AOS-W 8.6.0.6

Alcatel·Lucent Enterprise

Release Notes

Copyright Information

Open Source Code

Revision History

The following table provides the revision history of this document.

Table 1: *Revision History*

Revision	Change Description
Revision 02	Updated the **Important Points to Remember** section.
Revision 01	Initial release.

This AOS-W release notes includes the following topics:

NOTE

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

- New Features and Enhancements on page 8
- Supported Platforms on page 9
- Regulatory Updates on page 12
- Resolved Issues on page 13
- Known Issues and Limitations on page 29
- Upgrade Procedure on page 37

For a list of terms, refer to the Glossary.

Important Point Before Upgrading to AOS-W 8.6.0.0

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

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

Contacting Support

Table 2: *Contact Information*

Contact Center Online	
Main Site	https://www.al-enterprise.com
Support Site	https://businessportal2.alcatel-lucent.com
Email	ebg_global_supportcenter@al-enterprise.com
Service & Support Contact Center Telephone	
North America	1-800-995-2696
Latin America	1-877-919-9526
EMEA	+800 00200100 (Toll Free) or +1(650)385-2193
Asia Pacific	+65 6240 8484
Worldwide	1-818-878-4507

New Features and Enhancements in AOS-W 8.6.0.6

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

CLI

ip nexthop-list command

A new sub-parameter, **probe_wan_hc_ip** has been added to the **ip <ip-addr>** and **ip dhcp vlan <vlan>** parameters to enable nexthop failover, if the uplink health check of the nexthop is unreachable.

The following CLI commands enable nexthop failover:

```
(host) [mynode] (config) #ip nexthop-list <STRING>
(host) [mynode] (config-submode)#ip <ip-addr>  probe_wan_hc_ip
```

The **probe_wan_hc_ip** sub-parameter is disabled by default.

The **show ip nexthop-list** command displays the status of the WAN health check probe.

Image Upgrade

The timeout value of the **copy scp: <scphost> <username> <filename> system: partition <partition no>** command has been increased from 15 minutes to 3 hours. This enhancement provides enough time to download AOS-W images over slower uplinks.

jQuery Version

jQuery has been upgraded to 3.4.1 version.

Supported Platforms in AOS-W 8.6.0.6

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 8.6.0.6*

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 8.6.0.6*

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-10, MC-VA-50, MC-VA-250, MC-VA-1K, MC-VA 4K, MC-VA 6K

NOTE

MC-VA-4K and MC-VA-6K are not orderable SKUs. However, you can scale up by installing multiple instances of MC-VA-1K. For example to deploy 4K APs on a single Mobility Controller Virtual Appliance, you need to add four MC-VA-1K licenses.

AP Platforms

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

Table 5: *Supported AP Platforms in AOS-W 8.6.0.6*

AP Family	AP Model
OAW-AP100 Series	OAW-AP104, OAW-AP105
OAW-AP103 Series	OAW-AP103
OAW-AP110 Series	OAW-AP114, OAW-AP115
OAW-AP130 Series	OAW-AP134, OAW-AP135
OAW-AP 170 Series	OAW-AP175AC, OAW-AP175AC-F1, OAW-AP175DC, OAW-AP175DC-F1, OAW-AP175P, OAW-AP175P-F1
OAW-AP200 Series	OAW-AP204, OAW-AP205
OAW-AP203H Series	OAW-AP203H
OAW-AP205H Series	OAW-AP205H
OAW-AP207 Series	OAW-AP207
OAW-AP203R Series	OAW-AP203R, OAW-AP203RP
OAW-AP210 Series	OAW-AP214, OAW-AP215
OAW-AP 220 Series	OAW-AP224, OAW-AP225
228 Series	OAW-AP228
OAW-AP270 Series	OAW-AP274, OAW-AP275, OAW-AP277

Table 5: *Supported AP Platforms in AOS-W 8.6.0.6*

AP Family	AP Model
OAW-AP300 Series	OAW-AP304, OAW-AP305
OAW-AP303 Series	OAW-AP303
OAW-AP303H Series	OAW-AP303H
OAW-AP310 Series	OAW-AP314, OAW-AP315
OAW-AP318 Series	OAW-AP210AP-318
OAW-AP320 Series	OAW-APAP-324, OAW-AP325
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
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 4
Regulatory Updates

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

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

For a complete list of countries and the regulatory domains in which the APs are certified for operation, refer to the Downloadable Regulatory Table or the DRT Release Notes at businessportal2.alcatel-lucent.com.

Regulatory Updates in AOS-W 8.6.0.6

The following DRT file version is part of this release:

- DRT-1.0_76935

Resolved Issues in AOS-W 8.6.0.6

This chapter describes the issues resolved in this release.

Table 6: *Resolved Issues in AOS-W 8.6.0.6*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-157462 AOS-202579	194010	The **web_cc** process crashed on managed devices running AOS-W 8.2.2.6 or later versions. The fix ensures that the managed devices work as expected.	AOS-W 8.2.2.6
AOS-188527 AOS-193897 AOS-202879	—	The IP address of the NAT configured managed device was visible in the HTTP header of the web server. The fix ensures that the IP address is not visible in the HTTP header. This issue was observed in managed devices running AOS-W 8.3.0.0 or later versions.	AOS-W 8.3.0.0
AOS-191031	—	A few 802.11ax clients experienced poor MU-MIMO performance. Enhancements to the wireless driver resolved this issue. This issue was observed in OAW-AP535 and OAW-AP555 access points running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.0
AOS-192738 AOS-197047	—	The Mobility Master list in the WebUI incorrectly displayed the MAC address of the primary Mobility Master for the secondary Mobility Master. The fix ensures that the correct MAC address of the secondary Mobility Master is displayed. This issue was observed in Mobility Masters running AOS-W 8.3.0.10 or later versions.	AOS-W 8.3.0.10
AOS-195101	—	The traffic between master redundancy Mobility Masters was dropped causing a few processes to be in **PROCESS_NOT_RESPONDING** state. Hence, configurations were not synchronized between the peers. This issue occurred when the **ipsec-mark-mgmt-frames** parameter was enabled using the **firewall wireless-bridge-aging** command. This issue was resolved by disabling the **ipsec-mark-mgmt-frames** parameter using the **firewall wireless-bridge-aging** command. This issue was observed in Mobility Masters running AOS-W 8.2.0.0 or later versions.	AOS-W 8.5.0.2
AOS-195350	—	A few OAW-AP555 access points running AOS-W 8.6.0.0 or later versions crashed unexpectedly. The fix ensures that the APs work as expected.	AOS-W 8.6.0.0

Table 6: *Resolved Issues in AOS-W 8.6.0.6*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-195939 AOS-209347	—	UBT users were assigned **logon** role when they received the same IP addresses. The fix ensures that the user roles are not changed. This issue was observed in managed devices running AOS-W 8.5.0.2 or later versions.	AOS-W 8.5.0.2
AOS-196115	—	Users were unable to configure untrusted VLAN in the **Configuration > Interfaces > Ports** page of the WebUI. The fix ensures that the users are able to configure untrusted VLAN. This issue was observed in Mobility Masters running AOS-W 8.5.0.0 or later versions.	AOS-W 8.5.0.0
AOS-196229 AOS-196264 AOS-205903	—	Random values were displayed as the host name of a Mobility Master. The fix ensures that random values are not displayed. This issue was observed in Mobility Masters running AOS-W 8.5.0.8 or later versions.	AOS-W 8.5.0.0
AOS-196541	—	The API on a Mobility Master did not operate over port 443. The fix ensures that API operates over port 443. This issue occurred when no rule was applied for login or token generation over port 443. This issue was observed in Mobility Masters running AOS-W 8.5.0.4 or later versions.	AOS-W 8.5.0.4
AOS-197048	—	Some clients experienced degraded Wi-Fi download speed after the managed device resumed function post standby mode. Enhancements to the wireless driver resolved this issue. This issue occurred when the AP did not setup an aggregation session. This issue was observed in managed devices running AOS-W 8.3.0.8 or later versions.	AOS-W 8.3.0.8
AOS-197215	—	A few users were unable to delete the **Weekend** entry in **Start Day** of **Time range** field in the WebUI. The fix ensures that users are able to delete the **Weekend** entry. This issue occurred when the users created a new policy rule in the **Configuration** > **Roles & Policies** > **Policies** > **<policy_name>** > **<new_policy_rule>** page, and selected the **Access control** radio button in the **Rule type** field of the WebUI. This issue was observed in Mobility Masters running AOS-W 8.2.2.6-FIPS or later versions.	AOS-W 8.2.2.6
AOS-198044 AOS-207046	—	The mesh topology information was not synchronized among all the managed devices in a cluster. As a result, the output of the **show ap mesh topology** command did not display full information of all mesh portals and mesh points under a specific mesh topology. The fix ensures that the mesh topology information is synchronized among all the managed devices in a cluster. This issue was observed in managed devices running AOS-W 8.5.0.0 or later versions in a cluster setup.	AOS-W 8.5.0.11
AOS-198671	—	An AP did not send authentication response frames to the client's authentication request. Enhancements to the wireless driver resolved this issue. This issue occurred due to a fake radar detection causing deferred channel change, when the CSA was enabled. This issue was observed in OAW-AP135 access points running AOS-W 8.0.0.0 or later versions.	AOS-W 8.0.0.0

Table 6: *Resolved Issues in AOS-W 8.6.0.6*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-198825	—	A managed device displayed multiple stale entries for client-match pending events. The fix ensures that all pending events are cleared and no stale entries are displayed. This issue was observed in managed devices running AOS-W 8.0.0.0 or later versions.	AOS-W 8.5.0.9
AOS-199012 AOS-198865 AOS-208289	—	A managed device crashed and rebooted unexpectedly. The log file listed the reason for the event as **Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:4)**. The fix ensures that the managed device works as expected. This issue was observed in managed devices running AOS-W 8.4.0.4 or later versions.	AOS-W 8.4.0.4
AOS-199230 AOS-208835	—	The **cfgm** process crashed unexpectedly on a Mobility Controller Virtual Appliance running AOS-W 8.5.0.5 or later versions. The fix ensures that the Mobility Controller Virtual Appliance work as expected.	AOS-W 8.5.0.5
AOS-199384 AOS-208088	—	A few APs running AOS-W 8.6.0.0 or later versions crashed and rebooted unexpectedly. The log files listed the reason for the event as **kernel panic : PC is at wlc_twt_scb_get_schedid+0x8/0x38.** Enhancements to the wireless driver resolved this issue.	AOS-W 8.6.0.0
AOS-199423 AOS-205532	—	Some L3 redundant Mobility Masters generated **profmgr** error logs. The fix ensures that the **profmgr** error logs are not generated. This issue was observed in Mobility Masters running AOS-W 8.5.0.5-FIPS.	AOS-W 8.5.0.5
AOS-199884	—	A Mobility Master logged the following error messages, **PAPI_Free: This buffer 0x4f6c48 may already be freed** and **PAPI_Free: Bad state index 0 state 0x1.** The fix ensures that the Mobility Masters work as expected. This issue was observed in Mobility Masters running AOS-W 8.5.0.5 or later versions.	AOS-W 8.5.0.5
AOS-199947	—	The **Lic. FeatureBit** parameter in the **License Client Table** changed to **enabled** for Mobility Master Virtual Appliance and Mobility Controller Virtual Appliance. The fix ensures that the **Lic. FeatureBit** parameter is disabled. This issue occurred when EVAL license was deleted and number of the licenses were displayed as 0. This issue was observed in stand-alone switches running AOS-W 8.3.0.11 or later versions.	AOS-W 8.3.0.11
AOS-199991 AOS-202416	—	A few switches forwarded gratuitous ARP packets over standby L2 GRE tunnel and this caused network broadcast loop. This issue was resolved by adding ICMP keepalive message support for GRE tunnels. This issue was observed in stand-alone switches running AOS-W 8.5.0.0 or later versions	AOS-W 8.5.0.5
AOS-200446	—	Some users were unable to change the cluster profile in the **Configuration > Services > Cluster** tab of the WebUI. The fix ensures that users are able make changes to the cluster profile. This issue occurred when there was no VRRP ID configured but the cluster profile requested for a VRRP passphrase. This issue was observed in Mobility Masters running AOS-W 8.5.0.5 or later versions.	AOS-W 8.5.0.5

Table 6: *Resolved Issues in AOS-W 8.6.0.6*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-200601 AOS-200812 AOS-207772	—	A few switches were unable to detect the Huawei E3372h-153 (HiLink Mode) 4G LTE USB Modem. The fix ensures that the switches are able to detect the modem and and connect the 4G LTE USB modem for cellular network connectivity. This issue was observed in OAW-40xx Series switches running AOS-W 8.5.0.0 or later versions.	AOS-W 8.6.0.4
AOS-200766 AOS-201434 AOS-209172	—	A few session ACL were deleted after a reload of the managed device running AOS-W 8.3.0.0 or later versions. The fix ensures that the ACLs are not deleted.	AOS-W 8.3.0.0
AOS-200801	—	A few clients were unable to connect to APs, and incorrect ACL index values were displayed in the AP datapath. The fix ensures that the APs work as expected. This issue occurred when the clients were connected through bridge mode SSID, and the **SAPM** process sent duplicate access control entries. This issue was observed in APs connected to a stand-alone switch running AOS-W 8.3.0.0 or later versions.	AOS-W 8.5.0.11
AOS-200950 AOS-203934	—	A user was unable to access previously backed up data when the new backup-logs application was installed. The fix ensures that the user is able to access the backed up data. This issue was observed in managed devices running AOS-W 8.3.0.8 or later versions.	AOS-W 8.3.0.8
AOS-201166 AOS-207939 AOS-209042	—	A switch crashed and rebooted unexpectedly after the **HTTPD** process was restarted. The log files listed the reason for the event as **Reboot cause: Nanny rebooted machine - httpd_wrap process died (Intent:cause:register 34:86:0:2c)**. The fix ensures that the switch works as expected. This issue was observed in stand-alone switches running AOS-W 8.2.0.0 or later versions.	AOS-W 8.5.0.2
AOS-201200	—	The **show tech-support** command did not display any output for **license-pool-profile** and **license-pool-profile-root** when executed in the **/mm/mynode** hierarchy. The fix ensures that the command displays the correct output. This issue was observed in Mobility Master running AOS-W 8.3.0.6 or later versions.	AOS-W 8.5.0.5
AOS-201240	—	When a trusted VLAN was added using the **Interface > Ports > Allowed VLANs** page in the WebUI, the Mobility Master automatically issued the **no trusted vlan** command. The fix ensures that the users are able to add the trusted VLAN without any errors in the **Allowed VLANs** page. This issue occurred when trunk mode was initially configured using the CLI and later modified using the WebUI. This issue was observed in managed devices running AOS-W 8.5.0.2 or later versions.	AOS-W 8.5.0.2
AOS-201273 AOS-201395	—	IPsec tunnels were not established between the Mobility Master and managed devices in an IPv6 environment, and the controller-IP address was not displayed in the managed devices. The fix ensures that the IPsec tunnels are established and the controller-IP addresses are displayed formanaged devices. This issue was observed in Mobility Masters running AOS-W 8.5.0.0 or later versions.	AOS-W 8.6.0.0

Table 6: *Resolved Issues in AOS-W 8.6.0.6*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-201519	—	A few APs running AOS-W 8.6.0.0 or later versions crashed and rebooted unexpectedly. The log files listed the reason for the event as **PC is at 0x0; LR is at ieee80211_get_txstreams**. Enhancements to the wireless driver resolved this issue.	AOS-W 8.6.0.0
AOS-201541	—	Configuring a radius modifier in the WebUI required configuring a second dynamic field but it was optional in CLI. This issue is resolved by allowing the configuration of the radius modifier without having to configure the second dynamic field in the WebUI. This issue was observed in a managed device running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.2
AOS-201674 AOS-207166	—	The **VLAN-ID/Named VLAN is invalid** error message was displayed for a few user roles on the managed device. The fix ensures that the managed device works as expected. This issue was observed in managed devices running AOS-W 8.0.0.0 or later versions.	AOS-W 8.5.0.2
AOS-201699 AOS-205472 AOS-208964 AOS-208995	—	A user was unable to send or receive traffic. This issue occurred when an ACL was unavailable for a user role. This issue was observed in managed devices running AOS-W 8.3.0.0 or later versions. The fix ensures that the managed devices work as expected.	AOS-W 8.5.0.8
AOS-201951 AOS-203578 AOS-207402	—	The **ISAKMPD** process went into busy state when VIA or a third party VPN client tried to come up in a scale scenario. The fix ensures that IKE SA INIT packets are throttled at the beginning to avoid the **ISAKMPD** process from going into a busy state continuously. This issue occurred when VIA or the third party VPN client tried to establish a tunnel in a scale setup and experienced a delay in the authentication process. This issue was observed in Mobility Masters running AOS-W 8.0.0.0 or later versions.	AOS-W 8.2.0.0
AOS-202052	—	A few APs crashed and rebooted unexpectedly. The log file listed the reason for the event as **AP Reboot reason: Panic:Out of memory Warm-reset**. The fix ensures that the APs work as expected. This issue was observed in APs running AOS-W 8.3.0.0 or later versions.	AOS-W 8.6.0.2
AOS-202126 AOS-205098	—	The **profmgr** process restarted continuously on the Mobility Master and hence configurations were not forwarded to the managed devices. The fix ensures that the configurations are forwarded to the managed device. This issue was observed in managed devices running AOS-W 8.5.0.8 or later versions.	AOS-W 8.5.0.8
AOS-202219 AOS-207452	—	The radio mode of mesh APs was incorrectly displayed as **Mesh Portal** in the **Dashboard** > **Overview**> **Radios** page in the WebUI. The fix ensures that the radio mode is displayed as **Mesh Point** in the WebUI. This issue was observed in APs running AOS-W 8.5.0.0 or later versions.	AOS-W 8.5.0.11

Table 6: *Resolved Issues in AOS-W 8.6.0.6*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-202243	—	The **Security > Authentication > Servers > Server Group** page of the WebUI displayed the error message, **Error in getting 'show aaa server-group XXXX' data:null**. The fix ensures that the Mobility Masters work as expected. This issue was observed in Mobility Masters running AOS-W 8.3.0.0 or later versions.	AOS-W 8.3.0.0
AOS-202274	—	The **TRAPD** process crashed unexpectedly in a managed device running AOS-W 8.3.0.0 or later version. The fix ensures that the managed device works as expected. This issue was observed in managed devices running AOS-W 8.3.0.0 or later versions in a Mobility Master-Managed Device topology.	AOS-W 8.5.0.3
AOS-202290	—	The **Cannot modify existing server-group from different node in config path** error message was displayed when users tried to create or modify an aaa server group. This issue occurred when similar naming conventions were used for different folders under the same hierarchy. The fix ensures that the Mobility Master works as expected. This issue was observed in Mobility Masters running AOS-W 8.5.0.6 or later versions.	AOS-W 8.5.0.6
AOS-202341	—	A managed device running AOS-W 8.3.0.8 or later versions crashed and rebooted unexpectedly. The log file listed the reason for the event as **Datapath timeout (SOS Assert) ((Intent:cause:register 54:86:0:2c).** The fix ensures that the managed devices work as expected.	AOS-W 8.3.0.8
AOS-202349	—	A few users were unable to map the captive portal authentication profile under guest-logon user role, and the **Failed to remove reference of role guest-logon captive-portal profile default** error message was displayed. The fix ensures that the users are able to map the captive portal authentication profile under guest-logon user role. This issue was observed in stand-alone switches running AOS-W 8.4.0.0 or later versions.	AOS-W 8.5.0.4
AOS-202370	—	Some managed devices reset when the **activate sync** command was issued. This issue occurred when the node paths that were configured for Activate and Mobility Master used different cases. The fix ensures that the case insensitive function is used when the two nodes are compared. This issue was observed in Mobility Masters running AOS-W 8.5.0.5 or later versions.	AOS-W 8.5.0.5
AOS-202565 AOS-206895 AOS-208205 AOS-209117	—	Some OAW-AP515 access points running AOS-W 8.5.0.2 or later versions crashed and rebooted unexpectedly. The log file listed the reason for the event as **kfree+0x74/0xf8 crash**. Enhancements to the wireless driver resolved this issue.	AOS-W 8.5.0.2
AOS-202691	—	The **Key Management** column in the **Configuration > WLANs** page of the WebUI displayed multiple **wpa2-psk-tkip** entries. The fix ensures that multiple **wpa2-psk-tkip** entries are not displayed. This issue occurred when multiple wpa2-psk-tkip opmode SSIDs were created. This issue was observed in stand-alone switches running AOS-W 8.5.0.4 or later versions.	AOS-W 8.5.0.4

Table 6: *Resolved Issues in AOS-W 8.6.0.6*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-202816 AOS-203413	—	A managed device running AOS-W 8.3.0.0 or later versions crashed and rebooted unexpectedly. The log file listed the reason for the event as **Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:60)**. The fix ensures that the managed device works as expected. This issue occurred when SSL-fallback enabled VIA clients were connected to the managed device.	AOS-W 8.3.0.0
AOS-203097	—	WebUI prompted that additional VLANs will be deleted when a user tried to delete a VLAN. This issue is resolved by removing the wrong reference of port channel with VLAN in the VLAN table. This issue was observed in stand-alone switches running AOS-W 8.3.0.10 or later versions.	AOS-W 8.3.0.10
AOS-203098	—	Tunneled user entries were deleted on managed devices running AOS-W 8.6.0.4 or later versions. This issue occurred due to multiple cluster failovers. The fix ensures that the tunneled user entries are not deleted and the clients are able to come back on the primary managed device after a failover.	AOS-W 8.6.0.4
AOS-203170	—	The class attribute field was missing in the accounting packets of the VIA connection profile. This issue occurred when IKEv2 was enabled in the VIA connection profile. This issue was observed in managed devices running AOS-W 8.4.0.1 or later versions. The fix ensures that the managed devices work as expected.	AOS-W 8.4.0.1
AOS-203183	—	Incorrect values were returned when an SNMPGet was performed in a managed device running AOS-W 8.2.0.0 or later versions. This issue occurred while collecting AP LLDP neighbor details. The fix ensures that the correct values are displayed when SNMPGET is executed.	AOS-W 8.6.0.2
AOS-203184	—	Users were unable to perform captive portal authentication when login URL of the captive portal profile pointed to ClearPass Policy Manager. The fix ensures that the users are able to perform captive portal authentication. This issue was observed in managed devices running AOS-W 8.5.0.7 or later versions.	AOS-W 8.5.0.7
AOS-203351 AOS-207895 AOS-209017	—	User derivation rules were not applied when WPA3-SAE-AES opmode was used. The fix ensures that the user derivation rules are applied. This issue was observed in managed devices running AOS-W 8.6.0.2 or later versions.	AOS-W 8.6.0.2
AOS-203357	—	Traffic outage was observed in managed devices when the role of wired user got updated as a tunneled user with a different VLAN. This issue was observed in managed devices running AOS-W 8.5.0.0 or later versions. The fix ensures that the managed devices work as expected.	AOS-W 8.5.0.10
AOS-203374	—	VIA authentication timed out although the server responded without any delay. The fix ensures that the VIA authentication works without delay. This issue was observed in OAW-4550 switches running AOS-W 8.0.0.0 or later versions.	AOS-W 8.3.0.0

Table 6: *Resolved Issues in AOS-W 8.6.0.6*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-203597 AOS-203927	—	VIA license consumption was higher than the number of users connected to VIA in managed devices running AOS-W 8.6.0.2 or later versions. The fix ensures that the number of licenses being used matches the number of users connected.	AOS-W 8.4.0.1
AOS-203602 AOS-205942	—	A few OAW-4010 switches running AOS-W 8.5.0.0 or later versions crashed and rebooted unexpectedly. The log files listed the reason for the event as **Hardware Watchdog Reset (Intent:cause:register 54:86:50:8)**. The fix ensures that the switches work as expected.	AOS-W 8.5.0.8
AOS-203652 AOS-206320 AOS-208333 AOS-209043 AOS-209044 AOS-209813	—	A few APs running AOS-W 8.6.0.4 or later versions crashed and rebooted unexpectedly. The log files listed the reason for this event as **InternalError: Oops - undefined instruction.** Enhancements to the wireless driver resolved this issue.	AOS-W 8.6.0.4
AOS-203712 AOS-205655 AOS-209193 AOS-209423	—	An Avaya Spectalink wireless client device rebooted unexpectedly with the error message, **No AVPP response from 192.168.249.001**. The fix ensures that the client device works as expected. This issue was observed in managed devices running AOS-W 8.5.0.0 or later versions.	AOS-W 8.5.0.7
AOS-203773	—	A few users were unable to access network destinations after configuring the alias for the specific network. The fix ensures that the users are able to access the network destinations. This issue occurred because the destination IP address was not configured for the network. This issue was observed in managed devices running AOS-W 8.5.0.0 or later versions.	AOS-W 8.5.0.0
AOS-203840 AOS-203935	—	A few clients were unable to obtain the DHCP IP address and pass traffic in a OAW-4104 switch running AOS-W 8.5.0.0 or later versions. The fix ensures that the clients are able to obtain the DHCP IP address and pass traffic.	AOS-W 8.5.0.0
AOS-203860	—	The VIA installer file was unable to synchronize the logo, banner, or welcome html between the Mobility Master and managed devices. The fix ensures that the VIA installer is able to synchronize all the files. This issue was observed in Mobility Masters and managed devices running AOS-W 8.3.0.0 or later versions.	AOS-W 8.3.0.0
AOS-203958	—	Blacklisted clients were visible in **Dashboard > Security > Blacklisted Clients** although these clients were removed using the WebUI. This issue was observed in Mobility Masters running AOS-W 8.6.0.2 or later versions.	AOS-W 8.6.0.4

Table 6: *Resolved Issues in AOS-W 8.6.0.6*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-204036	—	Users are unable to configure multiple route ACEs with different TCP or UDP source ports. The fix ensures that the users are able to configure ACEs with different source ports. This issue was observed in Mobility Masters running AOS-W 8.0.0.0 or later versions.	AOS-W 8.5.0.0
AOS-204057	—	A 4-way handshake was not initiated when MAC authentication failed on OWE clients in a managed device running AOS-W 8.4.0.0 or later versions. The fix ensures that the managed device works as expected.	AOS-W 8.6.0.3
AOS-204142 AOS-207644	—	A few users were assigned the default 802.1X roles from AAA profile instead of SDR-configured roles. The fix ensures that the SDR-configured roles are assigned to the users. This issue occurred when the **no cert-cn-lookup** parameter in the **aaa authentication dot1x** command was configured on the 802.1X profile. This issue was observed in managed devices running AOS-W 8.4.0.0 or later versions.	AOS-W 8.6.0.4
AOS-204334 AOS-205224	—	The **Upgrademgr** process got stuck and stopped responding after a reboot of the Mobility Master. The fix ensures that the Mobility Masters work as expected. This issue was observed in Mobility Masters running AOS-W 8.5.0.0 or later versions.	AOS-W 8.5.0.0
AOS-204364	—	High channel utilization was observed in some APs, and the issue was continuously displayed until the APs were rebooted. Enhancements to the wireless driver resolved this issue. This issue was observed in APs running AOS-W 8.5.0.1 or later versions.	AOS-W 8.5.0.11
AOS-204385	—	Incorrect position of access policies were observed in the **Configuration > Roles & Policies > Policies** page of the WebUI as well as from the CLI. The fix ensures that the access policies are positioned correctly. This issue was observed in stand-alone switches running AOS-W 8.4.0.0 or later versions.	AOS-W 8.5.0.7
AOS-204529 AOS-204861 AOS-206217 AOS-207968	—	The IP addresses of wired clients in **Dashboard > Overview > Clients** page were displayed as 0.0.0.0. The fix ensures that the correct IP address are displayed in the WebUI. This issue was observed in managed devices running AOS-W 8.5.0.0 or later versions.	AOS-W 8.6.0.4
AOS-204545 AOS-208184 AOS-208757 AOS-209190	—	A few OAW-4750XM switches running AOS-W 8.5.0.0 or later versions crashed and rebooted unexpectedly. The log file listed the reason for the event as **Kernel Panic (Intent:cause:register 12:86:f0:2).** The fix ensures that the switches work as expected.	AOS-W 8.5.0.8
AOS-204663	—	The **show running-config** command did not display a few user roles. The fix ensures that the command displays all user roles. 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 8.6.0.6*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-204691	—	Some VIA users were unable to download the connection profile. This issue occurred when the user role exceeded 32 characters. The fix ensures that VIA users are able to download the connection profile. This issue was observed in stand-alone switches running AOS-W 8.0.0.0 or later versions.	AOS-W 8.6.0.2
AOS-204697	—	The **Auth** field for 802.1X Per User Tunnel Node users was incorrectly updated as **tunneled-user-MAC** instead of **tunneled-user-Dot1x** when the **show user-table** command was executed. The fix ensures that the correct output values are displayed when the **show user-table** command is executed. This issue was observed in managed devices running AOS-W 8.5.0.0 or later versions.	AOS-W 8.6.0.4
AOS-204764	—	AP configurations were reset and APs moved to the default AP group after a reboot. The fix ensures that the APs work as expected. This issue was observed in APs running AOS-W 8.3.0.7 or later versions.	AOS-W 8.3.0.7
AOS-204780	—	Mobility Masters running AOS-W 8.3.0.0 or later versions displayed the **Valid Client Misassociation** log even when the valid clients connected to a valid SSID. The fix ensures that the Mobility Masters work as expected.	AOS-W 8.3.0.0
AOS-204797	—	A client was unable to connect to OAW-AP303H Series access points running AOS-W 8.6.0.0 or later versions in a Mobility Master-Managed Device topology. Enhancements to the wireless driver resolved this issue.	AOS-W 8.6.0.4
AOS-204917 AOS-205979 AOS-207203 AOS-207924 AOS-207992 AOS-208343 AOS-208920 AOS-209865	—	The **dpagent** process on managed devices running AOS-W 8.5.0.0 or later versions crashed unexpectedly. The log file listed the reason for this event as **Memory usage limit exceeded for process: dpagent current pages**. The fix ensures that the managed devices work as expected. This issue occurred due to high memory utilization.	AOS-W 8.5.0.1
AOS-204948	—	APs running AOS-W 8.5.0.0 or later versions crashed and rebooted unexpectedly. The log file listed the reason for this event as **kernel panic: Fatal exception with NIP: e445c71c LR: e4490ac0 CTR: c0567b30**. Enhancements to the wireless driver resolved this issue.	AOS-W 8.5.0.7
AOS-205010	—	The **OFA** process crashed in managed devices running AOS-W 8.5.0.8 or later versions, due to an increase in the number of IP user events. The fix ensures that the managed devices work as expected.	AOS-W 8.5.0.8

Table 6: *Resolved Issues in AOS-W 8.6.0.6*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-205013	—	Layer 2 VLANs configured with option 82 were missing when the managed devices were reloaded. The fix ensures that VLAN configurations are available after reload. This issue was observed in managed devices running AOS-W 8.6.0.2 or later versions.	AOS-W 8.6.0.2
AOS-205025 AOS-209326	—	The switch did not retrieve cluster inner-IP from the whitelist database as the request is initiated from an OAW-IAP. This issue occurred when the switch used external authentication for OAW-RAP whitelisting. This issue is resolved by provisioning the OAW-IAP as a OAW-RAP. This issue was observed in switches running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.4
AOS-205112	—	Some managed devices running AOS-W 8.3.0.7 or later versions rebooted unexpectedly. This issue occurred due to a memory leak in the **OFA** process. The fix ensures that the managed devices work as expected.	AOS-W 8.3.0.7
AOS-205171	—	Mobility Masters and managed devices running AOS-W 8.5.0.7 or later versions displayed a log message, **Received MAP_ADD from IKE for default-local-master-ipsecmap**. This issue occurred when tunnels were established. The fix ensures that the Mobility Masters and managed devices work as expected.	AOS-W 8.5.0.7
AOS-205190	—	The **authentication** process in a managed device running AOS-W 8.3.0.7 or later versions crashed unexpectedly. This issue occurred when openflow was used to add or delete ACLs. The fix ensures that the managed devices work as expected.	AOS-W 8.3.0.7
AOS-205253 AOS-205644	—	SSH public key authentication failed on OpenSSH version 7. The fix ensures that SSH public key authentication works as expected. This issue was observed in Mobility Masters running AOS-W 8.5.0.0 or later versions.	AOS-W 8.5.0.5
AOS-205326	—	An 802.11ax client failed to complete a download throughput test. Enhancements to the wireless driver resolved this issue. This issue was observed in OAW-AP535 access points running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.4
AOS-205634	—	The WebUI did not display the port channel membership. This issue occurred when port members were added to the PC-0 port channel. The fix ensures that the WebUI displays the port channel membership. This issue was observed in managed devices running AOS-W 8.6.0.0 or later versions in a Mobility Master-Managed Device topology.	AOS-W 8.6.0.4
AOS-205666	—	Performance degradation was observed in OAW-AP535 access points running AOS-W 8.7.0.0 when OFDMA was enabled in the **wlan he-ssid-profile** command.	AOS-W 8.7.0.0

Table 6: *Resolved Issues in AOS-W 8.6.0.6*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-205702	—	A few OAW-4850 switches running AOS-W 8.3.0.0 or later versions disconnected TCP session and hence, internal captive portal stopped working. The fix ensures that the switches work as expected. This issue occurred due to **nginx** process crash.	AOS-W 8.5.0.8
AOS-205996	—	A user experienced network latency. This issue occurred due to high CPU utilization in a managed device. The fix ensures that the managed device works 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-206047	—	AirGroup cache entries were deleted from the Mobility Master running AOS-W 8.6.0.4 or later versions. This issue occurred when the maximum threshold limit was reached. The fix ensures that the AirGroup cache entries are not deleted.	AOS-W 8.6.0.4
AOS-206057	—	Poor performance was observed in OAW-AP535 access points running AOS-W 8.7.0.0 when the MU-MIMO was enabled. Enhancements to the wireless driver resolved this issue.	AOS-W 8.7.0.0
AOS-206071	—	The **Dashboard > Security > Bandwidth** page did not display information about the HT-type of the APs. The fix ensures that the WebUI displays the HT-type of the APs. This issue was observed in APs running AOS-W 8.6.0.4 or later versions.	AOS-W 8.6.0.4
AOS-206115	—	High efficiency and very high throughput values disabled using **wlan ht-ssid profile** command were displayed in the output of **show ap bss-table** command. The fix ensures that the AP BSS table does not display the disabled values. This issue was observed in managed devices running AOS-W 8.3.0.0 or later versions.	AOS-W 8.5.0.9
AOS-206123	—	Packet loss was observed on APs running AOS-W 8.2.2.0 or later versions. The fix ensures that the APs work as expected. This issue occurred when APs were configured with the default MTU value of 1300.	AOS-W 8.5.0.5
AOS-206221	—	APs did not come up during a datacenter failover. The fix ensures that the APs work as expected. This issue was observed in APs running AOS-W 8.5.0.3 or later versions.	AOS-W 8.5.0.3
AOS-206433	—	A few APs failed to send a DNS query to the server to resolve the managed device. As a result, the APs did not come up on the managed device. The fix ensures that the APs send the DNS query to resolve the managed device. This issue was observed in OAW-AP100 Series and OAW-AP200 Series access points running AOS-W 8.5.0.0 or later versions.	AOS-W 8.5.0.5

Table 6: *Resolved Issues in AOS-W 8.6.0.6*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-206452	—	An unknown IP address was displayed for **Standby Controller** in the **Dashboard** > **Overview** > **Clients** > **Wireless Clients** page in the WebUI. The fix ensures that the unknown IP address is not displayed for the wireless clients. This issue occurred when no standby switch was available. This issue was observed in Mobility Masters running AOS-W 8.3.0.0 or later versions in a Mobility Master-Managed Device topology.	AOS-W 8.6.0.2
AOS-206517	—	A captive portal user name changed after 802.1x reauthentication. The fix ensures that the user name does not change after 802.1x reauthentication. This issue was observed in managed devices running AOS-W 8.6.0.3 or later versions.	AOS-W 8.6.0.3
AOS-206636 AOS-206629	—	L2TP VPN connection failed on Mac, IOS, and android clients connected to the managed device. The fix ensures that the managed device works as expected. This issue occurred when: ■ clients initiated L2TP connection on random src port instead of the standard src port, 1701. ■ clients connected behind a NAT device. This issue was observed in managed devices running AOS-W 8.4.0.6 or later versions.	AOS-W 8.4.0.6
AOS-206689	—	A few users were unable to add a user name with a period to local-userdb. The fix ensures that the users are able to add the user name. This issue was observed in stand-alone switches running AOS-W 8.3.0.0 or later versions.	AOS-W 8.6.0.4
AOS-206713 AOS-207273 AOS-207332	—	Users were unable to remove a managed device from the L2 connected cluster. The fix ensures that the users are able to remove the managed device. This issue was observed in Mobility Controller Virtual Appliance running AOS-W 8.5.0.0 or later versions.	AOS-W 8.5.0.8
AOS-206817	—	The **Dashboard > Overview > Wireless Clients** page displayed invalid values for **Standby Controller**. The fix ensures that the WebUI does not display invalid values for Standby Controller. This issue was observed in managed devices running AOS-W 8.7.0.0.	AOS-W 8.7.0.0
AOS-206852	—	A managed device running AOS-W 8.6.0.2 or later versions sent disconnect-ACK messages using VRRP IPv6 address instead of sending using physical IPv6 address. Hence, ClearPass Policy Manager continuously sent disconnect request messages to the same client. The fix ensures that the managed device works as expected.	AOS-W 8.6.0.2
AOS-206861	—	An SNMP trap was not generated for a bridge mode user. The fix ensures that the SNMP trap is generated. This issue was observed in managed devices running AOS-W 8.5.0.8 or later versions.	AOS-W 8.5.0.8
AOS-206891	—	A delay was observed in sending the RADIUS interim accounting messages. This issue occurred when the clients roamed between switches. The fix ensures that there is no delay in sending the RADIUS interim accounting messages. This issue was observed in Mobility Masters running AOS-W 8.3.0.0 or later versions.	AOS-W 8.3.0.0

Table 6: *Resolved Issues in AOS-W 8.6.0.6*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-206998 AOS-208353	—	A few APs running AOS-W 8.6.0.2 or later versions crashed and rebooted unexpectedly. The log files listed the reason for the event as **[Kilchoman] AP555 crash: NOC_error.c:473 NOCError: FATAL ERRORparam0 :zero, param1 :zero, param2 :zero**. Enhancements to the wireless driver resolved this issue.	AOS-W 8.6.0.2
AOS-207007	—	A few clients faced intermittent connectivity issues while connected to OAW-AP303H, OAW-AP303, and OAW-AP303P access points running AOS-W 8.3.0.0 or later versions. The fix ensures seamless connectivity.	AOS-W 8.3.0.0
AOS-207011	—	A few OAW-AP325 access points running AOS-W 8.5.0.5 or later versions crashed and rebooted unexpectedly. The log file listed the reason for the event as **kernel panic: TARGET ASSERT DUE TO MORE THAN 5 RECOVERY.** Enhancements to the wireless driver resolved this issue.	AOS-W 8.5.0.5
AOS-207053	—	A switch port was able to read a large number of MAC addresses in the same subnet from the mesh portal. This issue occurred due to wrong mesh link information in the mesh link table for the mesh portal. This issue was resolved by removing the wrong mesh link entry from the mesh link table. This issue was observed in APs running AOS-W 8.5.0.0 or later versions.	AOS-W 8.5.0.7
AOS-207056	—	The managed devices in Data MultiZone was unable to forward L2 GRE packets. The fix ensures that the managed devices work as expected. This issue was observed in managed devices running AOS-W 8.6.0.4 or later versions.	AOS-W 8.6.0.4
AOS-207073	—	A few OAW-AP305 access points running AOS-W 8.3.0.0 or later versions crashed and rebooted unexpectedly. The log files listed the reason for the event as **Fatal exception in interrupt**. The fix ensures that the APs work as expected.	AOS-W 8.3.0.0
AOS-207159	—	The **Diagnostics** > **Tools** > **AAA Server Test** page incorrectly displayed the **Authentication** value as **failed** instead of **timeout** in the WebUI. The fix ensures that the **timeout** value is displayed for the **Authentication** field in the WebUI. This issue occurred while connecting to a server that was down. This issue was observed in managed devices running AOS-W 8.2.2.0 or later versions in a Mobility Master-Managed Device topology.	AOS-W 8.6.0.4
AOS-207416	—	The whitelist entry displayed the status of the OAW-RAP as **Provisioned** instead of **Authenticated**. Also, the OAW-RAP had to be authorized using the Ethernet port every time after a reload. The fix ensures that the status of the OAW-RAPs authenticated using the authorization profile remain authenticated. This issue was observed in OAW-RAPs running AOS-W 8.5.0.8 or later versions.	AOS-W 8.5.0.8

Table 6: *Resolved Issues in AOS-W 8.6.0.6*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-207439	—	Negative numbers were displayed in the output of the **show firewall-cp** command. The fix ensures that the command does not display negative numbers. This issue was observed in Mobility Masters running AOS-W 8.6.0.2 or later versions.	AOS-W 8.6.0.2
AOS-207552	—	A mismatch of MTU values was observed between the AP and the switch. The fix ensures that the MTU value is consistent across the AP and the switch. This issue occurred when the AP was rebooted after setting the default value of the **rap-gre-mtu** parameter. This issue was observed in APs connected to stand-alone switches running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.0
AOS-207565	—	A managed device failed to send user ID information to connect to Palo Alto Networks (PAN) firewall server. The fix ensures that the managed device sends user ID information to PAN firewall server when VIA VPN client is connected to the managed device. This issue was observed in managed devices running AOS-W 8.2.0.0 or later versions.	AOS-W 8.6.0.6
AOS-207619	—	Clients were not redirected to the captive portal page. The fix ensures that captive portal is working as expected. This issue was observed in managed devices running AOS-W 8.3.0.13 or later versions.	AOS-W 8.3.0.13
AOS-207659	—	The **profmgr** process crashed on managed devices running AOS-W 8.6.0.4 or later versions. The fix ensures that the managed devices work as expected.	AOS-W 8.6.0.4
AOS-207791	—	The **udbserver** process crashed multiple times on a managed device running AOS-W 8.5.0.8 or later versions. The fix ensures that the managed device works as expected.	AOS-W 8.5.0.8
AOS-207893	—	Clients were unable to receive IP addresses. This issue occurred due to high memory utilization in APs caused by the BLE daemon process. The fix ensures that memory utilization in APs is regulated by the creation of a new boot log file at every restart instance of the BLE daemon process. This issue was observed in APs running AOS-W 8.5.0.3 or later versions.	AOS-W 8.5.0.3
AOS-208017	—	Users were unable to remove an invalid virtual AP profile from the default AP group profile. The fix ensures that users are able to remove the virtual AP profile. This issue was observed in managed devices running AOS-W 8.6.0.5.	AOS-W 8.6.0.5
AOS-208193	—	User-based tunneled node and the users were not removed even after a heartbeat failure. The fix ensures that the tunneled node is removed after a heartbeat failure. This issue was observed in standby switches running AOS-W 8.6.0.1 or later versions.	AOS-W 8.6.0.1

Table 6: *Resolved Issues in AOS-W 8.6.0.6*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-208553	—	The **Test** button in **Diagnostics > Tools > AAA Server Test** was grayed out for read-only users. The fix ensures that the test button is not grayed out for read-only users. This issue was observed in managed devices running AOS-W 8.5.0.9 or later versions.	AOS-W 8.5.0.9
AOS-208557	—	OAW-AP534, OAW-AP535, and OAW-AP555 access points running AOS-W 8.6.0.4 or later versions crashed and rebooted unexpectedly. The log files listed the reason for the event as **reboot reason: due to Assertion failed! ic->ic_curchan->ic_ieee == dfs->dfs_curchan->dfs_ch_ieee:dfs_process_radar_found_ind.c:961**. Enhancements to the wireless driver resolved this issue.	AOS-W 8.6.0.4
AOS-210055	—	Clients were unable to connect to OAW-AP515 access points running AOS-W 8.6.0.5 in 5 Ghz mode. The fix ensures seamless connectivity.	AOS-W 8.6.0.5

Known Issues and Limitations in AOS-W 8.6.0.6

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

Limitation

No Support for Unique Local Address over IPv6 Network

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

Known Issues

Following are the known issues observed in this release.

Table 7: *Known Issues in AOS-W 8.6.0.6*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-151022 AOS-188417	185176	The output of the **show datapath uplink** command displays incorrect session count. This issue is observed in managed devices running AOS-W 8.1.0.0 or later versions.	AOS-W 8.1.0.0
AOS-151355	185602	A few managed devices are unable to pass traffic to the nexthop VPN concentrator (VPNC) using policy-based routing. This issue is observed in managed devices running AOS-W 8.0.1.0 or later versions.	AOS-W 8.0.1.0
AOS-153742 AOS-194948	188871	A stand-alone switch crashes and reboots unexpectedly. The log files list the reason for the event as **Hardware Watchdog Reset (Intent:cause:register 51:86:0:8)**. This issue is observed in OAW-4010 switches running AOS-W 8.5.0.1 or later versions in a Mobility Master-Managed Device topology.	AOS-W 8.5.0.1
AOS-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 crashes unexpectedly. This issue is observed in managed devices running AOS-W 8.2.1.1 or later versions.	AOS-W 8.2.1.1

Table 7: *Known Issues in AOS-W 8.6.0.6*

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 the WebUI. This issue is observed in managed devices running AOS-W 8.4.0.0 in a Mobility Master-Managed Device topology.	AOS-W 8.4.0.0
AOS-183706	—	The tx radio power of a few APs are lesser than the tx radio power of other APs in the same network. This issue is observed in APs running AOS-W 8.3.0.6 or later versions.	AOS-W 8.3.0.6
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 Master running AOS-W 8.4.0.4 or later versions.	AOS-W 8.4.0.4
AOS-185538	—	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	—	Memory leak is observed in **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-188090 AOS-196004 AOS-199152	—	The **Dashboard > Overview > Clients** page of the WebUI displays incorrect usage values intermittently. This issue is observed in Mobility Master Virtual Appliances running AOS-W 8.4.0.0 or later versions.	AOS-W 8.4.0.0
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-4005switches running AOS-W 8.4.0.0. **Workaround:** Perform the following steps to resolve the issue: ■ Remove web category from the ACL rules and apply **any any any permit** policy. ■ Disable WebCC on the user role. ■ Change the VLAN of user role from trunk mode to access mode.	AOS-W 8.4.0.0
AOS-192568 AOS-192736	—	A few clients are unable to connect to APs even though High-Efficiency was disabled on all the SSID profiles of the APs. This issue is observed in OAW-AP515 access points running AOS-W 8.5.0.0 or later versions.	AOS-W 8.5.0.1
AOS-192725 AOS-190476 AOS-196004	—	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.	AOS-W 8.3.0.8

Table 7: *Known Issues in AOS-W 8.6.0.6*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-193184	—	All L2 connected managed devices move to L3 connected state after 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-193560 AOS-198565 AOS-200262 AOS-204794	—	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.	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-193840	—	The managed device loses connectivity to IPv6 gateway intermittently. This issue is observed in managed devices running AOS-W 8.3.0.6 or later versions.	AOS-W 8.3.0.6
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 do 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 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-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
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-194919 AOS-195565 AOS-205648 AOS-206010	—	The **HTTPD** process in a Mobility Controller Virtual Appliance crashes unexpectedly. The log files list the reason for the event as **Reboot Cause: User reboot (Intent:cause: 86:50)**. This issue occurs when the Mobility Controller Virtual Appliance is scanned for security vulnerabilities. This issue is observed in Mobility Controller Virtual Appliances and stand-alone switches running AOS-W 8.2.0.0 or later versions.	AOS-W 8.6.0.0
AOS-194964	—	A few users are unable to clone configuration 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

Table 7: *Known Issues in AOS-W 8.6.0.6*

New Bug ID	Old Bug ID	Description	Reported Version
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	—	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-195526	—	Some clients are unable to get the DHCP addresses. This issue occurs when the ACE entries of the logon role ACL changes to **Deny all** when the PEFNG feature is disabled. This issue is observed in managed devices running AOS-W 8.3.0.8 or later versions.	AOS-W 8.3.0.8
AOS-196457	—	High radio noise floor is observed on APs. This issue is observed on OAW-AP515 access points running AOS-W 8.5.0.2 or later versions.	AOS-W 8.5.0.2
AOS-196864	—	Adding a new VLAN ID connects L3 but displays that the connected 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
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:** The following are recommended: In the CLI, execute the **ap regulatory-domain-profile** command to create an AP regulatory-domain- profile without any channel configuration, save the changes, and later add or delete channels as desired. In the WebUI, create an AP regulatory-domain-profile with default channel selected, save the changes, and later add or delete channels as desired in the **Configuration > AP Groups** page.	AOS-W 8.5.0.4

Table 7: *Known Issues in AOS-W 8.6.0.6*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-197127	—	A managed device crashes and reboots unexpectedly. The log file lists the reason for this event as **Datapath timeout (Fpapps Initiated) (Intent:cause:register 51:86:50:2).** This issue is observed in OAW-4x50 Series switches running AOS-W 8.3.0.7 or later versions in a cluster setup. **Duplicates:** AOS-197060, AOS-197130, AOS-197137, AOS-197161, AOS-197163, AOS-198720, and AOS-201821	AOS-W 8.3.0.7
AOS-197497	—	AirMatch selects the same channel for two neighboring APs even after radar detection. This issue is observed in managed devices running AOS-W 8.5.0.3 or later versions.	AOS-W 8.5.0.3
AOS-197812	—	A mismatch of user roles is observed in the WebUI and CLI of the Mobility Master and managed device. This issue occurs when UDR is configured to assign user role to clients. This issue is observed in both Mobility Masters and managed devices running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.0
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-198475	—	Users are unable to upgrade the Mobility Master Virtual Appliance to AOS-W 8.5.0.0 or later versions. This issue is observed in Mobility Master Virtual Appliance running AOS-W 8.5.0.5 or later versions.	AOS-W 8.5.0.5
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 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	—	A few APs do not get displayed in the **show airgroup aps** command output and the **auto-associate policy** stops working 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-200733	—	APs running AOS-W 8.5.0.3 or later versions crash and reboot unexpectedly. The log file list the reason for the event as **kernel page fault at virtual address 00005654, epc == c0bd7dd4, ra == c0bf95f8.**	AOS-W 8.5.0.3

Table 7: *Known Issues in AOS-W 8.6.0.6*

New Bug ID	Old Bug ID	Description	Reported Version
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-201150 AOS-201997 AOS-204328	—	510 Series access points running AOS-W 8.6.0.2 or later versions crash and reboot unexpectedly. The log file lists the reason for the event as **AP Reboot reason: External-WDT-reset.**	AOS-W 8.6.0.2
AOS-201439 AOS-201448	—	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 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 APs running AOS-W 8.6.0.4 crash and reboot unexpectedly. The log files lists 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-202803	—	The error message, **cluster was fractured during the upgrade** is displayed during the cluster live upgrade process and therefore, cluster live upgrade cannot be performed. This issue is observed in Mobility Masters running AOS-W 8.5.07 or later versions.	AOS-W 8.5.07
AOS-203077 AOS-203232	—	Configurations committed using the **firewall cp** command are not synchronized on the standby Mobility Master. This issue occurs when static firewall entries are deleted. This issue is observed in Mobility Masters running AOS-W 8.6.0.3 or later versions.	AOS-W 8.6.0.3
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
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 through the WebUI is not visible in the stand-alone switches running AOS-W 8.6.0.3 or later versions.	AOS-W 8.6.0.3

Table 7: *Known Issues in AOS-W 8.6.0.6*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-203459	—	It takes a long time to import a guest provisioning file with a very few users to the Mobility Master's local database. This issue is observed in Mobility Masters running AOS-W 8.5.0.0 or later versions.	AOS-W 8.6.0.3
AOS-203517 AOS-204709	—	The Datapath module crashes on managed devices unexpectedly. The log file lists the reason for the event as **Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2).** This issue occurs when data packets undergo multiple GRE encapsulation. This issue is observed in managed devices running AOS-W 8.3.0.7 or later versions.	AOS-W 8.3.0.7
AOS-204187	—	The command **vpn-peer peer-mac** does not support Suite-B cryptography for custom certificates. This issue is observed in Mobility Masters running AOS-W 8.2.2.8 or later versions.	AOS-W 8.2.2.8
AOS-204241	—	Managed devices log spurious DHCP DBUG messages. This issue is observed in managed devices running AOS-W 8.5.0.8 or later versions.	AOS-W 8.5.0.8
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-standlaone vlan-range.**	AOS-W 8.3.0.8
AOS-205176 AOS-205325 AOS-206533	—	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 **Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2).**	AOS-W 8.5.0.8
AOS-205935	—	Management users created on Mobility Master are not synchronized on standby Mobility Master. This issue is observed in Mobility Masters running AOS-W 8.4.0.0 or later versions.	AOS-W 8.5.0.8
AOS-206541	—	The **Maintenance > Software Management** page does not display the list of all managed devices that are a 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-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

Table 7: *Known Issues in AOS-W 8.6.0.6*

New Bug ID	Old Bug ID	Description	Reported Version
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-206907	—	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 **Kernel panic - not syncing: assert**.	AOS-W 8.5.0.5
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-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 are stuck in the **LAST SNAPSHOT** state.	AOS-W 8.5.0.9
AOS-207458 AOS-205925	—	When the **show ucc client-info** command is issued, the stand-alone switch running AOS-W 8.3.0.8 or later versions does not display the UCC client data.	AOS-W 8.3.0.8
AOS-207664	—	The login banner text is not displayed after upgrading the managed device to AOS-W 8.5.0.0 or later versions.	AOS-W 8.5.0.10
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

Chapter 7
Upgrade Procedure

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

CAUTION

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

Topics in this chapter include:

Important Points to Remember

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 150 MB of flash space is available. Execute the **show storage** command to identify the available flash space. If the output of the **show storage** command indicates that there is insufficient flash memory, free some used memory. Copy any log files, crash data, or flash backups from your 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 39 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 39 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 39 to copy the **logs.tar** file to an external server. Execute the **tar clean logs** command to delete the file from the managed device.

CAUTION

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

Deleting a File

You can delete a file using the WebUI or 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 38.

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 39 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 39 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 39.
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:

CAUTION

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

   a. Enter the FTP or TFTP server address and image file name.
   b. Select the backup system partition.
   c. Enable **Reboot Controller after upgrade**.
   d. Click **Upgrade**.
3. Navigate to the **Maintenance > Software Management > Reboot** page, select **Save configuration before reboot**, 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
```

CAUTION

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.