versions.	AP - Wireless	All platforms	AOS-W 8.5.0.0
AOS-185212 AOS-185375	—	**Symptom:** The **Authentication** process crashed in a stand-alone switch. The fix ensures that the switch works as expected. **Scenario:** This issue was observed in OAW-4750 switches running AOS-W 8.3.0.0 or later versions.	Base OS Security	OAW-4750 switches	AOS-W 8.3.0.0
AOS-185745	—	**Symptom:** The output of the **show lldp neighbor** command displayed incorrect remote interface information on a Mobility Master. Increasing the buffer size resolved the issue. **Scenario:** This issue occurred when the buffer size to display the remote interface information was insufficient. This issue was observed in Mobility Masters running AOS-W 8.3.0.0 or later versions.	LLDP	All platforms	AOS-W 8.3.0.0
AOS-186166 AOS-199190	—	**Symptom:** Access points displayed the error log, **sapd_sysctl.c function sapd_sysctl_write_param line 167 error Error opening /proc/sys/net/aruba101/wmm_eap_ac : No such file or directory. 255.** The fix ensures that the access points do not display this error message. **Scenario:** This issue was observed in OAW-AP105 and OAW-AP135 access points running AOS-W 8.5.0.0 or later versions.	AP-Wireless	OAW-AP105 and OAW-AP135 access points	AOS-W 8.5.0.5

Table 6: *Resolved Issues in AOS-W 8.5.0.7*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-186340	—	**Symptom:** The command **show firewall dns-names ap-name** did not display all the necessary information. The fix ensures that the command works as expected. **Scenario:** This issue was observed in access points running AOS-W 8.6.0.0 or later versions.	AP Datapath	All platforms	AOS-W 8.6.0.0
AOS-186649	—	**Symptom:** The word **Fragments** was misspelled in the **show datapath network ingress** command output. The fix ensures that the word fragments is spelled correctly. **Scenario:** This issue was not limited to any switch model or AOS-W release versions.	switch-Datapath	All platforms	AOS-W 8.3.0.0
AOS-186860	—	**Symptom:** RADIUS authentication requests were sent in IP address of the managed device though they are configured to go through the loopback IP. The fix ensures that the RADIUS authentication requests are sent through the loopback IP. **Scenario:** This issue was observed in managed devices running AOS-W 8.4.0.0 or later versions.	IPsec	All platforms	AOS-W 8.4.0.1
AOS-187479 AOS-188428 AOS-197503	—	**Symptom:** The authentication server configuration details were not forwarded from the primary Mobility Master to the secondary Mobility Master in Layer-3 redundancy configuration. The fix ensures that the authentication server configuration details are forwarded. **Scenario:** This issue was observed in a Mobility Master Virtual Appliance running AOS-W 8.4.0.0 or later versions.	Configuration	All platforms	AOS-W 8.4.0.2
AOS-187591	—	**Symptom:** Openflow status changed to enabled automatically after an upgrade. The fix ensures that the Openflow status does not change automatically. **Scenario:** This issue was observed when a managed device was upgraded from AOS-W 8.3.0.7 to AOS-W 8.4.0.3 version.	SDN-Platform	All platforms	AOS-W 8.4.0.3
AOS-187820	—	**Symptom:** The output of the **show cpuload per-cpu** command displayed the same CPU load statistics for each processor. **Scenario:** This issue occurred after a switch reboot. This issue was observed in managed devices running AOS-W 8.4.0.0 or later versions.	switch-Platform	All platforms	AOS-W 8.4.0.0

Table 6: *Resolved Issues in AOS-W 8.5.0.7*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-188002 AOS-195453	—	**Symptom:** The **OFA process** crashed in a managed device unexpectedly. The fix ensures that the **OFA process** works as expected. **Scenario:** This issue occurred due to a memory leak. This issue was observed in managed devices running AOS-W 8.2.2.0 or later versions.	SDN	All platforms	AOS-W 8.4.0.3
AOS-188271 AOS-196680 AOS-197718	—	**Symptom:** Access points crashed and rebooted unexpectedly. The fix ensures that the access point works as expected. **Scenario:** This issue was observed in OAW-AP515 access points running AOS-W 8.5.0.0 or later versions.	AP - Wireless	OAW-AP515 access points	AOS-W 8.5.0.0
AOS-188360	—	**Symptom:** The **show configuration effective detail** command displayed incorrect device level configuration hierarchy. The fix ensures that the command works as expected. **Scenario:** This issue was observed in Mobility Masters running AOS-W 8.3.0.7 or later versions.	Configuration	All platforms	AOS-W 8.3.0.0
AOS-188467	—	**Symptom:** The AMON messages from a peer cluster displayed wrong value **for cl_cluster_incompatible_reason**. The fix ensures that incompatible reason is reset to zero when the cluster is re-formed after resolving incompatibility. **Scenario:** This issue occurred when the incompatible reason was not reset after an incompatibility with a peer cluster member was resolved and the cluster was re-formed. This issue was observed in managed devices running AOS-W 8.3.0.6 in a cluster topology.	Cluster-Manager	All platforms	AOS-W 8.3.0.6
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 was displayed every second in APs. The fix ensures that these spurious message is not displayed. **Scenario:** This issue was observed in APs running AOS-W 8.4.0.0-FIPS in a Mobility Master - Managed Device topology.	SDN	All platforms	AOS-W 8.4.0.0

Table 6: *Resolved Issues in AOS-W 8.5.0.7*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-188490 AOS-189847 AOS-192747 AOS-197045 AOS-198835 AOS-199014	—	**Symptom:** A Mobility Master crashed and rebooted unexpectedly. The log file listed the reason for the event as **Datapath timeout (SOS Assert) (Intent:cause:register 54:86:0:20)**. The fix ensures that the Mobility Master works as expected. **Scenario:** This issue was 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-188897	—	**Symptom:** An AP crashed unexpectedly. The log files listed the reason for the event as **Internal error: Oops: 96000004 [#1] SMP**. The fix ensures that the access points work as expected. **Scenario:** This issue was observed in APs running AOS-W 8.3.0.6 or later versions.	AP-Wireless	All platforms	AOS-W 8.3.0.6
AOS-189118 AOS-200233	—	**Symptom:** VIA clients running Alcatel-Lucent VIA version 3.2 and 3.4 were unable to establish connection with the switch through SSL fallback mode and the following error messages were displayed: ■ **Controller is not responding** ■ **UDP packets are dropped** ■ **SSL tunneling could not be turned on** The fix ensures that the clients can establish connection with the switch through SSL fallback mode. **Scenario:** This issue occurred when UDP port 4500 was blocked. This issue was observed in Mobility Masters running AOS-W 8.3.0.1 or later versions.	IPsec	All platforms	AOS-W 8.3.0.1

Table 6: *Resolved Issues in AOS-W 8.5.0.7*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-189476 AOS-192948	—	**Symptom:** The managed device displayed the error message **authmgr[8721]: <522349> <8721> <DBUG> |authmgr| MAC 04:bd:88:c4:d7:6a IP 10.128.10.45: drop pkt non-DHCP pkt, Option-12 hostname needed for accounting**. The fix ensures that the user table is updated and the managed device does not show the error message. **Scenario:** This issue occurred because the user table was not updated when the aaa profile user name was configured with dhcp option 12. This issue was observed in managed devices running AOS-W 8.5.0.0 or later versions.	MAC-Based Authentication	All platforms	AOS-W 8.5.0.1
AOS-189772 AOS-196328 AOS-198374	—	**Symptom: dot1x** and **dot2x** processes crashed unexpectedly on a managed device. This fix ensures that the managed device works as expected. **Scenario:** 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-189845 AOS-200712 AOS-201675	—	**Symptom:** The **dpagent** module crashed on 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.	switch-Datapath	All platforms	AOS-W 8.5.0.5
AOS-189913 AOS-193777	—	**Symptom:** A stand-alone switch failed to establish communication with the Activate server during ZTP. The fix ensures that the stand-alone switch establish communication with the Activate server during ZTP. **Scenario:** This issue occurred when the database synchronization failed between stand-alone switches in L2 redundancy. As a result, the output of the **show database synchronize** command displayed the **Standby switch did not acknowledge the WMS database restore request** message. This issue was observed in OAW-4850 switches running AOS-W 8.5.0.0 or later versions.	switch-Platform	OAW-4850 switches	AOS-W 8.5.0.2

Table 6: *Resolved Issues in AOS-W 8.5.0.7*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-189977	—	**Symptom:** A managed device crashed and rebooted unexpectedly. The log file listed the reason for the event as **Reboot Cause: Datapath timeout (Fpapps Initiated) (Intent:cause:register 51:86:50:2)**. 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.	switch-Datapath	All platforms	AOS-W 8.3.0.7
AOS-190230 AOS-194760	—	**Symptom:** A few OAW-RAPs failed to come up on the managed device after reboot of the APs, and got the same inner IP address which was already assigned to other OAW-RAPs. The fix ensures that the OAW-RAPs work as expected. **Scenario:** This issue occurred when most of the OAW-RAP whitelist database entries were deleted from the Mobility Master. This issue was observed in APs running AOS-W 8.4.0.0 or later versions.	CPsec	All platforms	AOS-W 8.4.0.0
AOS-190380 AOS-196361	—	**Symptom:** A few users were unable to connect to VIA server from the guest account. The fix ensures that the users are able to connect to VIA server. **Scenario:** This issue occurred because PBR was not applied to data packets from UDP 4500 port. As a result, the client traffic was not forwarded correctly. This issue was observed in managed devices running AOS-W 8.0.0.0 or later versions.	switch-Datapath	All platforms	AOS-W 8.0.1.0
AOS-190633 AOS-191480 AOS-196430 AOS-196935	—	**Symptom:** Clients connected to APs through bridge mode SSID were unable to obtain IP address or forward traffic. Also, the APs crashed and rebooted unexpectedly when the **show ap debug acl-table ap-name <apname>** command was executed. The fix ensures that the APs work as expected and the clients are able to connect to them. **Scenario:** This issue was observed in OAW-AP215 access points running AOS-W 8.3.0.0 or later versions.	AP Datapath	OAW-AP215 access points	AOS-W 8.3.0.0
AOS-190836	—	**Symptom:** The output of the **show interface gigabitethernet 0/0/0 transceiver** command displayed the **Error reading Transceiver ID Prom on 0/0/0** message when the Small Form-factor Pluggable transceiver (SFP module) was connected to the Mobility Master. The fix ensures that the command works as expected. **Scenario:** This issue was observed in Mobility Masters running AOS-W 8.5.0.0 or later versions.	switch-Platform	All platforms	AOS-W 8.5.0.1

Table 6: *Resolved Issues in AOS-W 8.5.0.7*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-190927 AOS-192132	—	**Symptom:** A few managed devices became unresponsive without console access. The fix ensures that the managed devices work as expected. **Scenario:** This issue was observed due to a STM process memory leak. This issue was observed in managed devices running AOS-W 8.4.0.4 or later versions.	switch-Platform	All platforms	AOS-W 8.4.0.4
AOS-191348	—	**Symptom:** Client was unable to load the captive portal page. The fix ensures that the captive portal page loads without any issue. **Scenario:** This issue occurred in a system with proxy settings. This issue was observed in managed devices running AOS-W 8.3.0.7 or later versions.	Captive Portal	All platforms	AOS-W 8.3.0.7
AOS-191549	—	**Symptom:** Users were unable to discover Apple TV. The fix ensures that users are able to discover Apple TV. **Scenario:** The issue occurred when AirGroup was enabled in Centralized mode. This issue was observed in the Mobility Masters running AOS-W 8.4.0.3 or later versions.	AirGroup	All platforms	AOS-W 8.4.0.3
AOS-191565 AOS-197819	—	**Symptom:** A Mobility Master Virtual Appliance displayed high memory utilization. The fix ensures that the Mobility Master Virtual Appliance works as expected. **Scenario:** This issue was observed in Mobility Master Virtual Appliances running AOS-W 8.4.0.0 or later versions.	Firewall Visibility	All platforms	AOS-W 8.4.0.0
AOS-191579 AOS-199406 AOS-195733	—	**Symptom:** A few users were unable to connect to the wireless network. The fix ensures that the users are able to connect to the network. **Scenario:** This issue occurs when the **authentication** process crashed unexpectedly in a managed device. This issue was observed in managed devices running AOS-W 8.3.0.0 or later versions.	Base OS Security	All platforms	AOS-W 8.3.0.0
AOS-191820	—	**Symptom:** The output of the **show datapath dns-cache counter** command did not display any information. The fix ensures that the command works as expected. **Scenario:** This issue was observed in managed devices running AOS-W 8.5.0.1 or later versions.	switch-Datapath	All platforms	AOS-W 8.5.0.1

Table 6: *Resolved Issues in AOS-W 8.5.0.7*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-192005	—	**Symptom:** A Managed device was in **CONFIG FAILURE** state and displayed the error message, **Module CERT DOWNLOAD MANAGER PORT is busy. Please try later**. The fix ensures that the managed device works as expected. **Scenario:** This issue occurred while uploading server certificate for captive portal authentication. This issue was observed in managed devices running AOS-W 8.4.0.4 or later versions.	switch - Datapath	All platforms	AOS-W 8.4.0.4
AOS-192163	—	**Symptom:** A managed device crashed and rebooted unexpectedly. The log file listed the reason for this event as **Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2)**. The fix ensures that the managed device works as expected. **Scenario:** This issue was observed in managed devices running AOS-W 8.3.0.4 or later versions.	switch-Datapath	All platforms	AOS-W 8.3.0.4
AOS-192274	—	**Symptom:** The command **show running-config** did not display LACP related information. The fix ensures that the command displays LACP related information. **Scenario:** This issue was observed in Mobility Masters running AOS-W 8.3.0.8 or later versions.	Configuration	All platforms	AOS-W 8.3.0.8
AOS-192432	—	**Symptom:** Users were unable to edit crypto isakmp policies. The log files listed the reason for the event as **ERROR: Policy number greater than 10000 are reserved and cannot be created/edited**. The fix ensures that the user can edit the crypto isakmp policy even when the policy number is greater than 10000. **Scenario:** This issue occurred because the IKE policy numbers above 10000 were reserved. This issue was observed in managed devices running AOS-W 8.6.0.0 or later versions.	IPsec	All platforms	AOS-W 8.6.0.0
AOS-192529 AOS-199126	—	**Symptom:** Access points crashed and rebooted unexpectedly. The log file listed the reason for the event as **reboot caused by Kernel panic - not syncing: Fatal exception in interrupt with PC/LR is at asap_ firewall_forward+0xfc/0x92a0.** The fix ensures that the access points work as expected. **Scenario:** This issue was observed in access points running AOS-W 8.4.0.2 or later versions.	AP Datapath	All platforms	AOS-W 8.4.0.2

Table 6: *Resolved Issues in AOS-W 8.5.0.7*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-192568 AOS-192736	—	**Symptom:** A few clients were unable to connect to APs even though **High Efficiency** was disabled on all the SSID profiles of the APs. Enhancements to the wireless driver fixed the issue. **Scenario:** This issue was observed in OAW-AP515 access points running AOS-W 8.5.0.0 or later versions.	DDS	OAW-AP515 access points	AOS-W 8.5.0.1
AOS-192814 AOS-199107	—	**Symptom:** The Auto Associate feature of AirGroup did not work as expected and AP related information on AirGroup server was incorrect when clients roamed between different managed devices. The fix ensures that the feature works as expected. **Scenario:** This issue occurred when GSM entries were not updated. This issue was observed in managed devices running AOS-W 8.3.0.7 or later versions in centralized or distributed mode.	AirGroup	All platforms	AOS-W 8.3.0.7
AOS-192841	—	**Symptom:** The **STM** process crashed on a managed device and the APs were unable to communicate with the managed device. The fix ensures that the managed device works as expected. **Scenario:** This issue was observed in managed devices running AOS-W 8.3.0.1 or later versions.	AP-Platform	All platforms	AOS-W 8.0.0.0
AOS-193046 AOS-196703	—	**Symptom:** Master IP configuration details were missing on the managed device and the managed device acted as a stand-alone switch. 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 devices.	Configuration	All platforms	AOS-W 8.3.0.0
AOS-193188	—	**Symptom:** The **Reclassify Detected Radios** pop-up window displayed action commands for a specific SSID in the **Dashboard > Security > Detected Radios** page of the WebUI. The fix ensures that the action commands are not displayed in the WebUI. **Scenario:** This issue occurred when apostrophe and quotation were added to the ESSID of a stand-alone switch. This issue was observed in OAW-4550 switches running AOS-W 8.4.0.0 or later versions.	WebUI	OAW-4550 switches	AOS-W 8.5.0.1
AOS-193320	—	**Symptom:** Alcatel-Lucent SFP J8177D transceiver did not work with OAW-4450 switches. The fix ensures that the SFP J8177D transceiver works with OAW-4450 switches. **Scenario:** This issue was observed in OAW-4450 switches running AOS-W 8.3.0.7 or later versions.	switch-Platform	OAW-4450 switches	AOS-W 8.3.0.7

Table 6: *Resolved Issues in AOS-W 8.5.0.7*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-193362 AOS-198030	—	**Symptom:** A Mobility Master was unable to establish connection with OmniVista 3600 Air Manager. The fix ensures that the Mobility Master works as expected. **Scenario:** This issue occurred when OmniVista 3600 Air Manager was not reachable from the management interface. This issue was observed in Mobility Master Hardware Appliance running AOS-W 8.3.0.7 or later versions.	switch-Platform	All platforms	AOS-W 8.3.0.7
AOS-193425	—	**Symptom:** GSM entries were missing on the Mobility Master for some wireless users. The fix ensures that the GSM entries are available for the wireless users. **Scenario:** This issue was observed in managed devices running AOS-W 8.3.0.7 or later versions in a cluster setup.	GSM	All platforms	AOS-W 8.3.0.7
AOS-193744 AOS-198906	—	**Symptom:** The **mcell** process was in **PROCESS_NOT_RESPONDING** state after configuring master-redundancy on a Standby Mobility Master. The fix ensures that the process work as expected. **Scenario:** This issue occurred due to connectivity issue between active Mobility Master and the standby Mobility Master. This issue was observed in Mobility Masters running AOS-W 8.5.0.2 or later versions.	AirMatch	All platforms	AOS-W 8.5.0.2
AOS-193888	—	**Symptom:** A few APs rebooted unexpectedly. The fix ensures that the APs work as expected. **Scenario:** This issue occurred when the switch IP address was incorrect in a non-cluster datazone setup. This issue was observed in access points running AOS-W 8.5.0.1 or later versions.	AP Datapath	All platforms	AOS-W 8.5.0.1
AOS-193936 AOS-194470	—	**Symptom:** Some APs continuously display the error message **asap_firewall_forward: br0, insufficient headroom, require 60, but 16, skb data length 60**. The fix ensures that the access points do not display the error message. **Scenario:** This issue is observed in APs running AOS-W 8.3.0.0 or later versions.	AP Datapath	All platforms	AOS-W 8.3.0.0

Table 6: *Resolved Issues in AOS-W 8.5.0.7*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-193976	—	**Symptom:** APs rebooted unexpectedly. The log file listed the reason for the event as **Critical process /aruba/bin/sapd [pid XXXX] DIED, process marked as RESTART**. The fix ensures that the APs work as expected. **Scenario:** This issue occurred when the AP fails over to HA standby. This issue was observed in access points running AOS-W 8.1.0.0 or later versions.	AP-Platform	All platforms	AOS-W 8.5.0.1
AOS-194052	—	**Symptom:** A few clients were unable to obtain IP addresses. The fix ensures that the clients are able to obtain the IP addresses. **Scenario:** This issue occurred when **High Efficiency** was enabled on the WPA2-PSK SSID profile of the APs. This issue was observed in Mobility Controller Virtual Appliances running AOS-W 8.5.0.0 or later versions.	switch-Platform	All platforms	AOS-W 8.5.0.2
AOS-194146	—	**Symptom:** A managed device did not display any warning message when the cluster profile name contained more than 32 characters. The fix ensures that the managed device displays a warning message when the cluster profile name exceeds 32 characters. **Scenario:** This issue was observed in managed devices running AOS-W 8.5.0.2 or later versions in a cluster setup.	Cluster-Manager	All platforms	AOS-W 8.5.0.2
AOS-194201	—	**Symptom:** The value of Tx data bytes transmitted for 5 GHz radio was lesser than the actual transmitted value. The fix ensures that the actual values are transmitted for 5 GHz radio. **Scenario:** This issue was observed in OAW-AP205 access points running AOS-W 8.3.0.0 or later versions.	AP - Wireless	OAW-AP205 access points	AOS-W 8.3.0.0
AOS-194250	—	**Symptom:** The **Configuration > Interfaces > VLANs** page did not display the list of VLANs. The fix ensures that the WebUI displays the list of VLANs configured. **Scenario:** This issue occurred when a new VLAN ID was configured using the WebUI. This issue was observed in managed devices running AOS-W 8.5.0.2 or later versions.	WebUI	All platforms	AOS-W 8.5.0.2

Table 6: *Resolved Issues in AOS-W 8.5.0.7*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-194325 AOS-194579	—	**Symptom:** The **datapath** process in a managed device crashed multiple times. 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 Mobility Master-Managed Device topology.	switch-Datapath	All platforms	AOS-W 8.3.0.7
AOS-194390	—	**Symptom:** The **SAPD** process crashed in a managed device unexpectedly. The log files listed 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**. 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.	AP-Platform	All platforms	AOS-W 8.3.0.8
AOS-194706	—	**Symptom:** A managed device crashed and rebooted unexpectedly. The log files listed the reason for the event as **Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:4)**. The fix ensures that the managed device works as expected. **Scenario:** This issue was observed in managed devices running AOS-W 8.5.0.2 or later versions in a Mobility Master-Managed Device topology.	switch-Datapath	All platforms	AOS-W 8.5.0.2
AOS-194727	—	**Symptom:** An AP sent RTS requests continuously to one client only and this resulted in a delay or packet drop to other clients. The fix ensures that the APs work as expected. **Scenario:** This issue was observed in OAW-AP340 Series access points running AOS-W 8.3.0.7 or later versions.	AP-Wireless	OAW-AP340 Series access points	AOS-W 8.3.0.7
AOS-194785	—	**Symptom:** AP was unable to failover to a backup LMS controller and the AP rebooted with the error, **Unable to set up IPSec tunnel after 24 tries**. The fix ensures that the APs work as expected. **Scenario:** This issue was observed in OAW-AP375 access points connected to stand-alone controllers running AOS-W 8.3.0.8 or later versions.	AP-Platform	OAW-AP375 access points	AOS-W 8.3.0.8

Table 6: *Resolved Issues in AOS-W 8.5.0.7*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-194795 AOS-197097 AOS-201048	—	**Symptom:** Managed Devices did not perform RADIUS authentication. The log file listed the reason for the event as **Failed to send the radius request for Station**. 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.	802.1x	All platforms	AOS-W 8.3.0.0
AOS-194813 AOS-198001 AOS-199579 AOS-200149 AOS-200648 AOS-201658	—	**Symptom:** The **mDNS** process crashed and rebooted on a Mobility Master Virtual Appliance unexpectedly. The fix ensures that the Mobility Master Virtual Appliance works as expected. **Scenario:** This issue occurred due to memory leak. This issue was observed in Mobility Master Virtual Appliance running AOS-W 8.3.0.8 or later versions.	AirGroup	All platforms	AOS-W 8.3.0.8
AOS-194874	—	**Symptom:** High temperature was observed in CPU sensors. The fix ensures that the Mobility Master Hardware Appliance works as expected. **Scenario:** This issue was observed in Mobility Master Hardware Appliances running AOS-W 8.3.0.4 or later versions.	switch-Platform	All platforms	AOS-W 8.3.0.4
AOS-194962	—	**Symptom:** Some clients were unable to connect to the 2.4 GHz radio channel. The fix ensures that the clients can connect to the 2.4 GHz radio channel. **Scenario:** This issue occurred when clients disabled the 2.4 GHz radio and enabled it again, causing the 802.11r SSID profile to get disabled between connections. This issue is observed in APs running AOS-W 8.3.0.0 or later versions.	AP-Platform	All platforms	AOS-W 8.3.0.0
AOS-195000	—	**Symptom:** A few APs crashed unexpectedly. The log files listed the reason for the event as **Kernel panic: softlockup - hung tasks**. The fix ensures that the APs work as expected. **Scenario:** This issue was observed in OAW-AP515 access points running AOS-W 8.5.0.1 or later versions.	AP-Wireless	OAW-AP515 access points	AOS-W 8.5.0.1

Table 6: *Resolved Issues in AOS-W 8.5.0.7*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-195015	—	**Symptom:** An AP crashed and rebooted unexpectedly. The log file listed the reason for this event as **kernel panic: Fatal exception.** The fix ensures that the APs works as expected. **Scenario:** This issue is observed in OAW-AP335 access points running AOS-W 8.3.0.0 or later versions.	AP Datapath	OAW-AP335 access points	AOS-W 8.3.0.0
AOS-195036	—	**Symptom:** The **authentication** 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 8.3.0.0 or later versions.	802.1X	All platforms	AOS-W 8.3.0.6
AOS-195162	—	**Symptom:** The WebUI was unresponsive and the licenses were not visible in the **Mobility Master > Configuration > Licenses** page in the WebUI. The fix ensures that the WebUI is responsive and the licenses are visible. **Scenario:** This issue occurred when 29 non-default pools were configured and enabled. This issue was observed in Mobility Masters running AOS-W 8.5.0.1 or later versions.	Licensing	All platforms	AOS-W 8.5.0.1
AOS-195163 AOS-197980	—	**Symptom:** The **ofc_cli_agent** process in a Mobility Master crashed unexpectedly. The fix ensures that the Mobility Master works as expected. **Scenario:** This issue occurred due to mongo database buffer corruption. This issue was observed in Mobility Masters running AOS-W 8.5.0.4 or later versions.	SDN- Platform	All platforms	AOS-W 8.5.0.4
AOS-195265	—	**Symptom:** A managed device crashed and rebooted unexpectedly. The log files listed the reason for the event as **Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2)**. The fix ensures that the managed device works as expected. **Scenario:** This issue occurred due to ACL corruption. This issue was observed in managed devices running AOS-W 8.5.0.0 or later versions.	SDN	All platforms	AOS-W 8.5.0.3

Table 6: *Resolved Issues in AOS-W 8.5.0.7*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-195271	—	**Symptom:** The **mon_serv_fwv** process crashed unexpectedly. The log file listed the reason for the event as **PROCESS_NOT_RESPONDING_CRITICAL**. The fix ensures that the Mobility Master works as expected. **Scenario:** The issue occurred when the **mDNS** process was restarted in the Mobility Master. This issue was observed in Mobility Master - Managed Device deployment running AOS-W 8.5.0.3 or later versions in a centralized mode.	MON	All platforms	AOS-W 8.5.0.3
AOS-195322 AOS-198279	—	**Symptom:** The authentication module crashed on a managed device. The fix ensures that the managed device works as expected. **Scenario:** This issue occurred due to memory leak. This issue was observed in managed devices running AOS-W 8.3.0.7 or later versions.	Base OS Security	All platforms	AOS-W 8.3.0.7
AOS-195414 AOS-198954	—	**Symptom:** The **profmgr** process crashed on a switch. The fix ensures that the Mobility Master works as expected. **Scenario:** This issue occurs when interface access mode is configured on the Mobility Master. This issue is observed in OAW-4008 switches running AOS-W 8.3.0.10 or later versions.	Configuration	OAW-4008 switches	AOS-W 8.3.0.10
AOS-195444	—	**Symptom:** A managed device crashed and rebooted unexpectedly. The log file listed the reason for the event as **Datapath timeout (Fpapps Initiated) (Intent:cause:register 51:86:50:60)**. The fix ensures that the managed device works as expected. **Scenario:** This issue occurred due to high CPU utilization. This issue was observed in managed devices running AOS-W 8.5.0.1 or later versions.	switch-Datapath	All platforms	AOS-W 8.5.0.1
AOS-195525	—	**Symptom:** A few managed devices that were visible in the **Services > Clusters** page in the WebUI were not visible when the upgrade cluster task is performed using **Configuration > Tasks > Upgrade Cluster** page. The fix ensures that the WebUI displays the managed devices in the **Configuration > Tasks > Upgrade Cluster** page. **Scenario:** This issue was observed in managed devices running AOS-W 8.5.0.3 or later versions.	Cluster Manager	All platforms	AOS-W 8.5.0.3

Table 6: *Resolved Issues in AOS-W 8.5.0.7*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-195546 AOS-199490 AOS-199985	—	**Symptom:** Memory leak was observed in mDNS process. The fix ensures that the managed devices work as expected. **Scenario:** This issue occurred when AirGroup was enabled in distributed mode. This issue was observed in managed devices running AOS-W 8.5.0.5 or later versions.	AirGroup	All platforms	AOS-W 8.5.0.5
AOS-195589 AOS-196087 AOS-197914	—	**Symptom: Profmgr** process crashed unexpectedly in a Mobility Master. The fix ensures that the Mobility Master works as expected. **Scenario:** This issue occurred when the VLAN commands entered exceeded 256 characters. This issue is observed in Mobility Masters running AOS-W 8.3.0.4 or later versions in a cluster-setup.	Configuration	All platforms	AOS-W 8.3.0.4
AOS-195600	—	**Symptom:** Users were unable to discover Apple TV. The fix ensures that users are able to discover Apple TV. **Scenario:** The issue occurred because AirGroup MDNS packet sessions were flagged with 'o' flags during a Skype call initiation by UCC when AirGroup was enabled in Centralized mode. This issue was observed in the Mobility Masters running AOS-W 8.3.0.8 or later versions. **Duplicates:** AOS-197877, AOS-199006, AOS-199741, AOS-199284, AOS-200095, AOS-200188, and AOS-200406	SDN-Platform	All platforms	AOS-W 8.3.0.8
AOS-195677 AOS-196311	—	**Symptom:** The **airmatch_recv** process crashed unexpectedly in a Mobility Master. The fix ensures that the Mobility Master works as expected. **Scenario:** This issue was observed in Mobility Masters running AOS-W 8.3.0.0 or later versions in a Mobility Master-Managed Device topology.	AirMatch	All platforms	AOS-W 8.3.0.7
AOS-195688	—	**Symptom:** Some APs frequently detected wrong radars in a high density deployment. Enhancements to the wireless driver resolved this issue. **Scenario:** The issue was observed only on JP3 regulatory domain. This issue was observed in OAW-AP325 access points running AOS-W 8.3.0.0 or later versions.	AP-Wireless	OAW-AP325 access points	AOS-W 8.3.0.0

Table 6: *Resolved Issues in AOS-W 8.5.0.7*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-195749 AOS-195940 AOS-199401 AOS-200278	—	**Symptom:** The **mDNS** module crashed on a Mobility Master. The fix ensures that the Mobility Master works as expected. **Scenario:** This issue was observed in Mobility Masters running AOS-W 8.5.0.3 or later versions.	AirGroup	All platforms	AOS-W 8.5.0.3
AOS-195789	—	**Symptom:** An AP reported high channel usage on 5Ghz radio. The fix ensures that the access points work as expected. **Scenario:** This issue occurred due to a configuration error. This issue was observed in OAW-AP377 access points running AOS-W 8.4.0.1 or later versions.	AP - Wireless	OAW-AP377 access points	AOS-W 8.4.0.1
AOS-195835	—	**Symptom:** The CLI command **firewall attack-rate arp** did not allow the users to configure attack rate with any value higher than 1024. The fix ensures that users can configure any value between 1-16384. **Scenario:** This issue was observed in managed devices running AOS-W 8.4.0.4 or later versions.	switch-Datapath	All platforms	AOS-W 8.4.0.4
AOS-195839	—	**Symptom:** A VIA client could not auto-upgrade. The fix ensures that the auto-upgrade feature works as expected. **Scenario:** This issue occurred when the VIA client was terminated to a Virtual OmniAccess Mobility Controller. This issue was observed in managed devices running AOS-W 8.0.0.0 or later versions.	VRRP	All platforms	AOS-W 8.3.0.0
AOS-195968	—	**Symptom:** OAW-RAPs could not connect to the managed device after a failover. The fix ensures that the OAW-RAPs are able to connect to the managed device seamlessly. **Scenario:** This issue occurred when PSK authentication was used to provision a OAW-RAP. This issue was observed in managed devices running AOS-W 8.3.0.8 or later versions.	AP-Platform	All platforms	AOS-W 8.3.0.8

Table 6: *Resolved Issues in AOS-W 8.5.0.7*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-196043	—	**Symptom:** A mismatch of 802.11r configuration was observed between a Mobility Master and the managed devices, as well as between the WebUI and the CLI in a cluster. The fix ensures that 802.11r configuration is consistent across the Mobility Master and managed devices. **Scenario:** This issue occurred because 802.11r was not supported in split-tunnel forwarding mode. This issue was observed in Mobility Masters and managed devices running AOS-W 8.2.0.0 or later versions.	AP-Platform	All platforms	AOS-W 8.4.0.4
AOS-196101 AOS-197335	—	**Symptom:** Access points crashed and rebooted unexpectedly. The log file listed the reason for the event as **external watchdog reset.** The fix ensures that the access points work as expected. **Scenario:** This issue was observed in OAW-AP203H access points running AOS-W 8.3.0.10 or later versions.	AP-Platform	OAW-AP203H access points	AOS-W 8.3.0.10
AOS-196176 AOS-196945	—	**Symptom:** The **Dashboard > Security** page didn't load the **Detected Radios** and displayed the error message, **Error retrieving information. Please try again later.** The fix ensures that the WebUI displays the list of detected radios. **Scenario:** This issue was observed in Mobility Masters running AOS-W 8.5.0.4 or later versions.	WebUI	All platforms	AOS-W 8.5.0.4
AOS-196215 AOS-199712	—	**Symptom:** Some clients were unable to manage multiple clusters using a single Mobility Master. The fix ensures that the Mobility Master works as expected. **Scenario:** This issue occurred when the Mobility Master assumed that the clusters are on the same VLAN and cannot reuse the same VRRP ID in the cluster profile. This issue was observed in Mobility Masters running AOS-W 8.5.0.3 or later versions.	Cluster-Manager	All platforms	AOS-W 8.5.0.3
AOS-196231	—	**Symptom:** AirGroup clients trying to access Airplay services were unable to discover the AirGroup servers. The fix ensures that the clients are able to discover the AirGroup servers. **Scenario:** This issue occurred when the **Auto Associate** feature was enabled. This issue was observed in Mobility Masters running AOS-W 8.5.0.3 or later versions.	AirGroup	All platforms	AOS-W 8.5.0.3

Table 6: *Resolved Issues in AOS-W 8.5.0.7*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-196312 AOS-199450 AOS-199937 AOS-200235	—	**Symptom:** Access points were unable to connect to a cluster. The fix ensures that the **ap_move** flag is cleared after the **apmove** command is executed. **Scenario:** This issue occurred because the **ap_move** flag was not cleared after the **apmove** command. 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 8.3.0.0
AOS-196315	—	**Symptom:** The status of the managed devices constantly flapped after upgrading the Mobility Master. This issue is resolved by enabling multiversion support for OAW-4850 switches. **Scenario:** This issue occurred when multiversion support was not enabled on OAW-4850 switches. This issue was observed in OAW-4850 switches running AOS-W 8.5.0.3 or later versions.	Configuration	OAW-4850 switches	AOS-W 8.5.0.3
AOS-196325 AOS-200875	—	**Symptom:** Mobility Master rebooted unexpectedly. The fix ensures that the Mobility Master works as expected. **Scenario:** This issue occurred due to high memory consumption. This issue was observed in Mobility Masters running AOS-W 8.5.0.2 or later versions.	UCC	All platforms	AOS-W 8.5.0.2
AOS-196455 AOS-198499 AOS-200025	—	**Symptom:** Mobility Master sent incorrect AP regulatory-domain-profile channel changes to the managed device during the initial configuration propagation. The fix ensures that the Mobility Masters work as expected. **Scenario:** This issue was observed in Mobility Masters running AOS-W 8.0.0.0 or later versions.	Configuration	All platforms	AOS-W 8.5.0.4
AOS-196479	—	**Symptom:** Managed devices dropped bcast or mcast traffic on VLANs randomly. The fix ensures that the bcast or mcast traffic is not dropped. **Scenario:** This issue occurred because the clients were not getting IP addresses. This issue was observed in managed devices running AOS-W 8.2.0.0 or later versions.	VLAN	All platforms	AOS-W 8.3.0.6

Table 6: *Resolved Issues in AOS-W 8.5.0.7*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-196489 AOS-199172	—	**Symptom:** GSM entries for AirGroup servers were not updated when MAC authenticated clients moved between APs. The fix ensures that the GSM entries are updated with new bssid of the APs. **Scenario:** This issue was observed in managed devices running AOS-W 8.6.0.0 or later versions.	Base OS Security	All platforms	AOS-W 8.6.0.0
AOS-196499	—	**Symptom:** An access point rebooted multiple times. The fix ensures that the access point works as expected. **Scenario:** This issue was observed in OAW-AP535 access points running AOS-W 8.5.0.3 or later versions.	AP-Wireless	OAW-AP535 access points	AOS-W 8.5.0.3
AOS-196528	—	**Symptom:** Users were unable to remove port-channel using the **no port monitor port-channel** command and CLI displayed the error message, **Illegal operation: port-channel not being monitored.** The fix ensures that the users are able to remove port-channel from port monitor. **Scenario:** This issue was observed in managed devices running AOS-W 8.0.0.0 or later versions.	Interface	All platforms	AOS-W 8.5.0.2
AOS-196629	—	**Symptom:** When the **show switches** command was executed, the value of the **Configuration State** parameter was displayed as **LAST SNAPSHOT** for some managed devices. The fix ensures that the managed devices work as expected. **Scenario:** This issue occurred when a legacy master switch was successfully upgraded to AOS-W 8.6.0.2. This issue was observed in OAW-4850 and OAW-4104 managed devices running AOS-W 8.4.0.0 and AOS-W 8.5.0.0, or later versions.	Configuration	OAW-4850 and OAW-4104 managed devices	AOS-W 8.6.0.2
AOS-196678	—	**Symptom:** APs did not generate wireless containment frames and IDS protection was not applied. Hence, clients were not deauthenticated from non-valid APs. The fix ensures that the APs generate wireless containment frames and clients are deauthenticated from non-valid APs. **Scenario:** This issue occurred when the radio operated in AM mode. 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 8.5.0.2

Table 6: *Resolved Issues in AOS-W 8.5.0.7*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-196683	—	**Symptom:** Access points came up without standby APs. The fix ensures that the APs work as expected. **Scenario:** This issue occurred in a cluster when AP channel scanning detected an invalid AP and skipped scanning the remaining APs. This issue was observed in access points running AOS-W 8.5.0.3 or later versions.	Cluster-Manager	All platforms	AOS-W 8.5.0.3
AOS-196728	—	**Symptom:** A Mobility Master Virtual Appliance crashed unexpectedly. The fix ensures that the Mobility Master Virtual Appliance works as expected. **Scenario:** This issue was observed in Mobility Master Virtual Appliances AOS-W 8.3.0.0 or later versions in a cluster setup.	Cluster Manager	All platforms	AOS-W 8.3.0.8
AOS-196788	—	**Symptom:** The **OFA** process crashed unexpectedly. The fix ensures that the managed device works as expected. **Scenario:** This issue occurred due to frequent reboot of APs. This issue was observed in managed devices running AOS-W 8.4.0.4 or later versions.	SDN-Platform	All platforms	AOS-W 8.4.0.4
AOS-196805	—	**Symptom:** The command **show ap debug client-stats** displayed lower rates for management frames. The fix ensures that the rate used for management and control frames like RTS are not lower than the minimum basic rate set in the ssid-profile. **Scenario:** This issue was observed in APs running AOS-W 8.3.0.6 or later versions.	AP-Wireless	All platforms	AOS-W 8.3.0.6
AOS-196847 AOS-196941 AOS-198485 AOS-201783	—	**Symptom:** The **Dashboard > Infrastructure > Controller** page did not display the list of available switches. The fix ensures that the WebUI displays the list of switches. **Scenario:** This issue was observed in Mobility Masters running AOS-W 8.5.0.3 or later versions.	WebUI	All platforms	AOS-W 8.5.0.3
AOS-196852	—	**Symptom:** Access points crashed and rebooted unexpectedly. The fix ensures that the access points work as expected. **Scenario:** This issue was observed in access points running AOS-W 8.4.0.4 or later versions.	AP Datapath	All platforms	AOS-W 8.4.0.4

Table 6: *Resolved Issues in AOS-W 8.5.0.7*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-196879	—	**Symptom:** APs crashed unexpectedly. The log file listed the reason for the event as **PC is at aruba_am_tx_pkt_handler_data_ol.** The fix ensures that the APs work as expected. **Scenario:** This issue occurred after upgrading the APs to AOS-W 8.3.0.10. This issue was observed in OAW-AP315 access points running AOS-W 8.3.0.10 or later versions.	AP - Wireless	OAW-AP315 access points	AOS-W 8.3.0.10
AOS-196881	—	**Symptom:** Server configuration rules were not pushed to the managed devices. The fix ensures that the managed devices work as expected. **Scenario:** This issue was observed in managed devices running AOS-W 8.3.0.7 or later versions.	Base OS Security	All platforms	AOS-W 8.3.0.7
AOS-196887 AOS-196959	—	**Symptom:** WPA3-SAE-AES Opmode enabled clients were unable to connect to the AP and the AP sent **Deauthentication Reason Code: 49 Invalid pairwise masterkey identifier (PMKI) [24-25]** deauthentication code. The fix ensures that the access point works as expected. **Scenario:** This issue was observed in access points running AOS-W 8.5.0.5 or later versions in a cluster setup.	Base OS Security	All platforms	AOS-W 8.5.0.5
AOS-196896 AOS-197050 AOS-200076 AOS-200077	—	**Symptom:** APs crashed and rebooted unexpectedly. The fix ensures that the access points work as expected. **Scenario:** This issue occurred during the stm process crash when more than 256 clients connected to a OAW-RAP or OAW-AP on bridge mode got deleted. This issue was observed in OAW-AP325 access points running AOS-W 8.5.0.3 or later versions.	Station Management	OAW-AP325 access points	AOS-W 8.5.0.3
AOS-196911	—	**Symptom:** Users were unable to connect to APs. Enhancement to the wireless driver fixed the issue. **Scenario:** This issue was observed in OAW-AP555 access points running AOS-W 8.5.0.4 or later versions.	AP Datapath	OAW-AP555 access points	AOS-W 8.5.0.4

Table 6: *Resolved Issues in AOS-W 8.5.0.7*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-196928 AOS-196066 AOS-196943 AOS-197742 AOS-198048 AOS-198328 AOS-198682 AOS-199156	—	**Symptom:** Users were unable to discover the wired AirGroup server and experienced packet drops when a UCC Skype call was initiated. The fix ensures that the users are able to discover the wired AirGroup servers. **Scenario:** This issue occurred when AirGroup was enabled in centralized mode. This issue was observed in Mobility Masters running AOS-W 8.5.0.3 or later versions.	SDN-Platform	All platforms	AOS-W 8.5.0.3
AOS-197122	—	**Symptom:** Managed devices did not send SNMPv3 information to OmniVista 3600 Air Manager. The fix ensures that the managed devices send the SNMPv3 information to OmniVista 3600 Air Manager. **Scenario:** This issue was observed in managed devices running AOS-W 8.3.0.6 or later versions.	SNMP	All platforms	AOS-W 8.3.0.6
AOS-197160 AOS-198571 AOS-200427 AOS-201607	—	**Symptom:** Managed devices crashed and rebooted unexpectedly. The log file 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 device works as expected. **Scenario:** This issue occurred due to corrupt ACL entries. This issue was observed in managed devices running AOS-W 8.3.0.8 in a cluster-setup.	SDN-Platform	All platforms	AOS-W 8.3.0.8
AOS-197262	—	**Symptom:** The command **show crashinfo** did not display the crash information even when the crash symbol was displayed. The fix ensures that the **show crashinfo** command displays the crash information. **Scenario:** This issue was observed in managed devices running AOS-W 8.2.2.6 or later versions.	switch-Platform	All platforms	AOS-W 8.2.2.6

Table 6: *Resolved Issues in AOS-W 8.5.0.7*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-197310	—	**Symptom:** WebUI did not list the available cluster profiles in the **Configuration > Services > Cluster > Cluster group-membership** drop-down list. The fix ensures that the WebUI lists the available cluster profiles. **Scenario:** This issue was observed in managed devices running AOS-W 8.3.0.5 or later versions in a cluster setup.	WebUI	All platforms	AOS-W 8.3.0.5
AOS-197393 AOS-200407	—	**Symptom:** Radios experienced high number of resets and packet drops were also observed on APs. The fix ensures that the APs work as expected. **Scenario:** This issue was observed in OAW-AP340 Series access points running AOS-W 8.5.0.5 or later versions.	AP-Wireless	OAW-AP340 Series access points	AOS-W 8.5.0.5
AOS-197536 AOS-198286 AOS-200371	—	**Symptom:** Many clients got disconnected from APs. The fix ensures seamless connectivity. **Scenario:** This issue occurred when a new VLAN was added. This issue was observed in access points running AOS-W 8.3.0.0 or later versions.	Station Management	All platforms	AOS-W 8.5.0.0
AOS-197939 AOS-198087	—	**Symptom:** After configuring the heartbeat threshold in the WebUI, the VRRP IDs got reset to the default values. The fix ensures that the VRRP Ids are not reset to the default values. **Scenario:** This issue was observed in Mobility Masters running AOS-W 8.5.0.3 or later versions.	WebUI	All platforms	AOS-W 8.5.0.3
AOS-197977 AOS-198348 AOS-198349	—	**Symptom:** High memory consumption was observed in **dot1x1** and **dot1x2** processes. The fix ensures dot1x1 and dot1x2 process do not consume high memory. **Scenario:** This issue occurred due to memory leak when the EAP-fragmentation feature was enabled. This issue was observed in Mobility Masters running AOS-W 8.4.0.0 or later versions.	802.1X	All platforms	AOS-W 8.5.0.1
AOS-197993 AOS-198889	—	**Symptom:** A managed device crashed unexpectedly and high CPU utilization was also observed on the managed device. The fix ensures that the managed device works as expected. **Scenario:** This issue was observed in managed devices running AOS-W 8.5.0.1 or later versions.	switch-Datapath	All platforms	AOS-W 8.5.0.1

Table 6: *Resolved Issues in AOS-W 8.5.0.7*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-198003	—	**Symptom:** Network firewall dropped fragmented packets and hence clients faced connectivity issues. The fix ensures seamless connectivity. **Scenario:** This issue was 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-198110	—	**Symptom:** The command **configuration device move to** displayed the error message, **trusted Illegal Operation: There is Session ACL Defined. Cannot make the port untrusted.** The fix ensures that the command works as expected. **Scenario:** This issue occurred when the **trusted** command was executed before and after configuring the session ACL. This issue was observed in Mobility Masters running AOS-W 8.3.0.9 or later versions.	L2 Forwarding	All platforms	AOS-W 8.3.0.9
AOS-198112	—	**Symptom:** WebUI displayed an error message **Invalid IPv4** when users tried to configure OmniVista 3600 Air Manager IPv6 address under **Configuration > System > AirWave** in the Mobility Master node hierarchy. The fix ensures that the OmniVista 3600 Air Manager IPv6 address can be configured using the WebUI **Scenario:** This issue was observed in Mobility Masters running AOS-W 8.5.0.3 or later versions.	WebUI	All platforms	AOS-W 8.5.0.3
AOS-198290 AOS-198836	—	**Symptom:** The **show ip interface brief** command displayed incorrect radio channel information for AAC and non S-AAC managed devices. The fix ensures that the command works as expected. **Scenario:** This issue was observed in managed devices running AOS-W 8.3.0.10 or later versions.	Station Management	All platforms	AOS-W 8.3.0.10
AOS-198370	—	**Symptom:** The **Managed network > Configuration > Task > Bulk configuration upload** page displayed an error message, **Incorrect header field(Controller VLAN)** while uploading the bulk edit configuration. The fix ensures that the WebUI does not display the error message. **Scenario:** This issue was observed in Mobility Masters running AOS-W 8.5.0.5 or later versions.	switch-Datapath	All platforms	AOS-W 8.5.0.5

Table 6: *Resolved Issues in AOS-W 8.5.0.7*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-198669 AOS-198885	—	**Symptom:** All rules configured using **aaa server-group** command were displayed in lowercase. The fix ensures that the rules are displayed in the correct letter cases. **Scenario:** This issue was observed in Mobility Masters running AOS-W 8.5.0.3 or later versions.	Role/VLAN Derivation	All platforms	AOS-W 8.5.0.3
AOS-198670	—	**Symptom:** Forward slash **[/]** did not search for the next hit in CLI output. The fix ensures that the forward slash searches for the next hit in CLI output. **Scenario:** This issue was observed in managed devices running AOS-W 8.0.0.0 or later versions.	CLI	All platforms	AOS-W 8.3.0.8
AOS-198699	—	**Symptom:** Zero Touch Provisioning feature did not work on Huawei 4G dongle with model number E3372h-607. The fix ensures that ZTP works on the modem. **Scenario:** This issue was observed in OAW-4005 switches running AOS-W 8.5.0.0 or later versions.	switch-Platform	OAW-4005 switches	AOS-W 8.5.0.0
AOS-198738	—	**Symptom:** Users were unable to access CLI using SSH. The fix ensures that the users can access CLI using SSH. **Scenario:** This issue occurred in an IPv6 network when the multicast packets were not sent to the Mobility Master Virtual Appliance. This issue was observed in Mobility Master Virtual Appliance running AOS-W 8.5.0.1 or later versions.	switch-Datapath	All platforms	AOS-W 8.5.0.1
AOS-198741	—	**Symptom:** Users were unable to configure IPsec tunnels on a few third party VPN peers and the switch sent the error message, **INVALID SYNTAX.** The fix ensures that the users are able to configure IPsec tunnels. **Scenario:** This issue occurred when the third party VPN peers propose IKEV2_FRAGMENTATION_SUPPORTED notify payload but did not send the IKE_AUTH payload as fragments. This issue was observed in stand-alone switches running AOS-W 8.5.0.4 or later versions.	IPSec	All platforms	AOS-W 8.5.0.4
AOS-198743	—	**Symptom:** A few IPv6 enabled OAW-RAPs rebooted unexpectedly. The fix ensures that the APs work as expected. **Scenario:** This issue occurred when the Mobility Master was configured with VRRP IP. This issue was observed in OAW-RAPs running AOS-W 8.5.0.5 or later versions.	OAW-RAP	All platforms	AOS-W 8.5.0.5

Table 6: *Resolved Issues in AOS-W 8.5.0.7*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-198828	—	**Symptom:** Access points did not send temperature values to the server. The fix ensures that the access points work as expected. **Scenario:** This issue occurred when the APs did not properly relay RTLS Aeroscout tag to the server. This issue was observed in OAW-AP535 and OAW-AP555 access points running AOS-W 8.5.0.4 or later versions.	AP - Wireless	OAW-AP535 and OAW-AP555 access points	AOS-W 8.5.0.4
AOS-199217 AOS-199709	—	**Symptom:** Cluster heartbeats were randomly missed on managed devices. The fix ensures that the managed devices work as expected. **Scenario:** This issue was observed in managed devices running AOS-W 8.3.0.10 or later versions in a cluster setup.	Cluster-Manager	All platforms	AOS-W 8.3.0.10
AOS-199237	—	**Symptom:** Users were unable to establish connection with a managed device using the **mdconnect** and **logon** commands. The fix ensures that the commands work as expected. **Scenario:** This issue occurred when master-ssh-pub-certificate was not downloaded during the initial boot-up after ZTP. This issue was observed in managed devices running AOS-W 8.5.0.5 or later versions.	Certificate Manager	All platforms	AOS-W 8.5.0.5
AOS-199696	—	**Symptom:** Managed devices failed to establish connection with **IF-MAP** enabled ClearPass Policy Manager. The fix ensures that the managed devices work as expected. **Scenario:** This issue occurred when same certificates were added using different names. This issue was observed in managed devices running AOS-W 8.5.0.5 or later versions.	Certificate Manager	All platforms	AOS-W 8.5.0.5
AOS-199707	—	**Symptom:** A managed device crashed and rebooted unexpectedly. The log file listed the reason for the event as **Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:0:20.** The fix ensures that the managed device works as expected. **Scenario:** This issue was observed in managed devices running AOS-W 8.6.0.0 or later versions.	switch-Datapath	All platforms	AOS-W 8.6.0.0
AOS-199667 AOS-199736	—	**Symptom:** The system was unresponsive when the **show tech-support** command was executed. The fix ensures that the command works as expected. **Scenario:** This issue occurred when the **show datapath dhcp binding** command duplicated the output entries. 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

Table 6: *Resolved Issues in AOS-W 8.5.0.7*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-199739 AOS-201390	—	**Symptom:** A managed device crashed and rebooted unexpectedly. The log file 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 device works as expected. **Scenario:** This issue occurred after upgrading the managed device to AOS-W 8.6.0.2 version. This issue was observed in managed devices running AOS-W 8.6.0.2 or later versions.	switch-Datapath	All platforms	AOS-W 8.6.0.2
AOS-200102 AOS-200779	—	**Symptom:** Clients took a long time to failover to another managed device in a cluster. The fix ensures that the clients failover seamlessly. **Scenario:** This issue was observed in managed devices running AOS-W 8.5.0.0 or later versions in a cluster setup.	AP Datapath	All platforms	AOS-W 8.5.0.5
AOS-200146	—	**Symptom:** The **STM** process on an AP crashed. The fix ensures that the access point works as expected. **Scenario:** This issue was observed in OAW-AP535 access points running AOS-W 8.4.0.0 or later versions.	Station Management	OAW-AP535 access points	AOS-W 8.6.0.0
AOS-200165	—	**Symptom:** APs crashed and rebooted unexpectedly. The log file listed the reason for the event as **rebooted caused by BadPtr:00000010 PC:aruba_periodic_measurements+0x1b10/0x2748 [wl_v6] Warm-reset**. The fix ensures that the APs work as expected. **Scenario:** This issue was observed in OAW-AP515 access points running AOS-W 8.5.0.6 or later versions.	AP-Wireless	OAW-AP515 access points	AOS-W 8.5.0.6
AOS-200420	—	**Symptom:** Data traffic from VPNC concentrator was not routed back to the managed device. The fix ensures that the managed device works as expected. **Scenario:** This issue occurred when the managed device was provisioned with two uplinks. This issue was observed in branch office switches running AOS-W 8.5.0.5 or later versions.	IPsec	All platforms	AOS-W 8.5.0.5
AOS-200002 AOS-200649	—	**Symptom:** A managed device crashed and rebooted unexpectedly. The log file listed the reason for the event as **crashed and rebooted due to Datapath timeout (Heartbeat Initiated) (Intent:cause:register 53:86:0:2c)**. The fix ensures that the managed device works as expected. **Scenario:** This issue occurred due to high CPU utilization. This issue was observed in managed devices running AOS-W 8.5.0.5 or later versions.	switch-Datapath	All platforms	AOS-W 8.5.0.5

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

	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.

	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 8.5.0.7*

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
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

Table 7: *Known Issues in AOS-W 8.5.0.7*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
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
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 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

Table 7: *Known Issues in AOS-W 8.5.0.7*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
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 or later versions. **Workaround:** None.	IPsec	OAW-AP315 access points	AOS-W 8.3.0.5
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-183317 AOS-186033	—	**Symptom:** An AP detects multiple false radars on channel 100, with type ID 255. **Scenario:** This issue is observed in OAW-AP530 Series access points running AOS-W 8.5.0.0 or later versions. **Workaround:** None.	AP - Wireless	OAW-AP530 Series access points	AOS-W 8.5.0.0

Table 7: *Known Issues in AOS-W 8.5.0.7*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
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
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

Table 7: *Known Issues in AOS-W 8.5.0.7*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
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
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-187614 AOS-197718	—	**Symptom:** A few APs crash and reboot unexpectedly. The log files list the reason for the event as **kernel panic: Fatal exception in interrupt.** **Scenario:** This issue is observed in OAW-AP515 access points running AOS-W 8.5.0.4 or later versions in a Mobility Master-Managed Device topology. **Workaround:** None.	AP-Wireless	OAW-AP515 access points	AOS-W 8.5.0.4

Table 7: *Known Issues in AOS-W 8.5.0.7*

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-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-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 8.5.0.7*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
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-188793	—	**Symptom:** The output of the **show audit-trail** command displays incorrect message of the **BOCMGR process** in a Mobility Master. **Scenario:** This issue occurs when the Mobility Master connects to the Activate server. This issue is observed in Mobility Masters running AOS-W 8.2.2.3 or later versions. **Workaround:** None.	Configuration	All platforms	AOS-W 8.2.2.3
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 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 8.5.0.7*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
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
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 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-191783	—	**Symptom:** Some users experience SIP call drops. **Scenario:** This issue occurs when the DNS traffic to DNS server gets stalled instead of forwarding it to VPN tunnel. 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-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 8.5.0.7*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
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
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

Table 7: *Known Issues in AOS-W 8.5.0.7*

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-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
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-4650switches	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

Table 7: *Known Issues in AOS-W 8.5.0.7*

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-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
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-196864	—	**Symptom:** Adding a new VLAN ID connects L3 but displays that the connected 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 module 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 8.5.0.7*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-196970	—	**Symptom:** A few APs stop responding to data frames and cannot decode BA packets from the STAs causing packet drop. **Scenario:** This issue is observed in OAW-AP535 access points running AOS-W 8.5.0.0 or later versions. **Workaround:** None.	AP - Wireless	OAW-AP535 access points	AOS-W 8.5.0.0
AOS-193761	—	**Symptom:** The output of **show airmatch debug solution list-all** command does not display the AP name. **Scenario:** This issue is observed in managed devices running AOS-W 8.6.0.0 or later versions. **Workaround:** None.	AirMatch	All platforms	AOS-W 8.6.0.0
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, 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.	WebUI	All platforms	AOS-W 8.5.0.4
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
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

Table 7: *Known Issues in AOS-W 8.5.0.7*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
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-198218	—	**Symptom:** After reboot, 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
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-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-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

Table 7: *Known Issues in AOS-W 8.5.0.7*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-200319	—	**Symptom:** APs crash and reboot unexpectedly. The log file lists the reason for the event as **Kernel panic: WLAN FW crashes with Assertion vdev_handle->type == WAL_VDEV_TYPE_STA failed.** **Scenario:** This issue is observed in OAW-AP535 and OAW-AP555 access points running AOS-W 8.5.0.7. **Workaround:** None.	AP - Wireless	OAW-AP535 and OAW-AP555 access points	AOS-W 8.5.0.7
AOS-200442	—	**Symptom:** APs crash and reboot unexpectedly. The log file lists the reason for the event as **WLAN FW Crash at ar_wal_peer.c:7218 Assertion !CHK_TID_FLG(ptid, WAL_TID_IN_SCHEDQ) failed.** **Scenario:** This issue is observed in OAW-AP535 access points running AOS-W 8.5.0.7. **Workaround:** None.	AP - Wireless	OAW-AP535 access points	AOS-W 8.5.0.7
AOS-201449	—	**Symptom:** When the managed devices are upgraded, **C_ArubaOS_72xx_8.5.0.7_74601** is displayed as the file version name. **Scenario:** This issue is not limited to any specific platform or AOS-W version **Workaround:** Copy images on the image server with file name starting with **C_** before upgrading to the latest AOS-W version.	Image Upgrade	All platforms	AOS-W 8.5.0.7
AOS-201171	—	**Symptom:** An APs is unable to receive IPv6 address from IPv6 RA. **Scenario:** This issue occurs when large number of clients are associated to APs and when aggressive power saving transitions are observed on the associated clients. This issue is observed in access points AOS-W 8.5.0.7. **Workaround:** Do not configure static IPv4 addresses for LACP enabled APs..	AP - Wireless	All platforms	AOS-W 8.5.0.7
AOS-201463	—	**Symptom:** Clients are unable to receive traffic from APs. **Scenario:** This issue occurs when static IPv4 addresses are configured on LACP enabled APs. This issue is observed in access points running AOS-W 8.5.0.7. **Workaround:** None.	AP Datapath	All platforms	AOS-W 8.5.0.7

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 63 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 63 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 63 to copy the **logs.tar** files to an external server. Execute the **tar clean logs** command to delete the file from the managed device.

> In certain situations, a reboot or a shutdown could cause the managed device to lose the information stored in its flash memory. To avoid such issues, it is recommended that you execute the **halt** command before power cycling.

Deleting a File

You can delete a file using the WebUI or 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 <u>Memory Requirements on page 62</u>.

> 📝 **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 62 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 63 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 63.
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.