AOS-W 8.6.0.17 Release Notes

Copyright Information

Open Source Code

This product includes code licensed under the GNU General Public License, the GNU Lesser General Public License, and/or certain other open source licenses.

Contents

Contents 3

Revision History 4

Release Overview 5
- Related Documents 5
- Supported Browsers 5
- Terminology Change 5

Contacting Support 6

New Features and Enhancements in AOS-W 8.6.0.17 7
- CLI 7
- Regulation of Core Dump Files 9

Supported Platforms in AOS-W 8.6.0.17 10
- Mobility Master Platforms 10
- OmniAccess Mobility Controller Platforms 10
- AP Platforms 10

Regulatory Updates in AOS-W 8.6.0.17 13

Resolved Issues in AOS-W 8.6.0.17 14

Known Issues in AOS-W 8.6.0.17 34
- Limitation 34
- Known Issues 34

Upgrade Procedure 49
- Important Points to Remember 49
- Memory Requirements 49
- Backing up Critical Data 50
- Upgrading AOS-W 51
- Verifying the AOS-W Upgrade 53
- Downgrading AOS-W 53
- Before Calling Technical Support 55

Chapter 1
Revision History

The following table provides the revision history of this document.

Table 1: *Revision History*

Revision	Change Description
Revision 03	Updated the **New Features and Enhancements in AOS-W 8.6.0.17** section.
Revision 02	**AOS-208351** was added to the list of **Resolved Issues in AOS-W 8.6.0.17** section.
Revision 01	Initial release.

Chapter 2
Release Overview

This AOS-W release notes includes the following topics:

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

For a list of terms, refer Glossary.

Related Documents

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

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

Supported Browsers

The following browsers are officially supported for use with the AOS-W WebUI:

- Microsoft Internet Explorer 11 on Windows 7 and Windows 8
- Microsoft Edge (Microsoft Edge 38.14393.0.0 and Microsoft EdgeHTML 14.14393) on Windows 10
- Mozilla Firefox 48 or later on Windows 7, Windows 8, Windows 10, and macOS
- Apple Safari 9.0 or later on macOS
- Google Chrome 67 on Windows 7, Windows 8, Windows 10, and macOS

Terminology Change

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

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

Contacting Support

Table 2: *Contact Information*

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

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

CLI

Starting from AOS-W 8.6.0.17, the following CLI commands have been enhanced:

apflash command

The **ap31x-ap32x backup partition** parameter has been added to the **apflash** command to upgrade the backup partition of Alcatel-Lucent OAW-AP310 Series and 320 Series access points running AOS-W 6.4.x or earlier versions to the AOS-W version running on the Mobility Master.

```
(host) [mynode] #apflash ap31x-ap32x backup partition
```

clear command

The **iap statistics**, **iap branch-stats**, and **iap subnet-stats** parameters have been added to the **clear** command to clear the specified parameters of their current values.

```
(host) [mynode] #clear iap stattistics
(host) [mynode] #clear iap branch-key
(host) [mynode] #clear iap subnet-stats
```

cluster-debug command

The **bucketmap rebalance** parameter has been added to the **cluser-debug** command to evenly re-balance bucketmap distribution based on the cluster node's platform capacity.

```
(host) [mynode] (config) # cluster-debug bucketmap rebalance
```

firewall

The **deny-needfrag-df-ipsec** parameter has been added to the **firewall** command to drop IP packets with DF bit set when packet length is greater than IPsec tunnel MTU and an ICMP error message is sent. If this parameter is disabled, the IP packets will be fragmented after encryption and will not be dropped.

```
(host) [mynode] (config) # firewall deny-needfrag-df-ipsec
```

firewall-visibility command

The **feed sort-by-bssid** parameter has been added to the **firewall-visibility** command to enable sorting of firewall visibility sessions based on the BSSID. When you enable this feature, the **Firewall Monitoring** page on the **Dashboard** tab of the WebUI displays the summary of all sessions in the switch aggregated by BSSIDs.

```
(host) [mynode] (config) # firewall-visibility feed sort-by-bssid
```

show ap debug command

The **client-kickout-logs** parameter has been added to the **show ap debug** command to display the reasons why clients got deauthenticated due to consecutive TX failures.

```
(host) [mynode] (config) # show ap debug client-kickout-logs ap-name AP535 radio 0
Client kickout due to consecutive Tx failures
```

```
==========================================
Last 12 occurrence (most recent first)
------------------------------------------
client-mac: 00:01:5d:8d:50:8c
BSSID: 00:4e:35:c4:dc:f0
Association ID: 86
Total association time (ms): 97320
Total Tx frames transmitted: 9565
Consecutive Tx failure...
Failure counts per frame types
RTS: 0
BAR: 468
Trigger: 0
AMPDU: 44
Non-AMPDU: 0
Kickout thresh: 512
Elapsed time (ms): 42225
Fake sleep...
Number of entering fake sleep: 2
Number of timeout: 2
Rx event count during Tx failure: 0
Last Tx rate (Kbps): 270000
ACK SNR history (dB: ms before kickout)
63: 97180
56: 96180
43: 79180
32: 69180
22: 59180
Last ACK SNR (dB): 17
Rx SNR history (dB: ms before kickout)
59: 82180
38: 69180
20: 41180
Last Rx SNR (dB): 20
Time of kickout: UTC 2021-12-22 02:22:53
```

show iap command

The following parameters have been added to the **show iap** command to display IAP VPN statistics:

- The **show iap statistics** command displays the IAP VPN statistics information.
- The **show iap branch-stats branch-key <key>** command displays the statistics of an IAP VPN branch.
- The **show iap subnet-stats subnet <subnet>** command displays the statistics of an IAP VPN subnet.
- The **show iap subnets-summary** command displays the summary of IAP subnet information.

```
(host) [mynode]# show iap subnets-summary
Summary of IAP Branch Subnets
-----------------------------
S.No  Subnet Name             MaxBID   BIDs set in Bitmap  BIDs free in Bitmap  Allocated
Branches  Down Branches  Reclaimed from Down Branches
----  -----------            ------  ------------------  --------------------  -------------
-----  -------------  ----------------------------
1     1.1.1.0-1.1.1.255,1        64      4                   60                    4
          3              0
2     50.11.0.0-50.11.255.255,5  8192    5                   8187                  5
          4              0
3     59.59.95.0-59.59.95.100,4  12      2                   10                    2
          2              0
```

show mon-serv command

The following parameters have been added to the **show mon-serv** command to display the micro-bootstrapping and bootstrapping statistics of a cluster:

- The **show mon-serv-lc-table microboot-stats** command displays the micro-bootstrapping statistics of a cluster.
- The **show mon-serv-lc-table bootstrap-stats** command displays the bootstrapping statistics of a cluster.

show stm perf-history command

The output of the **show stm perf-history** command will now display the **Avg rate/s** to indicate the average number of association requests received by the switch. The command has been modified to display the number of association requests received by the switch for the past 3 hours.

```
host) #show stm perf-history
Association Rate History
------------------------
Day  Hour  Min  Total (roams)    Avg rate/s  Peak rate/s  Peak time
---  ----  ---  -------------    ----------  -----------  ---------
8    2     59   529 (529, 100%)  11.8        12.6         02:59:34
8    2     58   690 (690, 100%)  11.5        12.2         02:58:19
8    2     57   694 (694, 100%)  11.6        12.2         02:57:14
8    2     56   708 (707, 99%)   11.8        12.8         02:56:54
```

The output displays the association rate history for every one minute of the past 3 hours.

mgmt-server command

The **mgmt-server** command now allows users to control the generation of passive controller station AMON messages. The passive controller station AMON messages are not generated by default. To generate these messages, issue the **mgmt-server profile <name of the profile> inline-ctrl-assoc-stats** command on managed devices.

```
(host)[md] (config) #mgmt-server profile default-amp
(host)[md](Mgmt Config profile "default-amp") #inline-ctrl-assoc-stats
```

Regulation of Core Dump Files

Starting from AOS-W 8.6.0.17, users can issue the **ap system-profile <name> dump-collection-profile transfer-enable** command to send the core dump files to the managed device.

The AOS-W WebUI also allows users to regulate the core dump files sent to the managed device. In the **Managed Network** node hierarchy, navigate to the **Configuration > System > Profiles > Dump Collection** tab and select the **Transfer Enable** check box to send the core dump files to the managed device.

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 8.6.0.17*

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 8.6.0.17*

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 8.6.0.17*

AP Family	AP Model
OAW-AP100 Series	OAW-AP104, OAW-AP105

Table 5: *Supported AP Platforms in AOS-W 8.6.0.17*

AP Family	AP Model
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
OAW-AP228 Series	OAW-AP228
OAW-AP270 Series	OAW-AP274, OAW-AP275, OAW-AP277
OAW-AP300 Series	OAW-AP304, OAW-AP305
OAW-AP303 Series	OAW-AP303, OAW-AP303P
OAW-AP303H Series	OAW-AP303H
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
500 Series	OAW-AP504, OAW-AP505

Table 5: *Supported AP Platforms in AOS-W 8.6.0.17*

AP Family	AP Model
510 Series	OAW-AP514, OAW-AP515
530 Series	OAW-AP534, OAW-AP535
550 Series	OAW-AP555
OAW-RAP3 Series	OAW-RAP3WN, OAW-RAP3WNP
OAW-RAP100 Series	OAW-RAP108, OAW-RAP109
OAW-RAP155 Series	OAW-RAP155, OAW-RAP155P

Chapter 5
Regulatory Updates in AOS-W 8.6.0.17

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

Periodic regulatory changes may require modifications to the list of channels supported by an AP. For a complete list of channels supported by an AP using a specific country domain, access the switch Command Line Interface (CLI) and execute the **show ap allowed-channels country-code <country-code> ap-type <ap-model>** command.

For a complete list of countries and the regulatory domains in which the APs are certified for operation, refer to the Downloadable Regulatory Table or the DRT Release Notes at https://myportal.al-enterprise.com/.

The following DRT file version is part of this release:

- DRT-1.0_83381

Chapter 6
Resolved Issues in AOS-W 8.6.0.17

This chapter describes the issues resolved in this release.

Table 6: *Resolved Issues in AOS-W 8.6.0.17*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-156428 AOS-211063	–	All managed devices in a cluster responded to the ARP request of the client. This issue occurred when either local proxy or broadcast-multicast optimization was enabled on managed devices. The fix ensures that the managed devices work as expected. This issue was observed in managed devices running AOS-W 8.2.1.1 or later versions.	AOS-W 8.2.1.1
AOS-157472 AOS-209050	–	The MAC address of the AP was not present in the called-station-ID of RADIUS accounting messages. The fix ensures that the MAC address of the AP is available in the called-station-ID of RADIUS accounting messages. This issue was observed in APs running AOS-W 8.5.0.8 or later versions.	AOS-W 8.5.0.8
AOS-186503 AOS-194572 AOS-198513	–	The **show ap bss-table** command incorrectly displayed the details of eth1 as downlink when the same was configured as the member of LACP for the uplink. The fix ensures that the Mobility Master does not display incorrect information. This issue was observed in Mobility Masters running AOS-W 8.1.0.0 or later versions.	AOS-W 8.6.0.0
AOS-191880	–	Mobility Masters running AOS-W 8.3.0.0 or later versions crashed unexpectedly. The log files listed the reason for the event as **Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2)**. The fix ensures that the Mobility Masters work as expected.	AOS-W 8.3.0.0
AOS-196042 AOS-217995 AOS-221263	–	The output of the **show ucc dns-ip-learning** command displayed **Unknown** for **Service Provider**. The fix ensures that the command displays the correct **Service Provider**. This issue is observed in managed devices running AOS-W 8.6.0.9 or later versions.	AOS-W 8.6.0.9
AOS-197497	–	AirMatch selected the same channel for two neighboring APs even after radar detection. The fix ensures that AirMatch works as expected. This issue was observed in managed devices running AOS-W 8.5.0.3 or later versions.	AOS-W 8.5.0.3

Table 6: *Resolved Issues in AOS-W 8.6.0.17*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-197812 AOS-226345	–	A mismatch of user roles was observed in the WebUI and the CLI of the Mobility Master and managed device. This issue occurred when UDR was configured to assign user roles to clients. The fix ensures that there is no mismatch of user roles in the WebUI and the CLI of Mobility Master and managed device. This issue was observed in Mobility Masters and managed devices running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.0
AOS-199971 AOS-229489	–	Mobility Masters running AOS-W 8.5.0.6 or later versions generated a lot of httpd debug messages. This issue occurred when the logging levels configured using the CLI were not updated on the Mobility Master. The fix ensures that the logging levels are updated correctly and the Mobility Master works as expected.	AOS-W 8.5.0.6
AOS-200145 AOS-223533 AOS-226408	–	A few clients were disconnected from the network. The fix ensures seamless connectivity. This issue was observed in managed devices running AOS-W 8.5.0.11 or later versions in a cluster setup.	AOS-W 8.5.0.11
AOS-203025 AOS-224678	–	A few mesh point APs were down in the AP database. This issue occurred when CPsec was disabled. The fix ensures that the mesh point APs are not down. This issue was observed in managed devices running AOS-W 8.5.0.6 or later versions in a cluster setup.	AOS-W 8.5.0.6
AOS-203910	–	A few stand-alone switches running AOS-W 8.6.0.3 or later versions crashed and rebooted unexpectedly. The log file listed the reason for the event as, **Datapath timeout (Heartbeat Initiated) (Intent:cause:register 53:86:0:2c)**. The fix ensures that the stand-alone switches work as expected. Duplicates: AOS-209692, AOS-204905, AOS-217020, AOS-219688, and AOS-219064	AOS-W 8.6.0.3
AOS-205140 AOS-219614 AOS-227089	–	The AppRF ACLs using a voice role unexpectedly blocked WebRTC calls. This issue occurred when WebRTC audio and video ACLs were not part of the default **voip-applications-acl**. The fix ensures that the ACLs do not block the WebRTC calls. This issue was observed in Mobility Masters running AOS-W 8.6.0.8 or later versions.	AOS-W 8.6.0.8
AOS-205284 AOS-226338 AOS-229041	–	Some OAW-AP515 access points running AOS-W 8.6.0.10 or later versions crashed unexpectedly. The log files listed the reason for the event as **Warm-reset PC is at txq_hw_fill+0x13bc/0x21b8 [wl_v6]**. The fix ensures that the APs work as expected.	AOS-W 8.6.0.10
AOS-206653	–	The **SAPD** process crashed on a managed device and IPv6 APs were stuck in **D** flag. This issue was observed in CPsec-enabled VPNCs. The fix ensures that the managed devices work as expected.	AOS-W 8.6.0.16

Table 6: *Resolved Issues in AOS-W 8.6.0.17*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-206765 AOS-208978	–	A few show commands failed to display any output. The fix ensures that the commands display the output. This issue was observed in managed devices running AOS-W 8.7.0.0 or later versions.	AOS-W 8.7.0.0
AOS-207017	–	The SIP traffic of VPN users was incorrectly routed through a different port. The fix ensures that the traffic is routed through the configured port. This issue was observed in managed devices running AOS-W 8.6.0.2 or later versions.	AOS-W 8.6.0.2
AOS-207337	–	After upgrading from AOS-W 8.2.x.x to AOS-W 8.5.0.0-FIPS or later versions, a few managed devices were stuck in the **LAST SNAPSHOT** state. The fix ensures that the managed devices work as expected. This issue was observed in managed devices running AOS-W 8.5.0.0 or later versions.	AOS-W 8.5.0.0
AOS-208351	–	The maximum age out value of HTTP Strict-Transport-Security (HSTS) was incorrectly set as 7 days. The fix ensures that the maximum age out vale of HSTS is set to one year. This issue was observed in Mobility Masters running AOS-W 8.3.0.0 or later versions.	AOS-W 8.7.0.0
AOS-208483	–	Users failed to timeout after an AP reboot and the user entries were retained in the user table although the clients were disconnected few days back. The fix ensures that the user entries are removed from the user table after the clients get disconnected. This issue occurred when the wireless clients connected using bridge mode switched to a VAP terminated on another managed device deployed in a different cluster. This issue was observed in managed devices running AOS-W 8.7.0.0.	AOS-W 8.7.0.0
AOS-209276	–	The **show datapath crypto counters** command displayed the same output parameter, **AESCCM Decryption Invalid Replay Co** twice. The fix ensures that the command does not display the **AESCCM Decryption Invalid Replay Co** parameter twice. This issue was observed in Mobility Masters running AOS-W 8.5.0.0 or later versions.	AOS-W 8.5.0.10
AOS-209583 AOS-229056	–	Some APs running AOS-W 8.7.1.5 or later versions crashed unexpectedly. The log files listed the reason for the event as **PC is at inet_fill_ifaddr+0x84/0x2a0**. The fix ensures that the APs work as expected.	AOS-W 8.7.1.5
AOS-211720	–	The **STM** process crashed on managed devices and hence, APs performed a failover to another cluster. The fix ensures that the managed devices work as expected. This issue was observed in managed devices running AOS-W 8.5.0.5 or later versions.	AOS-W 8.5.0.5
AOS-211863	–	Some APs did not come up on managed devices. This issue occurred when	AOS-W 8.6.0.5

Table 6: *Resolved Issues in AOS-W 8.6.0.17*

New Bug ID	Old Bug ID	Description	Reported Version
		▪ the forwarding mode was changed to bridge mode. ▪ the name of the ACL was 64 bytes. The fix ensures that the managed devices work as expected. This issue is observed in managed devices running AOS-W 8.6.0.5 or later versions.	
AOS-212605 AOS-218721	–	Some APs running AOS-W 8.6.0.9 or later versions crashed unexpectedly. The log files listed the reason for the event as **wlc_key_get_info+0x4/0x60 [wl_v6]**. The fix ensures that the APs work as expected.	AOS-W 8.7.1.1
AOS-214041	–	A few APs running AOS-W 8.5.0.5 or later versions were unable to establish S-AAC tunnel with the managed devices. This issue occurred after configuring 802.1X authentication. The fix ensures that the APs are able to establish S-AAC tunnel with the managed devices.	AOS-W 8.5.0.5
AOS-214146 AOS-220374	–	The authentication server load balancing feature did not work as expected. The fix ensures that the authentication server load balancing feature works as expected. This issue was observed in managed devices running AOS-W 8.5.0.10 or later versions.	AOS-W 8.5.0.10
AOS-214524	–	Some APs running AOS-W 8.6.0.6 or later versions detected its own BSSIDs as rogue BSSIDs. Enhancements to the wireless driver resolved the issue. **Duplicates:** AOS-225132, AOS-226070, AOS-226617, AOS-218317	AOS-W 8.6.0.6
AOS-215063	–	The output of the **show gsm debug channel cluster_aac** and **show gsm debug channel cluster_ap** commands was not filtered correctly. The fix ensures that the commands display the output based on the applied filters. This issue was observed in Mobility Masters running AOS-W 8.5.0.10 or later versions.	AOS-W 8.5.0.10
AOS-215357 AOS-220057	–	A few managed devices were unable to transmit IPv4 traffic to the Mobility Master intermittently. This issue was observed in Mobility Masters running AOS-W 8.5.0.10 or later versions in a Mobility Master - Managed devices dual stack deployment. The fix ensures that the managed devices work as expected.	AOS-W 8.5.0.10
AOS-215461 AOS-220709	–	The database synchronization failed between standby and stand-alone switches running AOS-W 8.6.0.9 or later versions. The fix ensures that the database synchronization does not fail.	AOS-W 8.6.0.9
AOS-216133	–	A few clients were unable to connect to APs on A-band channels. The fix ensures seamless connectivity. This issue was observed in APs running AOS-W 8.7.1.0 or later versions.	AOS-W 8.7.1.0

Table 6: *Resolved Issues in AOS-W 8.6.0.17*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-216145	–	Mobility Masters running AOS-W 8.5.0.8 or later versions sent continuous DNS requests to the managed devices. This issue occurred when a folder that was not available on the /mm node was trying to get synchronized on the managed devices. The fix ensures that the Mobility Master works as expected.	AOS-W 8.5.0.8
AOS-216874 AOS-219841	–	The virtual MAC address of a VLAN got deleted from the bridge table and hence, resulted in a network outage. The fix ensures that the managed devices work as expected. This issue was observed in managed devices running AOS-W 8.5.0.11 or later versions.	AOS-W 8.5.0.11
AOS-217104 AOS-219159 AOS-227155	–	ESI redirect failed and traffic was forwarded to the default gateway. The fix ensures that the managed devices work as expected. This issue was observed in managed devices running AOS-W 8.6.0.6 or later versions.	AOS-W 8.6.0.6
AOS-217184	–	Some OAW-4750XM switches running AOS-W 8.7.1.1 or later versions crashed and rebooted unexpectedly. The log files listed the reason for the events as, **Kernel Panic (Intent:cause:register 12:86:b0:4)**. This issue occurred due to socket buffer corruption. The fix ensures that the OAW-4750XM switches work as expected. **Duplicates:** AOS-218026, AOS-220562, AOS-220616, AOS-220985, AOS-225001, AOS-225002, and AOS-226697	AOS-W 8.7.1.1
AOS-217653 AOS-224031 AOS-222483	–	Some OAW-AP535 access points running AOS-W 8.7.1.4 or later versions did not respond to the fragmented ping requests from a few clients. This issue occurred when the APs operated in tunnel mode. The fix ensures that the APs work as expected.	AOS-W 8.7.1.4
AOS-217775	–	Some OAW-AP224 access points running AOS-W 8.6.0.0 or later versions crashed unexpectedly in a cluster setup. The fix ensures that the APs work as expected.	AOS-W 8.6.0.0
AOS-217910 AOS-227007 AOS-227808	–	Some users got disconnected from the network. The log files listed the reason for the event as **Wlan driver excessive tx fail quick kickout**. This issue occurred when APs sent RTS frames on incorrect BSSIDs. The fix ensures that the APs work as expected. This issue was observed in OAW-AP535 access points running AOS-W 8.6.0.10 or later versions.	AOS-W 8.6.0.10
AOS-218162	–	The wired Ethernet port did not form a GRE tunnel with the managed device. The fix ensures that the wired Ethernet port forms a GRE tunnel with the managed device. This issue was observed in managed devices running AOS-W 8.7.1.1 or later versions.	AOS-W 8.7.1.1

Table 6: *Resolved Issues in AOS-W 8.6.0.17*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-218328 AOS-220026 AOS-223535	–	VRRP flapping was observed on managed devices running AOS-W 8.6.0.4 or later versions and hence, clients faced connectivity issues. The fix ensures that the managed devices work as expected.	AOS-W 8.6.0.4
AOS-218435	–	The status of the VRRP switch changed to **INIT** state after adding a VLAN. The fix ensures that the VRRP instance functions as expected. This issue was observed in managed devices running AOS-W 8.2.2.2 or later versions.	AOS-W 8.2.2.2
AOS-218519	–	A few mesh APs detected its own BSSIDs as phony BSSIDs. The fix ensures that the APs do not detect its own BSSIDs as phony BSSIDs. This issue was observed in APs running AOS-W 8.6.0.7 or later versions.	AOS-W 8.6.0.7
AOS-218988	–	Some managed devices running AOS-W 8.5.0.10 or later versions incorrectly used the VRRP IP address as the source interface to transmit PAPI traffic to the AMON server. The fix ensures that the managed devices work as expected.	AOS-W 8.5.0.10
AOS-219255 AOS-227048	–	The **show running-config** command did not display information related to session ACL. However, the **show configuration effective** command displayed information about the session ACL. The fix ensures that the **show running-config** command displays information related to session ACL. This issue was observed in managed devices running AOS-W 8.5.0.8 or later versions.	AOS-W 8.5.0.8
AOS-219376	–	Some users were unable to add VIA server details if the domain name exceeded 32 characters. The fix ensures that the domain name supports up to 128 characters. This issue was observed in Mobility Masters running AOS-W 8.7.1.2 or later versions.	AOS-W 8.7.1.2
AOS-219385	–	Some APs took a long time to come up on the backup data center after a primary data center failover. This issue was observed in APs running AOS-W 8.5.0.10 or later versions. The fix ensures that the APs do not take a long time to boot up.	AOS-W 8.5.0.10
AOS-219483	–	The output of the **show ap debug receive-config** command displayed incorrect value for **VLAN**. This issue was observed in Mobility Masters running AOS-W 8.6.0.0 or later versions. The fix ensures that the **show ap debug receive-config** command displays correct value for **VLAN**.	AOS-W 8.9.0.0

Table 6: *Resolved Issues in AOS-W 8.6.0.17*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-219619	–	Configurations inherited from the Mobility Master were incorrectly displayed as **local/mm** indicating that the configurations were locally enabled on the managed devices. The fix ensures that the configurations inherited from the Mobility Master are displayed correctly. This issue was observed in managed devices running AOS-W 8.5.0.8 or later versions.	AOS-W 8.5.0.8
AOS-219702	–	A few APs incorrectly reported a hotspotter attack. The fix ensures that the APs work as expected. This issue was observed in APs running AOS-W 8.6.0.7 or later versions.	AOS-W 8.6.0.7
AOS-219739	–	The **profmgr** process crashed on the backup Mobility Masters running AOS-W 8.7.1.0 or later versions. The fix ensures that the Mobility Master works as expected.	AOS-W 8.7.1.0
AOS-219894 AOS-220122	–	The BLE server displayed an incorrect **Last Sync Time**. The fix ensures that the BLE server displays the correct **Last Sync Time**. This issue was observed in managed devices running AOS-W 8.7.1.1 or later versions.	AOS-W 8.7.1.1
AOS-220108	–	The **OFA** process crashed on Mobility Master Virtual Appliances running AOS-W 8.6.0.6 or later versions. This issue occurred when the **show openflow debug ports** command was executed. The fix ensures that the Mobility Master Virtual Appliances work as expected.	AOS-W 8.6.0.6
AOS-220254 AOS-227702 AOS-227977	–	Some users were unable to pass traffic to the internet. This issue occurred when APs could not source NAT the traffic as the traffic got incorrectly tunneled to the switch. The fix ensures that the users are able to pass traffic to the internet. This issue was observed in stand-alone switches running AOS-W 8.7.1.2 or later versions.	AOS-W 8.7.1.2
AOS-220704 AOS-228881	–	Some APs were incorrectly displayed under different clusters. The fix ensures that the APs are not incorrectly displayed under different clusters. This issue was observed in managed devices running AOS-W 8.5.0.11 or later versions.	AOS-W 8.5.0.11
AOS-220706	–	The Mobility Master assigned duplicate IP addresses to the managed devices. This issue occurred after a failover. The fix ensures that the managed devices are not assigned duplicate IP addresses. This issue was observed in Mobility Masters running AOS-W 8.6.0.5 or later versions.	AOS-W 8.6.0.5
AOS-220841	–	Some clients were unable to connect to OAW-AP535 access points that operated on A band. This issue occurred due to false radar detection on non-DFS channels. The fix ensures that there is no false radar detection on non-DFS channels. This issue was observed in OAW-AP535 access points running AOS-W 8.6.0.8 or later versions.	AOS-W 8.6.0.8

Table 6: *Resolved Issues in AOS-W 8.6.0.17*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-220982	–	A few wireless clients were unable to pass traffic during a cluster failover. The fix ensures that the clients are able to pass traffic during a cluster failover. This issue was observed in managed devices running AOS-W 8.5.0.13 or later versions.	AOS-W 8.5.0.13
AOS-220996 AOS-227669	–	The **switch_daemon** process crashed on Mobility Masters running AOS-W 8.7.1.3 or later versions. The fix ensures that the Mobility Masters work as expected.	AOS-W 8.7.1.3
AOS-221018 AOS-220919	–	Some users were unable to connect to SSIDs. This issue occurred in 802.11r and MultiZone enabled configurations. The fix ensures seamless connectivity. This issue was observed in APs running AOS-W 8.5.0.11 or later versions.	AOS-W 8.5.0.11
AOS-221144 AOS-226631	–	ARP packets were not forwarded to the uplink switch when bcmc-optimization was enabled on the switches. This issue was observed in Mobility Masters and managed devices running AOS-W 8.5.0.9 or later versions. The fix ensures that the Mobility Masters and managed devices work as expected.	AOS-W 8.5.0.9
AOS-221225	–	Some OAW-AP387 access points running AOS-W 8.7.1.1 or later versions rebooted unexpectedly. The log files listed the reason for the event as **Reboot caused by kernel panic: Fatal exception**. The fix ensures that the APs work as expected.	AOS-W 8.7.1.1
AOS-221307	–	Adding a new VLAN removed all the existing VLANs on the port channel. This issue occurred when the existing VLAN list exceeded 256 characters. The fix ensures that the VLAN list supports up to 1024 characters. This issue was observed in managed devices running AOS-W 8.0.0.0 or later versions.	AOS-W 8.5.0.8
AOS-221429	–	Downloadable user roles were not applied correctly in the split tunnel mode. This issue was observed in stand-alone switches running AOS-W 8.6.0.9 or later versions. The fix ensures that the stand-alone switches work as expected.	AOS-W 8.6.0.9
AOS-221666 AOS-222708	–	Some OAW-RAPs running AOS-W 8.6.0.9 or later versions crashed and rebooted unexpectedly. The log file listed the reason for the event as, **Kernel panic - not syncing**. The fix ensures that the OAW-RAPs work as expected.	AOS-W 8.6.0.9
AOS-221743 AOS-212229 AOS-229253	–	Some APs running AOS-W 8.5.0.10 or later versions rebooted unexpectedly. The log files listed the reason for the events as, **skb_release_data+0xa0/0xc8/neigh_flush_dev+0x60**. The fix ensures that the APs work as expected.	AOS-W 8.5.0.10

Table 6: *Resolved Issues in AOS-W 8.6.0.17*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-221798	–	Mobility Controller Virtual Appliances running AOS-W 8.4.0.0 or later versions were unable to route jumbo data packets even when jumbo frames were enabled. This issue was observed in vSphere Hypervisor running 6.7 or later versions. The fix ensures that the Mobility Controller Virtual Appliances are able to route data packets.	AOS-W 8.8.0.0
AOS-222027 AOS-226135 AOS-229212	–	Some managed devices running AOS-W 8.7.1.3 or later versions in a cluster setup generated kernel slab corruption logs. The fix ensures that the managed devices work as expected.	AOS-W 8.7.1.3
AOS-222152	–	A few clients faced connectivity issues. This issue occurred due to a race condition, where the PHY mode of the initially configured VAP was incorrectly applied to all the other VAPs. The fix ensures that the APs work as expected. This issue was observed in APs running AOS-W 8.6.0.10 or later versions.	AOS-W 8.6.0.10
AOS-222346	–	Flash files removed using the **wipe out flash** command were available in the DIR folder and the switches were also stuck after a reboot. The fix ensures that the command erases all data and formats the flash file system in the switch. This issue was observed in OAW-40xx Series switches running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.0.
AOS-222401 AOS-227191	–	Some clients were unable to perform WPA3 authentication. This issue occurred after a cluster failover. The fix ensures that clients are able to perform WPA3 authentication. This issue was observed in stand-alone switches running AOS-W 8.6.0.13 or later versions.	AOS-W 8.6.0.13
AOS-222469	–	The number of APs in a network were higher than the number of licenses installed. The fix ensures that there is no discrepancy between the number of licenses and the number of APs. This issue was observed in stand-alone switches running AOS-W 8.5.0.12 or later versions.	AOS-W 8.5.0.12
AOS-222499 AOS-228446 AOS-226568	–	Clients that performed only four-way handshake were unable to update their VSA role derived after machine and user authentication. The fix ensures successful client authentication. This issue is observed in managed devices running AOS-W 8.6.0.6 or later versions.	AOS-W 8.6.0.6
AOS-222771	–	Some managed devices running AOS-W 8.5.0.12 or later versions did not send SNMPv3 information to the OmniVista 3600 Air Manager server. The fix ensures that the managed devices send SNMPv3 information to the OmniVista 3600 Air Manager server.	AOS-W 8.5.0.12

Table 6: *Resolved Issues in AOS-W 8.6.0.17*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-222931	–	Some APs did not form active tunnels with the AAC. The fix ensures that the APs form active tunnels with the AAC. This issue was observed in managed devices running AOS-W 8.7.1.4 or later versions.	AOS-W 8.7.1.4
AOS-222992 AOS-228891	–	A large number of log files were generated and stored at /flash1/log/backup folder. This issue occurred due to a cluster failover between clients and APs. The fix ensures that the switches work as expected. This issue was observed in OAW-4650 and OAW-4750XM switches running AOS-W 8.7.1.0 or later versions.	AOS-W 8.7.1.0
AOS-223094	–	The net destination ID value in ACEs was incorrectly set to 0 after a reboot. The fix ensures that the managed devices work as expected. This issue was observed in managed devices running AOS-W 8.2.0.0 or later versions. Duplicates: AOS-220190, AOS-224240, AOS-224792, AOS-226989, and AOS-228434	AOS-W 8.6.0.9
AOS-223337	–	The clients added to the client match unsupported list were considered for client match steers. The fix ensures that the unsupported clients are not considered for client match steers. This issue was observed in managed devices running AOS-W 8.5.0.10 or later versions.	AOS-W 8.5.0.10
AOS-223452	–	A delay was observed in the update of ARP table. This issue occurred when the clients used the same IP address but different MAC addresses. The fix ensures that the ARP table gets updated without any delay. This issue was observed in switches running AOS-W 8.6.0.9 or later versions.	AOS-W 8.6.0.9
AOS-223656 AOS-227360	–	Some OAW-RAPs were unable to come up on managed devices after a reboot. The fix ensures that the OAW-RAPs are able to come up on managed devices. This issue was observed in managed devices running AOS-W 8.7.1.4 or later versions.	AOS-W 8.7.1.4
AOS-223667	–	High CPU utilization was observed on managed devices running AOS-W 8.5.0.13 or later versions. This issue occurred when the network was scanned for security vulnerabilities. The fix ensures that the managed devices work as expected.	AOS-W 8.5.0.13
AOS-223669	–	Some users were unable to complete captive portal authentication. This issue occurred when ipv6-user snmpwalk populated IPv4 user details. The fix ensures that the users are able to complete captive portal authentication. This issue was observed in managed devices running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.4

Table 6: *Resolved Issues in AOS-W 8.6.0.17*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-223709	–	Mobility Masters running AOS-W 8.5.0.0 or later versions crashed unexpectedly. This issue occurred due to a race condition. The log files listed the reason for the event as **nanny rebooted machine - fpapps process died (Intent:cause:register 34:86:50:2)**. The fix ensures that the Mobility Masters work as expected.	AOS-W 8.8.0.0
AOS-223740	–	The expired machine authentication cache entries were not removed. The fix ensures that the expired machine authentication cache entries are removed. This issue was observed in stand-alone switches running AOS-W 8.7.1.3 or later versions.	AOS-W 8.7.1.3
AOS-223797	–	The **show ap remote auth-trace-buf** command did not display any output. The fix ensures that the command works as expected. This issue was observed in stand-alone switches and managed devices running AOS-W 8.6.0.9 or later versions.	AOS-W 8.6.0.9
AOS-223817	–	The **auth** process crashed on Mobility Masters running AOS-W 8.6.0.9 or later versions. The fix ensures that Mobility Masters work as expected. **Duplicates:** AOS-225761, AOS-226316, AOS-226846, AOS-227879, and AOS-225878	AOS-W 8.6.0.9
AOS-223839	–	The output of the **show ap active** command did not display any value for **Outer IP**. The fix ensures that the command displays the correct **Outer IP** value. This issue was observed in Mobility Masters running AOS-W 8.6.0.9 or later versions.	AOS-W 8.6.0.9
AOS-223848	–	The **+** symbol in the **Configuration > Services > AirGroup > Service-Based Policy** page of the WebUI did not allow users to create an AirGroup profile. Users can create an AirGroup profile only by navigating to the **Configuration > System > Profiles > AirGroup** page of the WebUI. The fix ensures that the **+** symbol is not available in the **Configuration > Services > AirGroup > Service-Based Policy** page of the WebUI. This issue was observed in Mobility Masters running AOS-W 8.0.0.0 or later versions.	AOS-W 8.7.1.4
AOS-224019	–	High dpagent memory utilization was observed. This issue was observed in managed devices running AOS-W 8.6.0.9 or later versions. The fix ensures that the managed devices work as expected. Duplicates: AOS-224821, AOS-225436, AOS-225976, AOS-226123,AOS-227558, AOS-228839, AOS-228983, AOS-229064, AOS-229981, AOS-230241, and AOS-230509	AOS-W 8.6.0.9

Table 6: *Resolved Issues in AOS-W 8.6.0.17*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-224105	–	The **wlsxVoiceClientLocationUpdate** SNMP traps were not generated when clients roamed to a new AP. The fix ensures that the SNMP location update traps are generated when clients roam between APs. This issue was observed in Mobility Masters running AOS-W 8.6.0.9 or later versions.	AOS-W 8.6.0.9
AOS-224186	–	The **show tech-support** command did not display any information about the kernel crash and displayed the message, **No kernel crash information available**. The fix ensures that the **show tech-support** command displays kernel crash information. This issue was observed in stand-alone switches running AOS-W 8.6.0.9 or later versions.	AOS-W 8.6.0.9
AOS-224197 AOS-227675	–	Some clients were unable to connect to managed devices running AOS-W 8.7.1.3 or later versions in a cluster setup. This issue occurred after a cluster flap. The fix ensures seamless connectivity.	AOS-W 8.7.1.3
AOS-224275 AOS-215206	–	The predefined v6-control policy did not allow DHCPv6 traffic. The fix ensures that DHCPv6 traffic is allowed. This issue is observed in managed devices running AOS-W 8.0.0.0 or later versions.	AOS-W 8.6.0.9
AOS-224326 AOS-226350	–	A few OAW-AP514 access points running AOS-W 8.7.1.5 or later versions crashed unexpectedly. The log files listed the reason for the event as **PC is at wlc_ratesel_set_link_bw+0x0**. The fix ensures that the APs work as expected.	AOS-W 8.7.1.5
AOS-224336	–	The telemetry websocket IoT transport profile authentication failed. This issue occurred when a remote server used a non-compliant HTTP header. The fix ensures successful authentication. This issue was observed in Mobility Masters running AOS-W 8.8.0.1 or later versions.	AOS-W 8.8.0.1
AOS-224538	–	A few APs running AOS-W 8.5.0.11 or later versions incorrectly fell back to the default AP group. The fix ensures that the APs do not fall back to the default AP group.	AOS-W 8.5.0.11
AOS-224688	–	The HE enabled APs were incorrectly displayed as **HTT None** in OmniVista 3600 Air Manager. The fix ensures that the status of the APs are correctly updated in OmniVista 3600 Air Manager. This issue was observed in APs running AOS-W 8.7.1.1 or later versions.	AOS-W 8.7.1.1
AOS-224767 AOS-221486	–	A few clients were disconnected from the network. The log file listed the reason for the event as **Wlan driver excessive tx fail quick kickout**. The fix ensures seamless connectivity. This issue was observed in OAW-AP535 and OAW-AP555 access points running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.8

Table 6: *Resolved Issues in AOS-W 8.6.0.17*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-224901	–	A few APs terminating in the backup LMS cluster did not move to the LMS cluster after a reboot. The fix ensures that the APs move to the LMS cluster after a reboot. This issue was observed in managed devices running AOS-W 8.6.0.9 or later versions.	AOS-W 8.6.0.9
AOS-224961	–	The global user entries table was not updated when clients roamed to a different AP. This issue occurred when 802.11r was enabled. The fix ensures that the global user entries table is updated even if the clients roam between APs. This issue was observed in APs running AOS-W 8.7.1.4 or later versions.	AOS-W 8.7.1.4
AOS-225231	–	The captive portal redirection URL did not display the complete ESSID. This issue occurred when the ESSID had 32 characters. The fix ensures that the captive portal redirection URL displays the complete BSSID. This issue was observed in managed devices running AOS-W 8.7.1.3 or later versions.	AOS-W 8.7.1.3
AOS-225508	–	Some managed devices running AOS-W 8.7.1.4 sent ARP requests with an incorrect MAC address. The fix ensures that the managed devices do not send ARP requests with an incorrect MAC address.	AOS-W 8.7.1.4
AOS-225517	–	Some APs running AOS-W 8.5.0.12 or later versions crashed and rebooted unexpectedly. The log files listed the reason for the event as **DHCP Lease expired**. The fix ensures that the APs work as expected.	AOS-W 8.5.0.12
AOS-225538	–	Some OAW-AP335 access points running AOS-W 8.6.0.9 or later versions crashed and rebooted unexpectedly. The log files listed the reason for the event as **Reboot caused by kernel panic:Fatal exception in interrupt with Target Assert**. The fix ensures that the APs work as expected.	AOS-W 8.6.0.9
AOS-225549	–	Some stand-alone switches running AOS-W 8.6.0.8 or later versions lost its netdestination aliases, user roles, and ACLs after a reboot. The fix ensures that the stand-alone switches work as expected.	AOS-W 8.6.0.8
AOS-225563	–	Low throughput issue was observed on OAW-AP515 access points running AOS-W 8.6.0.10 or later versions. This issue occurred when AP LACP is configured on OAW-AP515 access points. The fix ensures that the APs work as expected.	AOS-W 8.7.1.4
AOS-225659 AOS-226682	–	The **auth** process crashed on stand-alone switches running AOS-W 8.6.0.10 or later versions. The fix ensures that the stand-alone switches work as expected.	AOS-W 8.6.0.10

Table 6: *Resolved Issues in AOS-W 8.6.0.17*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-225817	–	Some OAW-AP315 access points running AOS-W 8.5.0.13 or later versions crashed and rebooted unexpectedly. The log files listed the reason for the event as **Reboot Reason: Reboot caused by kernel panic: assert**. The fix ensures that the APs work as expected.	AOS-W 8.5.0.13
AOS-225856 AOS-228686	–	The **im_helper** process was stuck in **Busy** state and high CPU utilization was also observed. This issue occurred after configuring a ble-service profile. The fix ensures that the Mobility Masters work as expected. This issue was observed in Mobility Masters running AOS-W 8.7.1.4 or later versions.	AOS-W 8.7.1.4
AOS-225873	–	Some managed devices running AOS-W 8.7.1.4 or later versions crashed and rebooted unexpectedly. The log files listed the reason for the event as **Reboot Cause: Datapath timeout (sos_xlp_process_poe_msg)**. The fix ensures that the managed devices work as expected.	AOS-W 8.7.1.4
AOS-226008	–	Cluster heartbeats were delayed and ping latency was also observed. This issue occurred due to continuous irregular traffic like ARP flooding. The fix ensures that the managed devices work as expected. This issue was observed in managed devices running AOS-W 8.7.1.4 or later versions in a cluster setup.	AOS-W 8.7.1.4
AOS-226012 AOS-226013	–	Mobility Controller Virtual Appliances running AOS-W 8.7.1.4 or later versions responded with its own MAC address as the management IP address for ARP requests. The fix ensures that the Mobility Controller Virtual Appliances work as expected.	AOS-W 8.7.1.4
AOS-226016	–	Some clients were able to access the internet even if the denyall user role was applied. The fix ensures that the clients are unable to access the internet if the denyall user role is applied. This issue was observed in managed devices running AOS-W 8.8.0.0 or later versions.	AOS-W 8.8.0.0
AOS-226075	–	The logs generated by the stand-alone switch did not have source and destination port details and the logs also indicated that all TCP packets are fragmented. The fix ensures that the logs have the necessary information. This issue was observed in stand-alone switches running AOS-W 8.6.0.12 or later versions.	AOS-W 8.6.0.12
AOS-226177	–	The **firewall deny-reserved-ip** and **ipv6 firewall deny-reserved-ip** commands incorrectly denied non-reserved IP addresses. The fix ensures that the commands work as expected. This issue was observed in Mobility Masters running AOS-W 8.6.0.9-FIPS or later versions.	AOS-W 8.6.0.9-FIPS

Table 6: *Resolved Issues in AOS-W 8.6.0.17*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-226306		The **show crypto isakmp** command displayed the output in an incorrect format. The fix ensures that the command displays the output in the correct format. This issue was observed in Mobility Masters running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.10
AOS-226320 AOS-228465	–	Some users were unable to perform the 802.1X authentication. This issue occurred when a few host IP addresses were removed from the netdestination list. The fix ensures that the users are able to perform the 802.1X authentication. This issue was observed in managed devices running AOS-W 8.6.0.10 or later versions.	AOS-W 8.6.0.10
AOS-226361 AOS-226850 AOS-227154	–	Mobility Masters running AOS-W 8.7.1.5 or later versions incorrectly routed traffic to different ports. The fix ensures that the Mobility Masters route data packets correctly.	AOS-W 8.7.1.5
AOS-226410	–	Cluster heartbeats were dropped in OAW-4850 switches running AOS-W 8.7.1.5 in a cluster setup. The fix ensures that the cluster heartbeats are not dropped.	AOS-W 8.7.1.5
AOS-226440	–	The **auth** process crashed on stand-alone switches running AOS-W 8.5.0.11 or later versions. This issue occurred after changing the downloadable role configuration. The fix ensures that the stand-alone switches work as expected.	AOS-W 8.5.0.11
AOS-226467 AOS-229346	–	The stale AirGroup server entries were not deleted even when the server was disconnected from the network. The fix ensures that the managed devices remove the stale AirGroup server entries. This issue was observed on managed devices running AOS-W 8.5.0.13 or later versions.	AOS-W 8.5.0.13
AOS-226475 AOS-229726	–	A few APs displayed flag **D**, indicating **Dirty or no config** state while provisioned to an AP group. The fix ensures that the APs do not display the **D** flag. This issue was observed in APs running AOS-W 8.5.0.11 or later versions.	AOS-W 8.5.0.11
AOS-226516 AOS-226552	–	Some AP-505H mesh access points running AOS-W 8.7.1.5 changed its wired MAC address after each reboot. The fix ensures that the APs do not change its MAC address after each reboot.	AOS-W 8.7.1.5
AOS-226548	–	Some managed devices running AOS-W 8.5.0.11 or later versions selected an incorrect next hop list after a reboot. This issue occurs when two uplinks were configured. The fix ensures that the managed devices select the correct nexthop list.	AOS-W 8.5.0.11
AOS-226555 AOS-224165	–	The **WMS** process crashed on Mobility Masters running AOS-W 8.7.1.3 or later versions. The fix ensures that the Mobility Masters work as expected.	AOS-W 8.7.1.3

Table 6: *Resolved Issues in AOS-W 8.6.0.17*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-226787 AOS-231935	–	Configuration failure was observed on managed devices running AOS-W 8.8.0.0 or later versions and an error message, **Error: System role 'default-iap-user-role' is not editable** was displayed. This issue occurred after configuring the PEFNG license. The fix ensures that the managed devices work as expected.	AOS-W 8.8.0.0
AOS-226824 AOS-227422	–	A few clients were unable to connect to APs running AOS-W 8.6.0.10 or later versions. This issue occurred when, ■ HT and VHT radio profiles were disabled but HE configuration was enabled on the APs. ■ the 4-way handshake was not successful. The fix ensures seamless connectivity.	AOS-W 8.6.0.10
AOS-226932 AOS-228418 AOS-229018	–	Some OAW-AP515 access points running AOS-W 8.7.1.5 crashed unexpectedly. The log files listed the reason for the event as **wlc_pktq_stats_free+0x48**.The fix ensures that the APs work as expected.	AOS-W 8.7.1.5
AOS-226970 AOS-228931	–	The bandwidth limit configured for a user role was not applied correctly for clients connected in bridge forwarding mode. The fix ensures that the bandwidth limit is applied correctly for clients connected in bridge forwarding mode. This issue was observed in managed devices running AOS-W 8.7.1.5 or later versions.	AOS-W 8.7.1.5
AOS-226978	–	The L2 option-82 feature did not work as expected on Mobility Controller Virtual Appliances running AOS-W 8.6.0.6 or later versions. This issue occurred due to incorrect endianness handling of the relayed DHCP packet. The fix ensures that the L2 option-82 feature work as expected.	AOS-W 8.6.0.6
AOS-227005 AOS-229010	–	A few APs running AOS-W 8.7.1.5 or later versions crashed unexpectedly. The log file listed the reason for the event as **PC is at ieee80211_parse_wnm_mbo_subelem+0x54/0x238 [umac]**. The fix ensures that the APs work as expected.	AOS-W 8.7.1.5
AOS-227039	–	Some AP-505H mesh access points running AOS-W 8.7.1.5 or later versions were stuck in **D** flag after an upgrade. The fix ensures that the APs work as expected.	AOS-W 8.7.1.5
AOS-227081 AOS-226543 AOS-213220	–	DPI failed to classify traffic and hence, application traffic was categorized as Port 0. The fix ensures that DPI classifies traffic as expected. This issue was observed in managed devices running AOS-W 8.6.0.11 or later versions.	AOS-W 8.6.0.11

Table 6: *Resolved Issues in AOS-W 8.6.0.17*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-227094	–	Heartbeats were missed and ping latency was also observed on managed devices running AOS-W 8.7.1.4 or later versions. This issue occurred after a cluster split. The fix ensures that the managed devices work as expected.	AOS-W 8.7.1.4
AOS-227292	–	HE-steers were triggered for HE-capable clients even when the high efficiency configuration was disabled in the wlan he-ssid-profile. The fix ensures that the HE-steers are not triggered when the high efficiency configuration is disabled in the wlan he-ssid-profile. This issue was observed in managed devices running AOS-W 8.6.0.10 or later versions.	AOS-W 8.6.0.10
AOS-227370 AOS-228184	–	Some OAW-AP535 access points running AOS-W 8.6.0.10 or later versions crashed and rebooted unexpectedly. The log files listed the reason for the event as **Reboot caused by kernel panic: Take care of the TARGET ASSERT first**. The fix ensures that the APs work as expected.	AOS-W 8.6.0.10
AOS-227457 AOS-227613	–	Data frames that were larger in size were dropped unexpectedly. This issue occurred when managed devices routed traffic through IPsec tunnels. The fix ensures that the managed devices do not drop data frames. This issue was observed in managed devices running AOS-W 8.6.0.10 or later versions.	AOS-W 8.6.0.10
AOS-227660	–	The second user that got connected to the network was unable to download the VIA profile. This issue occurred when the client was marked with the **D** flag in the datapath session for logon role. The fix ensures that the users are able to download the VIA profile. This issue was observed in managed devices running AOS-W 8.6.0.9 or later versions.	AOS-W 8.6.0.9
AOS-227858	–	Users were unable to load the XML file while configuring DHCP option 82 and an incorrect error message, **Error: Filename my_dhcp_option_82_mod2.xml has invalid keywords** was displayed. The fix ensures that the users are able to load the XML file and the Mobility Master displays appropriate error messages. This issue was observed in Mobility Masters running AOS-W 8.9.0.0 or later versions.	AOS-W 8.9.0.0
AOS-227905 AOS-227848	–	A few APs running AOS-W 8.6.0.14 or later versions generated a lot of kernel messages. The log files listed the reason for the event as **ipv6: Neighbour table overflow**. The fix ensures that the APs work as expected.	AOS-W 8.6.0.14

Table 6: *Resolved Issues in AOS-W 8.6.0.17*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-228112	–	The AirGroup server table incorrectly displayed duplicate AirGroup server entries with the same host name. The fix ensures that the AirGroup server table does not display duplicate entries. This issue was observed in Mobility Masters running AOS-W 8.6.0.11 or later versions.	AOS-W 8.6.0.11
AOS-228138 AOS-229159	–	A few clients were unable to perform authentication and incorrectly got reverted to the initial role. The fix ensures that the clients are able to perform authentication and they are assigned the correct role. This issue was observed in APs running AOS-W 8.7.1.6 or later versions.	AOS-W 8.7.1.6
AOS-228270 AOS-229544	–	Some OAW-AP535 access points running AOS-W 8.6.0.10 or later versions crashed unexpectedly. The log files listed the reason for the event as **FW assert at twt_protocol.c:224 Assertion twt_ie->wake_duration != 0.** The fix ensures that the APs work as expected.	AOS-W 8.6.0.10
AOS-228319	–	Some OAW-AP535 access points running AOS-W 8.7.1.6 or later versions crashed unexpectedly. The log files listed the reason for the event as **FW Exception :Excep :0 Exception detected, Thread ID: 0x00000069 Thread name : WLAN BE**. The fix ensures that the APs work as expected.	AOS-W 8.7.1.6
AOS-228390	–	A few managed devices running AOS-W 8.6.0.11 or later versions delayed sending the IGMP report to the multicast server. The fix ensures that the managed devices work as expected.	AOS-W 8.6.0.11
AOS-228466 AOS-224923	–	Some managed devices running AOS-W 8.8.0.0 or later versions incorrectly sent the inner IP address as the calling station ID for VIA authentication. The fix ensures that the managed devices do not send the inner IP address as the calling station ID for VIA authentication.	AOS-W 8.8.0.0
AOS-228571 AOS-230596 AOS-231216	–	High flash memory utilization was observed on Mobility Controller Virtual Appliances running AOS-W 8.7.1.6 or later versions. The fix ensures that the Mobility Controller Virtual Appliances work as expected.	AOS-W 8.7.1.6
AOS-228575	–	A few Intel clients experienced slow connection speed and high latency was also observed. Enhancements to the wireless driver resolved the issue, This issue was observed in APs running AOS-W 8.6.0.10 or later versions. Duplicates: AOS-226229, AOS-228049, AOS-228427, AOS-229037, AOS-229456, AOS-229476, AOS-230244, AOS-230601, AOS-230747, AOS-230805, AOS-227507	AOS-W 8.6.0.10

Table 6: *Resolved Issues in AOS-W 8.6.0.17*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-228579	–	A few clients were disconnected from the network while roaming between APs. This issue occurred when the 802.11r option was enabled on APs. The fix ensures that the clients are not disconnected from the network. This issue was observed in APs running AOS-W 8.9.0.0 or later versions.	AOS-W 8.9.0.0
AOS-228631	–	The TEXTUAL-CONVENTION and Timeticks MIBs were incorrectly defined and were imported from incorrect SNMP traps. The fix ensures that the MIBs are defined correctly. This issue was observed in Mobility Masters running AOS-W 8.6.0.9 or later versions.	AOS-W 8.6.0.9
AOS-228757	–	The **show wms rogue-ap list** command did not display the list of all rogue APs. This issue was observed in Mobility Masters running AOS-W 8.6.0.8 or later versions. The fix ensures that the command displays the list of all rogue APs.	AOS-W 8.6.0.8
AOS-228818	–	A few APs that operated in bridge mode dropped SMB packets. This issue occurred when the APs and clients were on different VLANs. The fix ensures that the APs work as expected. This issue was observed in OAW-AP535, OAW-AP555, and AP-635 access points access points running AOS-W 8.6.0.0 or later versions.	AOS-W 8.8.0.2
AOS-228886	–	Users were unable create a backup of the running configuration through TFTP server. This issue was observed in stand-alone switches running AOS-W 8.7.1.6 or later versions. The fix ensures that the users are able to create a backup of the running configuration through TFTP server.	AOS-W 8.7.1.6
AOS-228949 AOS-229237 AOS-229497	–	The cfg database was not available on managed devices running AOS-W 8.6.0.14 or later versions. This issue occurred when the managed devices failed to remove the old log files. The fix ensures that the managed devices work as expected.	AOS-W 8.6.0.14
AOS-229015 AOS-227266	–	A few clients were disconnected from the network with an error message, **Unspecified Failure**. The fix ensures seamless connectivity. This issue was observed in APs running AOS-W 8.5.0.11 or later versions.	AOS-W 8.5.0.11
AOS-229214 AOS-229324 AOS-227993	–	Some APs running AOS-W 8.7.1.5 or later versions crashed and rebooted unexpectedly. The log files listed the reason for the event as **Reboot caused by kernel panic: Take care of the TARGET ASSERT first**. The fix ensures that the APs work as expected.	AOS-W 8.7.1.5
AOS-230569	–	Clients connected to OAW-AP315 access points were unable to pass traffic. The fix ensures that clients are able to pass traffic. This issue was observed in OAW-AP315 access points running AOS-W 8.7.1.3 or later versions.	AOS-W 8.7.1.3

Table 6: *Resolved Issues in AOS-W 8.6.0.17*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-221983 AOS-227273	–	A few clients were disconnected from the network. The log file listed the reason for the event as **AP is resource constrained-Max Clients** even when the number of clients did not reach the maximum limit. The fix ensures seamless connectivity. This issue was observed in managed devices running AOS-W 8.6.0.11 or later versions.	AOS-W 8.6.0.11

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

Limitation

Following are the limitations observed in this release:

Port-Channel Limitation in OAW-4850 switches

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

No Support for Unique Local Address over IPv6 Network

The IPv6 addresses for interface tunnels do not accept unique local addresses.

Known Issues

Following are the known issues observed in this release.

Table 7: *Known Issues in AOS-W 8.6.0.17*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-151022 AOS-188417	185176	The output of the **show datapath uplink** command displays incorrect session count. This issue is observed in managed devices running AOS-W 8.1.0.0 or later versions.	AOS-W 8.1.0.0
AOS-151355	185602	A few managed devices are unable to pass traffic to the nexthop VPN concentrator (VPNC) using policy-based routing. This issue is observed in managed devices running AOS-W 8.0.1.0 or later versions.	AOS-W 8.0.1.0
AOS-155404 AOS-207878	191106	An AP is unable to establish IKE/IPsec tunnel with the managed device. This issue occurs when the AP is enrolled with EST certificates. This issue is observed in OAW-AP515 access points running AOS-W 8.5.0.0 or later versions in a Mobility Master-Managed Device topology.	AOS-W 8.6.0.4
AOS-156068	192100	The **DDS** process in a managed device running AOS-W 8.2.1.1 or later versions crashes unexpectedly.	AOS-W 8.2.1.1

Table 7: *Known Issues in AOS-W 8.6.0.17*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-182847	–	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. This issue occurs when a new SSID profile is created from an existing SSID profile using WebUI. This issue is observed in managed devices running AOS-W 8.4.0.0 or later versions in a Mobility Master-Managed Device topology.	AOS-W 8.4.0.0
AOS-184947 AOS-192737	–	The jitter and health score data are missing from the **Dashboard > Infrastructure > Uplink > Health** page in the WebUI. This issue is observed in Mobility Masters running AOS-W 8.4.0.4 or later versions.	AOS-W 8.4.0.4
AOS-185538 AOS-195334	–	High number of EAP-TLS timeouts are observed in a managed device. This issue occurs when multiple IP addresses are assigned to each client. This issue is observed in managed devices running AOS-W 8.3.0.8 or later versions.	AOS-W 8.3.0.8
AOS-187672 AOS-213397	–	Memory leak is observed in the **arci-cli-helper** process. This issue is observed in Mobility Masters and managed devices running AOS-W 8.3.0.6 or later versions.	AOS-W 8.3.0.6
AOS-188972 AOS-194746 AOS-208631 AOS-213627	–	Mobility Master displays the blacklisted clients although the clients were removed from the managed device. This issue is observed in Mobility Masters running AOS-W 8.4.0.4 or later versions in a cluster setup.	AOS-W 8.4.0.4
AOS-190071 AOS-190372	–	A few users are unable to access websites when WebCC is enabled on the user role. This issue occurs in a Per-User Tunnel Node (PUTN) setup when the VLAN of user role is in trunk mode. This issue is observed in OAW-4005 switches running AOS-W 8.4.0.0. **Workaround:** Perform the following steps to resolve the issue: 1.Remove web category from the ACL rules and apply **any any any permit** policy. 2. Disable WebCC on the user role. 3. Change the VLAN of user role from trunk mode to access mode.	AOS-W 8.4.0.0
AOS-190621	–	WebUI does not filter the names of the APs that begin with the special characters, + and %. This issue is observed in managed devices running AOS-W 8.4.0.2 or later versions.	AOS-W 8.4.0.2
AOS-192725	–	The **Dashboard > Overview** page of the WebUI displays incorrect number of users intermittently. This issue is observed in Mobility Masters running AOS-W 8.3.0.8 or later versions. **Duplicates:** AOS-188255, AOS-190476, AOS-190946, AOS-193586, AOS-194784, AOS-196004, AOS-200375, and AOS-210787	AOS-W 8.3.0.8

Table 7: *Known Issues in AOS-W 8.6.0.17*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-193184	–	All L2 connected managed devices move to L3 connected state after an upgrade. This issue is observed in managed devices running AOS-W 8.5.0.2 or later versions.	AOS-W 8.5.0.2
AOS-193231 AOS-200101 AOS-207456	–	The **Dashboard > Infrastructure > Access Devices** page of the WebUI displays an error message, **Error retrieving information**. This issue is observed in Mobility Masters running AOS-W 8.5.0.3 or later versions.	AOS-W 8.5.0.3
AOS-193278 AOS-228782	–	Users are unable to bring up the VPNC after an upgrade. The switch is stuck with an error message, **CONTROLLER-IP/V6 NOT SET(00:1a:1e:05:cd:28)**. This issue is observed in Mobility Masters running AOS-W 8.4.0.4 or later versions.	AOS-W 8.4.0.4
AOS-193560	–	The number of APs that are DOWN are incorrectly displayed in the **Dashboard > Overview** page of the WebUI. However, the CLI displays the correct status of APs. This issue is observed in Mobility Masters running AOS-W 8.4.0.4 or later versions. **Duplicates**: AOS-198565, AOS-200262, AOS-204794, AOS-212249, AOS-208110, AOS-209989, and AOS-212249	AOS-W 8.4.0.4
AOS-193775 AOS-194581 AOS-197372	–	A mismatch of AP count and client count is observed between the Mobility Master and the managed device. This issue is observed in Mobility Masters running AOS-W 8.3.0.0 or later versions.	AOS-W 8.5.0.2
AOS-193883 AOS-197756	–	A few APs are unable to use DHCP IPv6 addresses and option 52 for master discovery. This issue occurs when APs did not clear the previous LMS entries after an upgrade. This issue is observed in access points running AOS-W 8.3.0.8 or later versions. **Workaround:** Delete the IPv4 addresses from the ap system profile using the command, **ap system-profile** and from high availability profiles using the command, **ha.**	AOS-W 8.3.0.8
AOS-194080	–	Some managed devices display the error log, **Deleting a user IP=fe80::1c4d:d31f:a935:2107 with flags=0x0 from the datapath that does not exist in auth** even if IPv6 is disabled on the managed devices. This issue is observed in stand-alone switches running AOS-W 8.2.2.10 or later versions.	AOS-W 8.2.2.10
AOS-194381	–	Some managed devices lose the route-cache entries and drop the VRRP IP addresses sporadically. This issue is observed in managed devices running AOS-W 8.3.0.7 or later versions.	AOS-W 8.3.0.7

Table 7: *Known Issues in AOS-W 8.6.0.17*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-194911	–	Incorrect flag output is displayed for APs configured with 802.1X authentication when the **show ap database** command is executed. This issue is observed in APs running AOS-W 8.5.0.2 or later versions.	AOS-W 8.5.0.2
AOS-194964	–	A few users are unable to clone configurations from an existing group to a new group in a Mobility Master. This issue is observed in Mobility Masters running AOS-W 8.4.0.1 or later versions. **Workaround:** Execute the **rf dot11a-radio-profile <profile name>** command to change the operating mode of the AP from am-mode to ap-mode.	AOS-W 8.5.0.2
AOS-195089	–	The DNS traffic is incorrectly getting classified as **Thunder** and is getting blocked. This issue occurs when the DNS traffic is blocked and peer-peer ACL is denied for users. This issue is observed in managed devices running AOS-W 8.3.0.7 or later versions.	AOS-W 8.3.0.7
AOS-195100 AOS-198302 AOS-204455 AOS-206735	–	The health status of a managed device is incorrectly displayed as **Poor** in the **Dashboard > Infrastructure** page of the Mobility Master's WebUI. This issue is observed in Mobility Masters running AOS-W 8.3.0.7 or later versions.	AOS-W 8.3.0.7
AOS-195177	–	Some managed devices frequently generate internal system error logs. 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.	AOS-W 8.3.0.7
AOS-195434	–	An AP crashes and reboots unexpectedly. The log files list the reason for the event as **Reboot caused by kernel panic: Fatal exception**. This issue is observed in APs running AOS-W 8.5.0.0 o or later versions in a Mobility Master-Managed Device topology.	AOS-W 8.5.0.2
AOS-196457	–	High radio noise floor is observed on APs. This issue is observed in OAW-AP515 access points running AOS-W 8.5.0.2 or later versions.	AOS-W 8.5.0.2
AOS-196864	–	Although a new VLAN ID is successfully connected, the managed device displays that the VLAN ID fails with a different ID. This issue is observed when new VLANs are added and the total number of VLANs are 100/101, 200/201, 300/301 and so on. This issue is observed in managed devices running AOS-W 8.5.0.3 or later versions.	AOS-W 8.5.0.3
AOS-196878 AOS-197216	–	The **Datapath** process crashes on a managed device. The log file lists the reason for the event as **wlan-n09-nc1.gw.illinois.edu.** This issue is observed in managed devices running AOS-W 8.5.0.2 or later versions.	AOS-W 8.5.0.2

Table 7: *Known Issues in AOS-W 8.6.0.17*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-197023	–	Mobility Master sends incorrect AP regulatory-domain-profile channel changes to the managed device during the initial configuration propagation. This issue is observed in Mobility Masters running AOS-W 8.0.0.0 or later versions. **Workaround:** Perform one of the following steps to resolve the issue: ■ In the CLI, execute the **ap regulatory-domain-profile** command to create an AP regulatory-domain-profile without any channel configuration, save the changes, and later add or delete channels as desired. ■ In the WebUI, create an AP regulatory-domain-profile with default channel selected, save the changes, and later add or delete channels as desired in the **Configuration > AP Groups** page.	AOS-W 8.5.0.4
AOS-198024	–	Users are unable to access any page after the fifth page using the **Maintenance > Access Point** page in the WebUI. This issue is observed in stand-alone switches running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.0
AOS-198281	–	The details of the **Up** time in **Managed network > Dashboard > Access Points > Access Points** table does not get updated correctly. This issue is observed in Mobility Masters running AOS-W 8.2.2.6 or later versions.	AOS-W 8.2.2.6
AOS-198483	–	WebUI does not have an option to map the **rf dot11-60GHz-radio-profile** to an AP group. This issue is observed in Mobility Masters running AOS-W 8.5.0.4 or later versions.	AOS-W 8.5.0.4
AOS-198849 AOS-198850	–	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 an error message, **Feature is not enabled in the license.** This issue is observed in stand-alone switches running AOS-W 8.5.0.3 or later versions.	AOS-W 8.5.0.3
AOS-198991	–	Users are unable to add a VLAN to an existing trunk port using the **Configuration > Interfaces > VLANs** page of the WebUI. This issue is observed in Mobility Masters running AOS-W 8.6.0.1 or later versions.	AOS-W 8.6.0.2
AOS-199492	–	Some APs do not get displayed in the **show airgroup aps** command output and the auto-associate policy does not work as expected. This issue occurs when the AirGroup domain is in distributed mode and is not validated in a cluster deployment. This issue is observed in managed devices running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.0
AOS-200515 AOS-219987	–	The **DDS** process crashes on managed devices running AOS-W 8.3.0.10 or later versions.	AOS-W 8.3.0.10

Table 7: *Known Issues in AOS-W 8.6.0.17*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-200733	–	Some APs running AOS-W 8.5.0.3 or later versions crash and reboot unexpectedly. The log file lists the reason for the event as **kernel page fault at virtual address 00005654, epc == c0bd7dd4, ra == c0bf95f8.**	AOS-W 8.5.0.3
AOS-200765	–	Some managed devices running AOS-W 8.3.0.7 or later versions in a cluster setup log the error message, **<199804> <4844> |authmgr| |cluster| gsm_auth.c, auth_gsm_publish_ip_user_local_section:1011: auth_gsm_publish_ip_user_local_section: ip_user_local_flags.**	AOS-W 8.3.0.7
AOS-201042	–	A large number of packet drops are observed in a few APs running AOS-W 8.3.0.6 or later versions. This issue occurs when the AP SAP MTU datapath tunnel is set to 1514.	AOS-W 8.3.0.6
AOS-201376	–	The measured power, **Meas. Pow** column in the **show ap debug ble-table** command does not get updated when the TX power of an AP is changed. This issue is observed in APs running AOS-W 8.5.0.6 or later versions.	AOS-W 8.5.0.6
AOS-201428	–	The **show log all** command does not display output in a chronological order. This issue is observed in Mobility Masters running AOS-W 8.3.0.0 or later versions.	AOS-W 8.3.0.0
AOS-201439 AOS-201448	–	Some OAW-AP303H access points running AOS-W 8.5.0.5 or later versions crash and reboot unexpectedly. The log file lists the reason for the event as **PC is at skb_panic+0x5c/0x68**.	AOS-W 8.5.0.5
AOS-202129 AOS-204127	–	The **Configuration > AP groups** page does not have the **Split radio** toggle button to enable the tri-radio feature. This issue is observed in stand-alone switches running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.0
AOS-202426 AOS-203652	–	Some 510 Series access points running AOS-W 8.6.0.4 crash and reboot unexpectedly. The log files list the reason for the event as **PC is at: wlc_phy_enable_hwaci_28nm+0x938 - undefined instruction: 0 [#1]**.	AOS-W 8.6.0.4
AOS-202552 AOS-203990	–	The **Dashboard > Traffic Analysis > AppRF** page of the WebUI displays **Unknown** for WLANs, Roles, and Devices. This issue is observed in Mobility Masters running AOS-W 8.3.0.0 or later versions.	AOS-W 8.3.0.0
AOS-203201	–	A managed device is unable to download configurations from the Mobility Master using VPNC. This issue is observed in managed devices running AOS-W 8.2.2.6 or later versions.	AOS-W 8.2.2.6

Table 7: *Known Issues in AOS-W 8.6.0.17*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-203336	–	The **Dashboard > Infrastructure > Access Points** page of the WebUI and the **show log** command display different values for the last AP reboot time. This issue is observed in stand-alone switches running AOS-W 8.5.0.5 or later versions.	AOS-W 8.5.0.5
AOS-203438	–	The configuration for EIRP made using the WebUI is not visible in stand-alone switches running AOS-W 8.6.0.3 or later versions.	AOS-W 8.6.0.3
AOS-203614 AOS-209261	–	The Mobility Master dashboard does not display the number of APs and clients present in the network. This issue is observed in Mobility Masters running AOS-W 8.6.0.2 or later versions.	AOS-W 8.6.0.2
AOS-203682	–	The **Dashboard > WLANs** page of the WebUI does not display the list of all the clients and APs. This issue is observed in Mobility Masters running AOS-W 8.5.0.2 or later versions. **Duplicates:** AOS-195432, AOS-195433, AOS-218290, and AOS-220829	AOS-W 8.6.0.15
AOS-204414	–	The VLAN range configured using the **ntp-standalone vlan-range** command is not correctly sent to the managed devices. This issue occurs when the user repeatedly modifies the VLAN range. This issue occurs in Mobility Masters running AOS-W 8.0.1.0 or later versions. **Workaround:** Delete the VLAN range configured on the Mobility Master and re-configure the **ntp-standalone vlan-range.**	AOS-W 8.3.0.8
AOS-205319 AOS-206993 AOS-216577 AOS-218524	–	Some APs running AOS-W 8.6.0.5 or later versions crash and reboot unexpectedly. The log file lists the reason as **Reboot caused by kernel panic: Fatal exception in interrupt**.	AOS-W 8.6.0.5
AOS-206178	–	System logs do not display the reason why an AP has shut down. This issue is observed in Mobility Masters running AOS-W 8.6.0.4 or later versions.	AOS-W 8.6.0.4
AOS-206541	–	The **Maintenance > Software Management** page does not display the list of all managed devices that are part of a cluster. This issue is observed in Mobility Masters running AOS-W 8.5.0.8 or later versions.	AOS-W 8.5.0.8
AOS-206601	–	Some OAW-AP535 access points running AOS-W 8.7.0.0 or later versions crash unexpectedly. The log files list the reason for the event as **crash: hif_ce.c:566 Assertion ce_ret == CE_SUCCESS Thread name : WLAN_HIF**. This issue occurs when, ■ there is continuous bi-directional traffic flow in a mixed-client network. ■ channels are busy.	AOS-W 8.7.0.0

Table 7: *Known Issues in AOS-W 8.6.0.17*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-206752	–	The console log of OAW-4450 switches running AOS-W 8.5.0.9 or later versions displays the **ofald| |sdn| ERRS ofconn_rx:476 <10.50.1.26:6633> socket read failed, err:Resource temporarily unavailable(11)** message.	AOS-W 8.5.0.9
AOS-206795	–	A user is unable to rename a node from the Mobility Master node hierarchy. This issue is observed in Mobility Masters running AOS-W 8.3.0.7 or later versions. **Workaround:** Restart **profmgr** process to rename the node.	AOS-W 8.3.0.7
AOS-206890	–	The **body** field in the **Configuration > Services > Guest Provisioning** page of the WebUI does not allow users to add multiple paragraphs for email messages. This issue is observed in Mobility Masters running AOS-W 8.6.0.4 or later versions.	AOS-W 8.6.0.4
AOS-206902 AOS-208241	–	AirGroup users are unable to connect to Sonos speakers. This issue is observed in managed devices running AOS-W 8.5.0.9 or later versions.	AOS-W 8.5.0.9
AOS-207006 AOS-215138	–	APs go down and UDP 8209 traffic is sent without UDP 4500 traffic. This issue is observed in managed devices running AOS-W 8.6.0.4 or later versions.	AOS-W 8.6.0.4
AOS-207245	–	Some managed devices running AOS-W 8.5.0.8 or later versions crash and reboot unexpectedly. The log file lists the reason for the event as **Hardware Watchdog Reset (Intent:cause:register 53:86:0:802c).**	AOS-W 8.5.0.8
AOS-207366	–	The **show advanced options** menu is not available in the **Configuration > Access Points > Campus APs** page of the WebUI. This issue occurs when more than one AP is selected. This issue is observed in Mobility Masters running AOS-W 8.3.0.13.	AOS-W 8.3.0.13
AOS-207692	–	Some managed devices running AOS-W 8.6.0.4 or later versions log multiple authentication error messages.	AOS-W 8.6.0.4
AOS-208853	–	Some OAW-AP555 access points in bridge mode do not transmit multicast traffic at the configured multicast rate and continue to transmit multicast traffic at the lowest default tx-rate. This issue is observed in OAW-AP555 access points running AOS-W 8.6.0.5 or later versions.	AOS-W 8.6.0.5
AOS-208957 AOS-229568	–	Some APs are stuck in ID flag. This issue is observed in APs running AOS-W 8.6.0.10 or later versions. **Workaround:** Reboot the APs to resolve the issue.	AOS-W 8.6.0.10
AOS-209888 AOS-224884 AOS-228474	–	The **Diagnostics > Tools > AAA Server Test** page of the WebUI displays the **Authentication** status as **0** instead of **Authentication Successful**. This issue is observed in managed devices running AOS-W 8.6.0.14 or later versions.	AOS-W 8.6.0.14

Table 7: *Known Issues in AOS-W 8.6.0.17*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-209912	–	A few managed devices fail to filter and drop spoofed ARP responses from the clients. The user entry for the other IP address was present on the managed devices but not in the route cache table. This issue is observed in managed devices running AOS-W 8.6.0.5 or later versions.	AOS-W 8.6.0.5
AOS-209977	–	SNMP query with an incorrect string fails to record the offending IP address. This issue is observed in managed devices running AOS-W 8.5.0.10 or later versions.	AOS-W 8.5.0.10
AOS-210198	–	The **Dashboard > Security > Detected Radio** page of the WebUI displays incorrect number of **Clients**. This issue is observed in Mobility Masters running AOS-W 8.6.0.5 or later versions.	AOS-W 8.6.0.5
AOS-210482	–	Some managed devices running AOS-W 8.3.0.6 or later versions display the error message, **Invalid set request** while configuring ESSID for a Beacon Report Request profile.	AOS-W 8.3.0.6
AOS-210490	–	Some managed devices running AOS-W 8.5.0.8 or later versions display the error message, **Error: Tunnel is part of a tunnel-group** while deleting an L2 GRE tunnel which is not a part of any tunnel group.	AOS-W 8.5.0.8
AOS-210992	–	The Mobility Master displays an error message, **Flow Group delete: id not found** after an upgrade. This issue occurs when logging levels are not configured correctly. This issue is observed in Mobility Masters running AOS-W 8.6.0.5 or later versions.	AOS-W 8.6.0.5
AOS-211658	–	A few clients are unable to connect to OAW-AP535 access points running AOS-W 8.6.0.5 or later versions in a cluster setup. This issue occurs when WMM and HT configurations are enabled.	AOS-W 8.6.0.5
AOS-212038	–	The **show memory <process-name>** command does not display information related to the **dpagent** process. This issue is observed in managed devices running AOS-W 8.6.0.5 or later versions.	AOS-W 8.6.0.5
AOS-212255	–	Some APs are stuck in **Not in Progress** state during cluster live upgrade. This issue is observed in managed devices running AOS-W 8.5.0.10 or later versions.	AOS-W 8.5.0.10
AOS-212772 AOS-221882	–	Some IPv6 clients are unable to access websites that have only IPv4 addresses. This issue is observed in Mobility Masters running AOS-W 8.3.0.7 or later versions.	AOS-W 8.3.0.7
AOS-214575 AOS-228506	–	A few APs running AOS-W 8.3.0.13 or later versions take a long time to come up on the Mobility Controller Virtual Appliance. This issue occurs when,	AOS-W 8.3.0.13

Table 7: *Known Issues in AOS-W 8.6.0.17*

New Bug ID	Old Bug ID	Description	Reported Version
		▪ factory reset APs are re-provisioned from Mobility Master Hardware Appliances. ▪ the IP address of the Mobility Controller Virtual Appliance is configured as the LMS IP address in the AP system profile.	
AOS-215669	–	Some managed devices running AOS-W 8.6.0.7 or later versions crash and reboot unexpectedly. The log file lists the reason for the event as **Datapath timeout (Heartbeat Initiated) (Intent:cause:register 53:86:50:4)**.	AOS-W 8.6.0.7
AOS-215727 AOS-216896 AOS-217593	–	Stale AP entries that were cleared using the **clear gap-db** command prior to the upgrade reappears on the Mobility Master after the upgrade. This issue is observed in Mobility Masters running AOS-W 8.5.0.11 or later versions.	AOS-W 8.5.0.11
AOS-215852	–	Mobility Masters running AOS-W 8.6.0.6 or later versions log the error message, **ofa: 07765|ofproto|INFO|Aruba-SDN: 1 flow_mods 28 s ago (1 modifications).** This issue occurs when openflow is enabled and 35 seconds is configured as UCC session idle timeout.	AOS-W 8.6.0.6
AOS-217890	–	Some managed devices running AOS-W 8.5.0.10 or later versions crash and reboot unexpectedly. The log file lists the reason for the event as, **Datapath timeout (SOS Assert)**.	AOS-W 8.5.0.10
AOS-220515	–	Some managed devices running AOS-W 8.0.0.0 or later versions display the error message, **|fpapps| filling up the default gateway configuration.**	AOS-W 8.5.0.12
AOS-220903	–	The **s** flag indicating LACP striping is not displayed in the output of the **show ap database long** command even if LLDP is enabled on two uplinks. This issue is observed in APs running AOS-W 8.6.0.8 or later versions.	AOS-W 8.6.0.8
AOS-222290 AOS-229250	–	Memory leak is observed in the **cli** process. This issue occurs when multiple CLI commands are executed without logging out from the session for a long period of time. This issue is observed in Mobility Masters running AOS-W 8.0.0.0 or later versions.	AOS-W 8.5.0.13
AOS-224081 AOS-224083 AOS-225940	–	The **Dashboard > Overview> WLANs** page of the WebUI displays incorrect **Usage** value. This issue is observed in managed devices running AOS-W 8.5.0.10 or later versions in a cluster setup.	AOS-W 8.5.0.10
AOS-225070	–	The AirGroup server table incorrectly displays duplicate host names. This issue is observed in managed devices running AOS-W 8.6.0.11 or later versions.	AOS-W 8.6.0.11

Table 7: *Known Issues in AOS-W 8.6.0.17*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-225135	–	Clients connected to APs are unable to send or receive data packets from APs. This issue occurs when the ACL changes are not updated on APs. This issue is observed in APs running AOS-W 8.6.0.9 or later versions.	AOS-W 8.6.0.9
AOS-225214	–	A few managed devices incorrectly send the VPNC IP address as 0.0.0.0 to the OmniVista 3600 Air Manager server. This issue is observed in managed devices running AOS-W 8.5.0.6 or later versions.	AOS-W 8.5.0.6
AOS-225268	–	Some OAW-RAPs are assigned to incorrect nodes. This issue is observed in managed devices running AOS-W 8.7.1.3 or later versions in a cluster setup.	AOS-W 8.7.1.3
AOS-226331	–	The MTU discovery does not work as expected when the OAW-RAP is connected to the VRRP virtual IP of the switch. This issue is observed in stand-alone switches running AOS-W 8.6.0.9 or later versions.	AOS-W 8.6.0.9
AOS-226683	–	The **show running-config** command does not display information related to IP RADIUS source-interface loopback. However, the **show configuration effective detail** command displays information about the IP RADIUS source-interface loopback. This issue is observed in managed devices running AOS-W 8.5.0.12 or later versions.	AOS-W 8.5.0.12
AOS-226880	–	The LLDP process returns incorrect value for **lldpLocSysName**. This issue occurs due to memory corruption. This issue is observed in managed devices running AOS-W 8.6.0.9 or later versions.	AOS-W 8.6.0.9
AOS-227016 AOS-229420	–	Some users experience a delay while downloading the VIA VPN profile. This issue is observed in managed devices running AOS-W 8.6.0.9 or later versions.	AOS-W 8.6.0.9
AOS-227076 AOS-226143	–	AppRF fails to classify traffic for a few applications. This issue is observed in stand-alone switches running AOS-W 8.5.0.12 or later versions.	AOS-W 8.5.0.12
AOS-227258	–	The **Dashboard > Overview** page of the WebUI displays the status of 2.4 GHz radio even when 2.4 GHz radio was disabled in the rf dot11g-radio-profile. This issue is observed in managed devices running AOS-W 8.6.0.9 or later versions.	AOS-W 8.6.0.9
AOS-227300	–	Some OAW-AP555 access points running AOS-W 8.6.0.9 or later versions crash and reboot unexpectedly. The log files list the reason for the event as **error: kernel panic: Fatal exception in interrupt**. This issue occurs due to memory leak.	AOS-W 8.6.0.9

Table 7: *Known Issues in AOS-W 8.6.0.17*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-227324	–	The **ofc_cli_agent** process crashes on Mobility Masters running AOS-W 8.6.0.13 or later versions. This issue occurs when the **show openflow-controlller ports** command is executed.	AOS-W 8.6.0.13
AOS-227350 AOS-227420	–	A few OAW-AP505 access points are unable to download images using FTP server. This issue is observed in OAW-AP505 access points running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.8
AOS-227454	–	Users are unable to connect to IKEv1 authenticated VIA. This issue occurs when **isakmd** process is stuck is busy state. This issue is observed in OAW-4750XM switches running AOS-W 8.6.0.7 or later versions.	AOS-W 8.6.0.7
AOS-227719	–	The **Dashboard > Infrastructure** page of the WebUI displays an incorrect **UPTIME** of the Mobility Master. This issue occurs when the Mobility Master has been UP for more than a year. This issue is observed in Mobility Masters running AOS-W 8.5.0.13 or later versions.	AOS-W 8.5.0.13
AOS-228104	–	Some OAW-AP535 access points running AOS-W 8.6.0.16 or later versions crash unexpectedly. The log files list the reason for the event as **Firmware Assert - PC : 0x4b1ce6dc, whal_reset.c:943 Assertion (wait < wait_timeout) failedparam0**. This issue occurs when, ■ there is continuous bi-directional traffic flow in a mixed-client network. ■ channels are busy.	AOS-W 8.6.0.16
AOS-228318	–	Some OAW-AP535 aceess points running AOS-W 8.6.0.16 or later versions crash unexpectedly. The log files list the reason for the event as **Firmware Assert - PC: 0x4b1ce6dc, ar_wal_tx_de.c:68 Assertion 0 failedparam0 :zero.** This issue occurs when, ■ there is continuous bi-directional traffic flow in a mixed-client network. ■ channels are busy.	AOS-W 8.6.0.16
AOS-228356	–	The **detect-wireless-hosted-network** and **protect-wireless-hosted-network** parameters of the **ids unauthorized-device-profile** command does not work as expected in stand-alone switches running AOS-W 8.6.0.13 or later versions.	AOS-W 8.6.0.13
AOS-228375	–	Some OAW-AP515 access points running AOS-W 8.6.0.15 or later versions crash unexpectedly. The log files list the reason for the event as **esp_ output+0x3e8/0x588/LR:tun_net_xmit+0x5e8/0xb60**.	AOS-W 8.6.0.15

Table 7: *Known Issues in AOS-W 8.6.0.17*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-228429	–	A few clients are unable to obtain the correct role from the ClearPass Policy Manager. This issue is observed in Mobility Masters running AOS-W 8.5.0.13 or later versions.	AOS-W 8.5.0.13
AOS-228495 AOS-230660 AOS-231656	–	Some OAW-AP535 access points running AOS-W 8.6.0.16 or later versions crash unexpectedly. The log files list the reason for the event as **FW crash: wal_soc_dev_hw.c:630 Assertion 0 failed**. This issue occurs when, ■ there is continuous bi-directional traffic flow in a mixed-client network. ■ channels are busy.	AOS-W 8.6.0.16
AOS-228714	–	APs located in different geographical locations are incorrectly present in the same AirMatch partition. This issue occurs when interferers with same MAC address is present at different geographical locations. This issue is observed in APs running AOS-W 8.6.0.14 or later versions.	AOS-W 8.6.0.14
AOS-229049 AOS-230190	–	The **Maintenance > Software Management** page of the parent node hierarchy displays the list of all individual switches instead of clusters and hence, users are unable to upgrade multiple clusters. This issue is observed in Mobility Masters running AOS-W 8.8.0.2 or later versions.	AOS-W 8.8.0.2
AOS-229114	–	Some OAW-4750XM switches running AOS-W 8.6.0.10 or later versions crash and reboot unexpectedly. The log files list the reason for the event as **Reboot Cause: Kernel Panic (Intent:cause:register 12:86:e0:2)**	AOS-W 8.6.0.10
AOS-229190	–	The **Dashboard > Overview > Wireless Clients** page of the WebUI does not display any value for the **Active Controller** and **Standby Controller** fields for a few clients. This issue is observed in Mobility Masters running AOS-W 8.6.0.17.	AOS-W 8.6.0.17
AOS-229205	–	A few OAW-AP515 access points running AOS-W 8.6.0.15 or later versions crash and reboot unexpectedly. The log files list the reason for the event as **Reboot reason: SomeCrash Warm-reset**.	AOS-W 8.6.0.15
AOS-229206	–	The output of the **show ap debug radio-stats ap-name** command incorrectly displays **0** for **Avail TX Buffers**. This issue is observed in Mobility Masters running AOS-W 8.6.0.10 or later versions.	AOS-W 8.6.0.10
AOS-229319	–	Some clients in decrypt-tunnel mode were deautheticated and sapcp ageout is also observed in management frames. This issue is observed in managed devices running AOS-W 8.6.0.9 or later versions.	AOS-W 8.6.0.9

Table 7: *Known Issues in AOS-W 8.6.0.17*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-229947	–	The **stm** process crashes on managed devices running AOS-W 8.6.0.16 or later versions in a cluster setup. This issue occurs when the operating mode of the AP is changed from AP mode to AM mode.	AOS-W 8.6.0.16
AOS-230242	–	The **Configuration > WLANs** page of the WebUI does not display the list of available WLANs. This issue is observed in Mobility Masters running AOS-W 8.6.0.15 or later versions.	AOS-W 8.6.0.15
AOS-230310	–	Some OAW-AP535 access points running AOS-W 8.7.1.4 or later versions crash unexpectedly. The log files list the reason for the event as **Reboot caused by kernel panic: Take care of the TARGET ASSERT first**.	AOS-W 8.7.1.4
AOS-231083	–	Some OAW-AP555 access points running AOS-W 8.7.1.7 or later versions crash and reboot unexpectedly. The log files list the reason for the event as **Reboot caused by kernel panic: Take care of the TARGET ASSERT first.**	AOS-W 8.7.1.7
AOS-231206	–	The **wpa3_sae** process crashes is stuck in **PROCESS_NOT_RESPONDING_CRITICAL** state. This issue occurs due to a timer corruption. However, this issue does not affect the connectivity of clients that are already connected. This issue is observed in Mobility Masters running AOS-W 8.6.0.17.	AOS-W 8.6.0.17
AOS-231305	–	Cluster live upgrade fails when the cluster profile name has the special characters, **$** or **'**. This issue is observed in managed devices running AOS-W 8.6.0.17.	AOS-W 8.6.0.17
AOS-231317	–	The **auth** process crashes on managed devices running AOS-W 8.6.0.16 or later versions. This issue occurs due to race condition when a bridge mode user is idled out.	AOS-W 8.6.0.16
AOS-231393	–	The output of the **show running-config** command does not display the crypto-local isakmp route that was added to advertise the subnet of the managed device to VPNC. This issue occurs when the WAN uplink interface is down. This issue is observed in managed devices running AOS-W 8.6.0.16 or later versions.	AOS-W 8.6.0.16
AOS-231849	–	Mesh Portal APs do not change channels even after AirMatch changes the channels. This issue is observed in APs that have only mesh vaps configured. This issue is observed in APs running AOS-W 8.6.0.16 or later versions. **Workaround:** Configure a **wlan virtual-ap profile <name>** to resolve the issue.	AOS-W 8.6.0.16
AOS-231996	–	Some OAW-AP555 access points running AOS-W 8.7.1.4 or later versions crash and reboot unexpectedly. The log files list the reason for the event as **Take care of the TARGET ASSERT first - wmi_svc.c:490 Assertion 0 fail.**	AOS-W 8.7.1.4

Table 7: *Known Issues in AOS-W 8.6.0.17*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-232129	–	Some OAW-AP535 aceess points running AOS-W 8.6.0.16 or later versions crash unexpectedly. The log files list the reason for the event as **NOC_error.c:476 NOCError: FATAL ERRORparam0 :zero, param1 :zero, param2 :zero.** This issue occurs when, ■ there is continuous bi-directional traffic flow in a mixed-client network. ■ channels are busy.	AOS-W 8.6.0.16
AOS-232165	–	Users are unable to upgrade a cluster using the WebUI. This issue occurs when the cluster name has the special character, **#**. However, CLI allows to upgrade the cluster. This issue is observed in managed devices running AOS-W 8.6.0.17.	AOS-W 8.6.0.16
AOS-232230	–	Some managed devices running AOS-W 8.6.0.17 fail to classify Skype calls.	AOS-W 8.6.0.17

Chapter 8
Upgrade Procedure

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

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

Important Points to Remember

To upgrade your managed device or Mobility Master:

- Schedule the upgrade during a maintenance window and notify your community of the planned upgrade. This prevents users from being surprised by a brief wireless network outage during the upgrade.
- Avoid making any changes to your network, such as configuration changes, hardware upgrades, or changes to the rest of the network during the upgrade. This simplifies troubleshooting.
- Know your network and verify the state of the network by answering the following questions:
  - How many APs are assigned to each managed device? Verify this information by navigating to the **Dashboard > Access Points** page in the WebUI, or by executing the **show ap active** or **show ap database** commands.
  - How are those APs discovering the managed device (DNS, DHCP Option, Broadcast)?
  - What version of AOS-W runs on your managed device?
  - Are all managed devices running the same version of AOS-W?
  - What services are used on your managed device (employee wireless, guest access, OAW-RAP, wireless voice)?
- Resolve any existing issues (consistent or intermittent) before you upgrade.
- If possible, use FTP to load AOS-W images to the managed device. FTP is faster than TFTP and offers more resilience over slow links. If you must use TFTP, ensure the TFTP server can send over 30 MB of data.
- Always upgrade the non-boot partition first. If you encounter any issue during the upgrade, you can restore the flash, and switch back to the boot partition. Upgrading the non-boot partition gives you a smoother downgrade path, if required.
- Before you upgrade to this version of AOS-W, assess your software license requirements and load any new or expanded licenses that you might require. For a detailed description of these new license modules, refer the *Alcatel-Lucent Mobility Master Licensing Guide*.
- Multiversion is supported in a topology where the managed devices are running the same version as the Mobility Master, or two versions lower. For example multiversion is supported if a Mobility Master is running AOS-W 8.5.0.0 and the managed devices are running AOS-W 8.5.0.0, AOS-W 8.4.0.0, or AOS-W 8.3.0.0.

Memory Requirements

All Alcatel-Lucent managed devices store critical configuration data on an onboard compact flash memory module. Ensure that there is always free flash space on the managed device. Loading multiple large files such as

JPEG images for RF Plan can consume flash space quickly. Following are best practices for memory management:

- Do not proceed with an upgrade unless 100 MB of free memory is available. Execute the **show memory** command to identify the available free memory. To recover memory, reboot the managed device. After the managed device comes up, upgrade immediately.
- Do not proceed with an upgrade unless the minimum flash space inis available. Execute the **show storage** command to identify the available flash space. If the output of the **show storage** command indicates that there is insufficient flash memory, free some used memory. Copy any log files, crash data, or flash backups from your the managed device to a desired location. Delete the following files from the managed device to free some memory:
  - **Crash data:** Execute the **tar crash** command to compress crash files to a file named **crash.tar**. Use the procedures described in Backing up Critical Data on page 50 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 50 to back up the flash directory to a file named **flash.tar.gz**. Execute the **tar clean flash** command to delete the file from the managed device.
  - **Log files:** Execute the **tar logs** command to compress log files to a file named **logs.tar**. Use the procedures described in Backing up Critical Data on page 50 to copy the **logs.tar** file to an external server. Execute the **tar clean logs** command to delete the file from the managed device.

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

Deleting a File

You can delete a file using the WebUI or CLI.

In the WebUI

From the Mobility 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
- Log files
- Flash backup

Backing up and Restoring Flash Memory

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

In the WebUI

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

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

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

In the CLI

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

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

```
(host) #write memory
```

2. Execute the following command to back up the contents of the flash memory to the **flashbackup.tar.gz** file.

```
(host) #backup flash
Please wait while we take the flash backup.......
File flashbackup.tar.gz created successfully on flash.
Please copy it out of the controller and delete it when done.
```

3. Execute either of the following command to transfer the flash backup file to an external server or storage device.

```
(host) #copy flash: flashbackup.tar.gz ftp: <ftphost> <ftpusername> <ftpuserpassword>
<remote directory>


(host) #copy flash: flashbackup.tar.gz usb: partition <partition-number>
```

   You can transfer the flash backup file from the external server or storage device to the flash memory by executing either of the following command:

```
(host) #copy tftp: <tftphost> <filename> flash: flashbackup.tar.gz

(host) #copy usb: partition <partition-number> <filename> flash: flashbackup.tar.gz
```

4. Execute the following command to untar and extract the **flashbackup.tar.gz** file to the flash memory.

```
(host) #restore flash
Please wait while we restore the flash backup........
Flash restored successfully.
Please reload (reboot) the controller for the new files to take effect.
```

Upgrading AOS-W

Upgrade AOS-W using the WebUI or CLI.

CAUTION

Ensure that there is enough free memory and flash space on your Mobility Master or managed device. For details, see Memory Requirements on page 49.

NOTE

When you navigate to the **Configuration** tab in the WebUI, the managed device might display the **Error getting information: command is not supported on this platform** message. This message is displayed ccurs when you

upgrade using the WebUI and navigate to the **Configuration** tab after the managed device reboots. This message disappears after clearing the Web browser cache.

In the WebUI

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

1. Download the AOS-W image from the customer support site.
2. Upload the AOS-W image to a PC or workstation on your network.
3. Validate the SHA hash for the AOS-W image:
   a. Download the **Alcatel.sha256** file from the download directory.
   b. Load the AOS-W image to a Linux system and execute the **sha256sum <filename>** command. Alternatively, use a suitable tool for your operating system that can generate a **SHA256** hash of a file.
   c. Verify that the output produced by this command matches the hash value found on the customer support site.

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** option from the **Upgrade using** drop-down list.
   b. Click **Browse** from the **Image file name** to navigate to the saved image file on your PC or workstation.
6. Select the downloaded image file.
7. Choose the partition from the **Partition to Upgrade** option.
8. Enable the **Reboot Controller After Upgrade** toggle switch to automatically reboot after upgrading. If you do not want to reboot immediately, disable this option.

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 the 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 partition. The partition number appears in the **Partition** row; **0:0** is partition 0, and **0:1** is partition 1. The active boot partition is marked as **Default boot**.

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

5. Execute the **copy** command to load the new image to the non-boot partition.

```
(host)# copy ftp: <ftphost> <ftpusername> <image filename> system: partition <0|1>
```

or

```
(host)# copy tftp: <tftphost> <image filename> system: partition <0|1>
```

or

```
(host)# copy scp: <scphost> <scpusername> <image filename> system: partition <0|1>
```

or

```
(host)# copy usb: partition <partition-number> <image filename> system: partition <0|1>
```

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

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

7. Reboot the Mobility Master.

```
(host)#reload
```

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

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

Verifying the AOS-W Upgrade

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

In the WebUI

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

1. Log in to the WebUI and navigate to the **Dashboard > WLANs** page to verify the AOS-W image version.
2. Verify if all the managed devices are up after the reboot.
3. Navigate to the **Dashboard > Access Points** page to determine if your APs are up and ready to accept clients.
4. Verify that the number of APs and clients are as expected.
5. Test a different type of client in different locations, for each access method used.
6. Complete a backup of all critical configuration data and files on the flash memory to an external server or mass storage facility. See Backing up Critical Data on page 50 for information on creating a backup.

In the CLI

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 version** command to verify the AOS-W image version.
3. Execute the **show ap active** command to determine if your APs are up and ready to accept clients.
4. Execute the **show ap database** command to verify that the number of APs and clients are as expected.
5. Test a different type of client in different locations, for each access method used.
6. Complete a backup of all critical configuration data and files on the flash memory to an external server or mass storage facility. See Backing up Critical Data on page 50 for information on creating a backup.

Downgrading AOS-W

A 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 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 50.
2. Verify that the control plane security is disabled.
3. Set the Mobility Master or managed device to boot with the previously saved configuration file.
4. Set the Mobility Master or managed device to boot from the partition that contains the pre-upgrade 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 the 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 is unchanged, do not import it. If the RF plan was changed before switching the boot partition, the changed RF plan does not appear in the downgraded AOS-W version.
- If any new certificates were added in the upgraded AOS-W version, reinstall these certificates in the downgraded AOS-W version.

Downgrade AOS-W version using the WebUI or CLI.

In the WebUI

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

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

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

   a. Enter the FTP or TFTP server address and image file name.
   b. Select the backup system partition.
   c. Enable **Reboot Controller after upgrade**.
   d. Click **Upgrade**.

3. Navigate to the **Maintenance > Software Management > Reboot** page, select **Save configuration before reboot**, and click **Reboot**.

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

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

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

or

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

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

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

3. Execute the **show image version** command to view the partition on which your pre-upgrade AOS-W version is stored.

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

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

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

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

5. Reboot the Mobility 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 the Technical Support:

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