AOS-W 8.7.1.1

Release Notes

Contents

Revision History

The following table lists the revision numbers and the corresponding changes that were made in this release:

Table 1: *Revision History*

Revision	Change Description
Revision 04	OAW-AP303P has been added to the list of **Supported Platforms.**
Revision 03	The bug, **AOS-192568** has been removed from the **Known Issues and Limitations** section.
Revision 02	The bugs, **AOS-195434, AOS-196188,** and **AOS-196457** have been removed from the **Known Issues and Limitations** section.
Revision 01	Initial release.

This AOS-W release notes includes the following topics:

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

For a list of terms, refer to the 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

Contacting Support

Table 2: *Contact Information*

Contact Center Online	
Main Site	https://www.al-enterprise.com
Support Site	https://businessportal.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 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.

no ap ap-blacklist-time command

The **ap ap-blacklist-time** command determines the time, in seconds, for which a client is manually blacklisted. Starting from AOS-W 8.7.1.1, the **no ap ap-blacklist-time** command removes the blacklist time configured using the **ap-blacklist-time** command and restores the default value of 3600 seconds.

rf dot11a-radio-profile command

The range of the **energy-detect-threshold** parameter of the **rf dot11a-radio-profile** command has been modified from 0-12 to 12 to -29 dB.

disable-crc-workaround

Starting from AOS-W 8.6.0.7, users can issue the **disable-crc-workaround** command when port flaps of the uplink switch are not detected by the Mobility Master. This command dumps all the PHY register data like alarms, warnings, signal strength and hence, will be helpful for debugging.

It is to be noted that when this configuration is enabled, the CRC workaround will be initiated only when the uplink switch shuts down and come up and not when the the device is stable.

```
(host) [mynode] (config) #disable-crc-workaround
(host) [mynode] (config) #write memory
```

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 8.7.1.1*

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 8.7.1.1*

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, OAW-4112
MC-VA-xxx Virtual OmniAccess Mobility Controllers	MC-VA-10, 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 8.7.1.1*

AP Family	AP Model
OAW-AP200 Series	OAW-AP204, OAW-AP205
OAW-AP203H Series	OAW-AP203H
OAW-AP203R Series	OAW-AP203R, OAW-AP203RP
OAW-AP205H Series	OAW-AP205H
OAW-AP207 Series	OAW-AP207
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-AP303HR
OAW-AP310 Series	OAW-AP314, OAW-AP315
OAW-AP318 Series	OAW-AP318
OAW-AP320 Series	OAW-AP324, OAW-AP325
OAW-AP330 Series	OAW-AP334, OAW-AP335
OAW-AP340 Series	OAW-AP344, OAW-AP345

Table 5: *Supported AP Platforms in AOS-W 8.7.1.1*

AP Family	AP Model
OAW-AP360 Series	OAW-AP365, OAW-AP367
OAW-AP370 Series	OAW-AP374, OAW-AP375, OAW-AP377
OAW-AP370EX Series	OAW-AP375EX, OAW-AP377EX
OAW-AP387	OAW-AP387
OAW-AP500 Series	OAW-AP504, OAW-AP505
OAW-AP500H Series	OAW-AP503H, OAW-AP505H
510 Series	OAW-AP514, OAW-AP515, OAW-AP518
OAW-AP530 Series	OAW-AP534, OAW-AP535
OAW-AP550 Series	OAW-AP555
OAW-AP560 Series	OAW-AP565, OAW-AP567
OAW-AP570 Series	OAW-AP574, OAW-AP575, OAW-AP577

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.

The following DRT file version is part of this release:

- DRT-1.0_78105

The following issues are resolved in this release.

Table 6: *Resolved Issues in AOS-W 8.7.1.1*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-149413 AOS-196453	—	The **Dashboard > Overview > Remote Clients** page of the WebUI did not display any value for **OS** and **Connected to** fields. The fix ensures that the WebUI displays the **OS** and **Connected to** data. This issue was observed in Mobility Masters running AOS-W 8.4.0.0 or later versions.	AOS-W 8.4.0.0
AOS-187672	—	Memory leak was observed in the **arci-cli-helper** process. The fix ensures that the Mobility Masters and managed devices work as expected. This issue was observed in Mobility Masters and managed devices running AOS-W 8.3.0.6 or later versions.	AOS-W 8.3.0.6
AOS-194520	—	The VRRP preempt delay timer did not reset even after receiving heartbeats from the VRRP-master although VRRP preempt was enabled with preemption delay. The fix ensures that the VRRP preempt delay timer gets reset upon receiving the heartbeat from the VRRP-master before the preempt delay timer expires. This issue was observed in managed devices running AOS-W 8.3.0.0 or later versions.	AOS-W 8.3.0.0
AOS-194774	—	Some clients were unable to program the VLAN IP address in the control plane when the VRRP peers were reloaded together. This issue occurred when the VRRP VLANs did not have a single physical port associated and were L2 connected through L2 GRE tunnels. The fix ensures that clients are able to program the VLAN IP address. This issue was observed in managed devices running AOS-W 8.3.0.0 or later versions.	AOS-W 8.3.0.0
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-197134	—	User roles were incorrectly listed as downloaded user roles and the error message, **user role already exists** was displayed. The fix ensures that the correct user roles are listed and the error message is not displayed. 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 8.7.1.1*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-197552 AOS-206767	—	Some OAW-AP305 access points running AOS-W 8.3.0.0 or later versions crashed and rebooted unexpectedly. The log file listed the reason for the event as **kernel panic: Fatal exception in interrupt**. The fix ensures that the APs work as expected.	AOS-W 8.3.0.0
AOS-199423 AOS-205532	—	Some L3 redundant Mobility Masters running AOS-W 8.5.0.5-FIPS generated **profmgr** error logs. The fix ensures that the Mobility Masters work as expected.	AOS-W 8.5.0.5
AOS-199744 AOS-209046	—	The **show iap table long** command did not display the **Bid(Subnet Name)**. The fix ensures that the command displays the **Bid(Subnet Name)**. This issue occurred on backup switches when an IAP branch fails over from a primary switch. This issue was observed in switches running AOS-W 8.0.0.0 or later versions in an IAP-VPN deployment.	AOS-W 8.5.0.7
AOS-200962 AOS-202568 AOS-210225	—	A few APs running AOS-W 8.5.0.2 or later versions crashed and rebooted unexpectedly. The log file listed the reason for the event as **BadAddr:300000004 PC:put_page+0x8/0x50 Warm-reset**. The fix ensures that the APs work as expected.	AOS-W 8.5.0.2
AOS-201149 AOS-208332 AOS-211746	—	Some OAW-AP515 access points running AOS-W 8.6.0.2 or later versions crashed and rebooted unexpectedly. The log file listed the reason for the event as **Reboot reason: BadPtr:00000000 PC:ppr_ create_prealloc+0x3c/0x90 [wl_v6] Warm-reset**. The fix ensures that the APs work as expected.	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-201763	—	Some users were unable to access CLI using SSH. The fix ensures that the users can access CLI using SSH. This issue was observed in managed devices running AOS-W 8.4.0.4 or later versions.	AOS-W 8.4.0.4
AOS-201812 AOS-201813	—	Disabled VLANs generated the **wlsxVlanLinkDown** and **wlsxVlanInterfaceEntryChanged** traps. The fix ensures that the traps are not generated. This issue was observed in Mobility Masters running AOS-W 8.3.0.7 or later versions.	AOS-W 8.3.0.7

Table 6: *Resolved Issues in AOS-W 8.7.1.1*

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 WebUI does not display the error message. This issue was observed in Mobility Masters running AOS-W 8.3.0.0 or later versions.	AOS-W 8.3.0.0
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-203536	—	A few clients took a long time to roam between APs. The fix ensures that clients do not take a long time to roam between APs. This issue was observed in stand-alone switches running AOS-W 8.3.0.0 or later versions.	AOS-W 8.3.0.0
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 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-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 8.5.0.1
AOS-204520	—	Some 510 Series access points running AOS-W 8.7.0.0 or later versions crashed and rebooted unexpectedly. The log file listed the reason for the event as **AP Reboot reason: External-WDT-reset.** Enhancements to the driver resolved the issue.	AOS-W 8.7.0.0
AOS-204760	—	Some stand-alone switches running AOS-W 8.6.0.3 or later versions failed to set deny-all as initial role when PEF license was disabled. The fix ensures that the stand-alone switches work as expected.	AOS-W 8.6.0.3
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-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

Table 6: *Resolved Issues in AOS-W 8.7.1.1*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-205176 AOS-205325 AOS-206533	—	Some managed devices running AOS-W 8.5.0.8 or later versions crashed and rebooted unexpectedly. The log file listed the reason for the event as **Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2)**. The fix ensures that the managed devices work as expected.	AOS-W 8.5.0.8
AOS-205344	—	A few clients experienced slow connection speed when they connected to APs using mobile devices. This issue was observed in regions that operate under legacy regulatory rules. Enhancements to the wireless driver resolved this issue. This issue was observed in APs running AOS-W 8.6.0.4 or later versions.	AOS-W 8.6.0.4
AOS-205636	—	A few 802.1X clients experienced random timeouts. This issue was observed in OAW-AP203RP access points running AOS-W 8.0.0.0 or later versions. The fix ensures that the APs work as expected.	AOS-W 8.3.0.0
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-205728 AOS-210336	—	The **show license-usage client** command did not display the entire list of managed devices. The fix ensures that the command displays the entire list of managed devices. This issue was observed in Mobility Masters running AOS-W 8.5.0.8 or later versions.	AOS-W 8.5.0.8
AOS-205869	—	Users were unable to delete ACLs and the error message, **Invalid data: FW CP ACL not found** was displayed. The fix ensures that users are able to delete ACLs. This issue was observed in managed devices running AOS-W 8.3.0.12 or later versions.	AOS-W 8.3.0.12
AOS-205935 AOS-211851	—	Management users created on Mobility Master were not synchronized on standby Mobility Master. The fix ensures that the entries are synchronized between Mobility Master and the standby Mobility Master. This issue was observed in Mobility Masters running AOS-W 8.4.0.0 or later versions.	AOS-W 8.5.0.8
AOS-206045	—	A managed device running AOS-W 8.5.0.4 or later versions did not send the accounting request packets. The fix ensures that the managed device works as expected.	AOS-W 8.5.0.4
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 in APs running AOS-W 8.2.2.0 or later versions. This issue occurred when APs were configured with the default MTU value of 1300. The fix ensures that the APs work as expected.	AOS-W 8.5.0.5

Table 6: *Resolved Issues in AOS-W 8.7.1.1*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-206221	—	Some 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
AOS-206498 AOS-212922	—	APs running AOS-W 8.5.0.0 or later versions were unable to ping the managed devices. This issue occurred when APs were configured as OAW-RAPs and were present behind the NAT device. The fix ensures that APs work as expected.	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 displays the correct 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 the message 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
AOS-206896	—	Some OAW-RAPs running AOS-W 8.6.0.4 or later versions took a log time to failover. The fix ensures that OAW-RAPs work as expected.	AOS-W 8.6.0.4
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

Table 6: *Resolved Issues in AOS-W 8.7.1.1*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-207056	—	The managed devices in datazone e 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-207157 AOS-208746	—	Mobility Master lost the server certificate and hence, the newly added managed devices were unable to download server certificate from the Mobility Master. The fix ensures that the server certificate is always available on the Mobility Master. This issue was observed in Mobility Masters running AOS-W 8.5.0.9 or later versions.	AOS-W 8.5.0.9
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-207175 AOS-208334 AOS-211183	—	A few APs running AOS-W 8.6.0.4 or later versions crashed and rebooted unexpectedly. The log file listed the reason for the event as **AP Reboot reason: External-WDT-reset**. The fix ensures that the APs work as expected.	AOS-W 8.6.0.4
AOS-207318 AOS-207996	—	Clients experienced poor performance with OAW-AP505 access points running AOS-W 8.7.0.0 or later versions. Enhancements to the wireless driver resolved this issue.	AOS-W 8.7.0.0
AOS-207358	—	Some APs running AOS-W 8.7.0.0 or later versions logged the error message, **ctrlr not found, ip 0.0.0.0 id (3.57.164.244,5ef0f615,18)**. The fix ensures that the APs work as expected.	AOS-W 8.7.0.0
AOS-207458 AOS-205925	—	When the **show ucc client-info** command was issued, the stand-alone switch running AOS-W 8.3.0.8 or later versions did not display the UCC client data. The fix ensures that the command displays the UCC client data.	AOS-W 8.3.0.8
AOS-207492 AOS-210872	—	Clients were not redirected to the captive portal page. The fix ensures that captive portal works as expected. This issue was observed in managed devices running AOS-W 8.6.0.3 or later versions.	AOS-W 8.6.0.3
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 8.2.0.0

Table 6: *Resolved Issues in AOS-W 8.7.1.1*

New Bug ID	Old Bug ID	Description	Reported Version
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-207629	—	A Mobility Master running AOS-W 8.3.0.0-FIPS displayed the PPTP port status as open although FIPS mode disable both the PPTP configuration and PPTP port. The fix ensures that the PPTP port is not open in FIPS mode.	AOS-W 8.3.0.0-FIPS
AOS-207970	—	A few APs running AOS-W 8.7.0.0 or later versions stopped sending unicast packets after a few configuration changes. The fix ensures that APs continue to send unicast packets.	AOS-W 8.7.0.0
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-208030 AOS-208287 AOS-209499	—	A few clients were unable to connect to APs. This issue occurred when EAPOL frames were not sent from the AP. The fix ensures that APs work as expected. This issue was observed in APs running AOS-W 8.6.0.4 or later versions.	AOS-W 8.6.0.4
AOS-208044 AOS-211207	—	The **stm** process crashed on Mobility Masters running AOS-W 8.7.0.0 or later versions. This issue occurred when AP regulatory configuration was reset. The fix ensures that the Mobility Masters work as expected.	AOS-W 8.7.0.0
AOS-208113	—	Intermittent data loss was observed for a few clients connected to APs. The fix ensures that APs work as expected. This issue was observed in APs running AOS-W 8.5.0.8 or later versions.	AOS-W 8.5.0.8
AOS-208160	—	The status of OpenFlow for a few managed devices was displayed as disabled, whereas the status was enabled for the other managed devices in a network. This issue occurred when the **OFA** process pushed the **no OpenFlow-enable** command to the managed devices during ZTP. The fix ensures that the managed devices work as expected. This issue was observed in managed devices running AOS-W 8.5.0.8 or later versions.	AOS-W 8.5.0.8
AOS-208269	—	Clients experienced poor performance with APs. Also, APs did not prioritize traffic from active stations and hence, stations went to sleep mode. The fix ensures that APs work as expected. This issue was observed in APs running AOS-W 8.6.0.4 or later versions.	AOS-W 8.6.0.4
AOS-208433 AOS-208728	—	Users were unable to change the port configuration status to untrusted. The fix ensures that users are able to change the port configuration status. This issue was observed in Mobility Masters running AOS-W 8.6.0.4 or later versions.	AOS-W 8.6.0.4

Table 6: *Resolved Issues in AOS-W 8.7.1.1*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-208492 AOS-208806	—	A few APs logged the **Phony BSSID Detection** error message and detected its own BSSIDs as phony BSSIDs. The fix ensures that the APs work as expected. This issue was observed in Air Monitor APs running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.4
AOS-208568	—	The **show ap essid** command displayed incorrect **VLAN(s)** values. The fix ensures that the correct VLAN values are displayed. This issue was observed in managed devices running AOS-W 8.3.0.13.	AOS-W 8.3.0.13
AOS-208625	—	RADIUS accounting packets did not have location and AP group related details. The fix ensures that location and AP group related details are available in RADIUS accounting packets. This issue was observed in managed devices running AOS-W 8.5.0.7 or later versions.	AOS-W 8.5.0.7
AOS-208756	—	The authentication request is discarded in a managed device because some of the attributes needed for authentication were not sent from Auth to dot1X process. This issue occurred because the Hotspot 2.0 operator name was not added to the access-request packets. The fix ensures that the attributes are included in the message sent to dot1X process. This issue was observed in managed devices running AOS-W 8.6.0.4 or later versions.	AOS-W 8.6.0.4
AOS-208790	—	A few APs running AOS-W 8.5.0.9 or later versions logged the error message**, Unexpected stm (Station management) runtime error at wifi_mgmt_recv_frame, 10284, wifi_mgmt_recv_frame:10284: NULL src-mac, frame type=0, subtype=15**. The fix ensures that the APs work as expected.	AOS-W 8.5.0.9
AOS-208807	—	The CLI displayed the list of expired certificates which were deleted using the WebUI and hence, resulted in configuration failure when new certificates were added. The fix ensures that the Mobility Master works as expected. This issue was observed in Mobility Masters running AOS-W 8.6.0.4 or later versions.	AOS-W 8.6.0.4
AOS-209243 AOS-210135	—	Some OAW-AP535 access points running AOS-W 8.5.0.10 or later versions crashed and rebooted unexpectedly. The log file 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 8.5.0.10
AOS-209256	—	Some OAW-AP515 access points running AOS-W 8.6.0.5 or later versions crashed and rebooted unexpectedly. The log file listed the reason for the event as **Kernel panic - not syncing: Out of memory**. The fix ensures that APs work as expected.	AOS-W 8.6.0.5
AOS-209324	—	The **lagm** process crashed while configuring port channels. The fix ensures that the managed device works as expected. This issue was observed in managed devices running AOS-W 8.2.0.0 or later versions.	AOS-W 8.5.0.6
AOS-209406 AOS-211798	—	The **ISAKMPD** process crashed on managed devices running AOS-W 8.5.0.10 or later versions. The fix ensures that the managed device works as expected.	AOS-W 8.5.0.10

Table 6: *Resolved Issues in AOS-W 8.7.1.1*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-209533	—	While importing guest entries from CSV file, users were unable to download the summary text file. The fix ensures that users are able to download the summary text file. This issue was observed in stand-alone switches running AOS-W 8.7.0.0 or later versions.	AOS-W 8.7.0.0
AOS-209551	—	Some OAW-RAPs running AOS-W 8.5.0.10 or later versions rebooted unexpectedly. This issue occurred when the **activate whitelist download** command was executed. The fix ensures that the OAW-RAPs work as expected.	AOS-W 8.5.0.10
AOS-209553	—	Mobility Controller Virtual Appliances allowed users to log in to the Debug CLI during boot up without requesting for the AOS-W decryption key. The fix ensures that users log in to Debug CLI only after entering the AOS-W decryption key. This issue was observed in Mobility Controller Virtual Appliances running AOS-W 8.3.0.0 or later versions.	AOS-W 8.3.0.0
AOS-209599	—	The **OFA** process crashed on managed devices running AOS-W 8.6.0.5 or later versions. The fix ensures that managed devices work as expected.	AOS-W 8.6.0.5
AOS-209612	—	The value of Tx data bytes transmitted for 5 GHz radio was lower than the actual transmitted value. The fix ensures that the actual values are transmitted for 5 GHz radio. This issue was observed in OAW-AP205 access points running AOS-W 8.6.0.5 or later versions.	AOS-W 8.6.0.5
AOS-209679 AOS-210115	—	The **SAPD** process crashed on APs running AOS-W 8.5.0.10 or later versions. The fix ensures that the APs work as expected.	AOS-W 8.5.0.10
AOS-209691	—	Clients were unable to pass traffic with packet size more than 1470. This issue occurred when connected to mesh point APs. The fix ensures that clients are able to pass traffic. This issue was observed in stand-alone switches running AOS-W 8.6.0.4 or later versions.	AOS-W 8.6.0.4
AOS-209701	—	Users were unable to connect to OAW-AP303 access points running AOS-W 8.5.0.10 or later versions. The fix ensures seamless connectivity.	AOS-W 8.5.0.10
AOS-209774 AOS-209778	—	The old outer IP address of an AP was displayed in the user table. The fix ensures that the stale entries are remove from the user table. This issue was observed in APs running AOS-W 8.6.0.5 or later versions.	AOS-W 8.6.0.5
AOS-209805	—	Users were not assigned VLANs and hence, they did not receive IP addresses. As a result, clients experienced connectivity issues. This issue occurred when users were connected to MPSK BSSIDs. The fix ensures that the managed device 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

Table 6: *Resolved Issues in AOS-W 8.7.1.1*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-209855		Some APs running AOS-W 8.7.0.0 or later versions crashed and rebooted unexpectedly. The log file listed the reason for the event as **Kernel panic - not syncing: Fatal exception in interrupt.** The fix ensures that the APs work as expected. **Duplicates:** AOS-210214, AOS-211809, AOS-212590, AOS-214704, and AOS-212823	
AOS-209887	—	Some OAW-AP515 access points running AOS-W 8.6.0.5 or later versions crashed and rebooted unexpectedly. The log file listed the reason for the event as **rebooted by Panic:Ktrace core monitor: cpu1 hung for 45 seconds, hung cpu count: 3 Warm-reset.** The fix ensures that APs work as expected.	AOS-W 8.6.0.5
AOS-209916	—	A managed device running AOS-W 8.6.0.0 or later versions displayed the error message, **Sos packet processing: bad opcode 0x3a, expects VRRP (hapiSosReceive)**. The fix ensures that the managed device works as expected.	AOS-W 8.6.0.0
AOS-209998	—	Users were unable to configure a password for VPN dialer in the **Configuration > Roles > VPN** page of the WebUI. The fix ensures that users are able to configure a password for VPN dialer configuration. This issue was observed in managed devices running AOS-W 8.6.0.5 or later versions.	AOS-W 8.6.0.5
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
AOS-210126	—	A few 802.1X clients were unable to connect to an SSID. The fix ensures seamless connectivity. This issue was observed in APs running AOS-W 8.6.0.5 or later versions.	AOS-W 8.6.0.5
AOS-210448	—	Some OAW-AP200 Series access points running AOS-W 8.6.0.4 or later versions crashed and rebooted unexpectedly. This issue occurred when wireless containment was enabled. Enhancements to the driver resolved the issue.	AOS-W 8.6.0.4
AOS-210506	—	Clients were disconnected from the network because some APs changed channels. This issue occurred when AirMatch was configured after 48 hours of a failover. The fix ensures seamless connectivity. This issue was observed in APs running AOS-W 8.5.0.8 or later versions.	AOS-W 8.5.0.8
AOS-210529	—	Some users were unable to upgrade the managed device using the WebUI. The fix ensures that users are able to upgrade the managed device using the WebUI. This issue was observed in managed devices running AOS-W 8.5.0.10 or later versions.	AOS-W 8.5.0.10
AOS-210715	—	The **ValidUser** ACL displayed only IPv6 entries even when the PEFNG license was not enabled. The fix ensures that the **ValidUser** ACL displays all valid entries. This issue was observed in managed devices running AOS-W 8.6.0.4 or later versions.	AOS-W 8.6.0.4

Table 6: *Resolved Issues in AOS-W 8.7.1.1*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-210805	—	The **Traffic Analysis** window in the **Dashboard > Overview > Wireless Clients** page displayed the error message, **Error retrieving information Please try again later**. The fix ensures that the WebUI displays the traffic analysis data. This issue was observed in stand-alone switches and managed devices running AOS-W 8.7.0.0 or later versions.	AOS-W 8.7.0.0
AOS-211227	—	Some APs sent beamforming sounding frames during EAPoL authentication. The fix ensures that beamforming sounding frames are sent after EAPoL authentication. This issue was observed in APs running AOS-W 8.6.0.5 or later versions.	AOS-W 8.6.0.5
AOS-211429	—	The **Authmgr** process generated the **Error ERROR: value too long for type character varying(32)** error message when the TACACS user name exceeded 32 characters. The fix ensures that the managed devices work as expected. This issue was observed in managed devices running AOS-W 8.3.0.0 or later versions.	AOS-W 8.3.0.0
AOS-211476	—	Some APs came up in a restricted mode after upgrading from AOS-W 8.2.2.6 to AOS-W 8.6.0.5 or later versions. This issue occurred due to AP LLDP power negotiation interoperability issue with Cisco 9000 switches. The fix ensures that the APs do not come up in restricted mode.	AOS-W 8.6.0.5
AOS-212298	—	Some OAW-AP514 access points running AOS-W 8.5.0.10 or later versions crashed and rebooted unexpectedly. The log file listed the reason for the event as **BadAddr:ffffffffffffffb0 PC:shash_ahash_digest+0x4c/0x138 Warm-reset**. The fix ensures that the APs work as expected.	AOS-W 8.5.0.10
AOS-212305	—	ACLs created using upper case characters were displayed in lower case when the **show running-config** command was executed. The fix ensures that the ACL names are displayed correctly. This issue was observed in stand-alone switches running AOS-W 8.6.0.5 or later versions.	AOS-W 8.6.0.5
AOS-212373 AOS-212529	—	Some OAW-AP515 access points running AOS-W 8.5.0.10 or later versions crashed and rebooted unexpectedly. The log file listed the reason for the event as **wlc_sendampdu+0x2e84/ampdu_cleanup_tid_ini+0x23c**. The fix ensures that the APs work as expected.	AOS-W 8.5.0.10
AOS-212856	—	A managed device running AOS-W 8.6.0.2 or later versions displayed a very low **Max/Actual-EIRP** value. The fix ensures that the managed device displays the correct **Max/Actual-EIRP** value.	AOS-W 8.6.0.2
AOS-212973	—	The **no ipv6 enable** command did not disable the IPv6 feature. The fix ensures that the command disables the IPv6 feature. This issue was observed in Mobility Masters running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.0
AOS-213510	—	IoT manager did not send the correct configuration to APB. The fix ensures that the IoT feature works as expected. This issue was observed in Mobility Masters running AOS-W 8.7.1.0.	AOS-W 8.7.1.0

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 8.7.1.1*

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

Table 7: *Known Issues in AOS-W 8.7.1.1*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-188972	—	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: ■ 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-193701 AOS-209485	—	The **Rx Data Bytes** value in the **show ap debug radio-stats** command was lower than the actual value. The fix ensures that the correct number of data bytes are received. This issue was observed in stand-alone switches running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.0
AOS-194919	—	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. **Duplicates:** AOS-195565, AOS-205648, AOS-206010, AOS-208602, AOS-208661, AOS-209625, AOS-212628, and AOS-213869	AOS-W 8.6.0.0
AOS-196399	—	DDS traffic causes IP reassembly failures in datapath. This issue is observed in Mobility Masters running AOS-W 8.3.0.6 or later versions.	AOS-W 8.3.0.6
AOS-197210	—	WebUI takes a long time to display data. 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-199884	—	Mobility Master logs the following error messages, **PAPI_Free: This buffer 0x4f6c48 may already be freed** and **PAPI_Free: Bad state index 0 state 0x1.** This issue is observed in Mobility Masters running AOS-W 8.5.0.5 or later versions.	AOS-W 8.5.0.5
AOS-201166 AOS-207939 AOS-209042	—	A switch crashes and reboots unexpectedly when the **HTTPD** process is restarted. The log files list the reason for the event as **Reboot cause: Nanny rebooted machine - httpd_wrap process died (Intent:cause:register 34:86:0:2c)**. This issue is observed in stand-alone switches running AOS-W 8.2.0.0 or later versions.	AOS-W 8.5.0.2

Table 7: *Known Issues in AOS-W 8.7.1.1*

New Bug ID	Old Bug ID	Description	Reported Version
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-203049 AOS-207780 AOS-208611 AOS-210394 AOS-212485 AOS-214564	—	Some managed devices running AOS-W 8.5.0.5 or later versions crash and reboot unexpectedly. The log file lists the reason for the event as **Reboot Cause: Datapath timeout (SOS Assert) (sp_sbeth_poe_map_age).**	AOS-W 8.5.0.5
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-203517 AOS-204709	—	The **Datapath** process 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-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-203910 AOS-209692	—	The stand-alone switches running AOS-W 8.6.0.3 or later versions crash and reboot unexpectedly. The log file lists the reason for the event as, **Datapath timeout (Heartbeat Initiated) (Intent:cause:register 53:86:0:2c)**.	AOS-W 8.6.0.3
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-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-206537	—	The **H** flag indicating standby tunnel is not displayed in the output of the **show datapath tunnel-table** command and this results in a network loop. This issue is observed in Mobility Masters running AOS-W 8.6.0.4 or later versions.	AOS-W 8.6.0.4

Table 7: *Known Issues in AOS-W 8.7.1.1*

New Bug ID	Old Bug ID	Description	Reported Version
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-206725	—	High CPU utilization is observed on a Mobility Master when the user inserts a USB modem. This issue is observed in Mobility Masters running AOS-W 8.6.0.3 or later versions.	AOS-W 8.6.0.3
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-206765 AOS-208978	—	A few show commands fail to display output. This issue is observed in managed devices running AOS-W 8.7.0.0 or later versions.	AOS-W 8.7.0.0
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-206801	—	A managed device running AOS-W 8.2.2.3 or later versions contacts the Activate server more than once during ZTP. This issue is observed in managed devices running AOS-W 8.2.2.3 or later versions.	AOS-W 8.2.2.3
AOS-206888	—	A few APs take up to 30 minutes to be operational and join the managed device, when they are provisioned for the first time in a native IPv6 deployment. This issue is observed in OAW-AP515 and OAW-AP555 access points running AOS-W 8.7.0.0 in a cluster setup.	AOS-W 8.7.0.0
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-206907	—	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 **Kernel panic - not syncing: assert**.	AOS-W 8.5.0.5
AOS-206929	—	The **show global-user-table** command does not provide an IPv6 based filtering option. This issue is observed in Mobility Masters running AOS-W 8.7.0.0 or later versions.	AOS-W 8.7.0.0

Table 7: *Known Issues in AOS-W 8.7.1.1*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-206930	—	Some Mobility Masters running AOS-W 8.7.0.0 or later versions allow to configure the same IPv6 address twice. This issue occurs when the user enters the same IPv6 address in a different format.	AOS-W 8.7.0.0
AOS-207237	—	A few clients are unable to connect to APs running AOS-W 8.6.0.4 or later versions. **Duplicates:** AOS-203038, AOS-209048, AOS-210038, AOS-210443, AOS-210641, AOS-210664, AOS-212228, AOS-212388, AOS-213327, AOS-213496, AOS-209237, and AOS-209443	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-207303	—	Users are unable to add a managed device to an existing cluster of managed devices configured with rap-public-ip. This issue is observed in managed devices running AOS-W 8.7.0.0 or later versions.	AOS-W 8.7.0.0
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-207691	—	CLI displays incorrect IP address for a TACACS server. This issue is observed in managed devices running AOS-W 8.3.0.8 or later versions. **Workaround:** Restart the **profmgr** process for CLI to display the correct IP address.	AOS-W 8.3.0.8
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-207701	—	The RADIUS request packets do not contain the state attribute value and hence, clients face connectivity issue. This issue occurs due to a race condition. This issue is observed in managed devices running AOS-W 8.4.0.0 or later versions.	AOS-W 8.4.0.0
AOS-207795	—	Users are unable to access the WebUI of the Mobility Master. This issue is observed in Mobility Masters running AOS-W 8.2.2.6 or later versions.	AOS-W 8.2.2.6
AOS-207915	—	Some OAW-AP500 Series access points running AOS-W 8.6.0.4 or later versions crash and reboot unexpectedly. The log file lists the reason for the event as **AP Reboot reason: BadAddr:ecf47526bb436b6e PC:wlc_mutx_bw_policy_update+0x156c/0x2938 [wl_v6] Warm-reset.** **Duplicates:** AOS-208119, AOS-209128, AOS-210182, AOS-210217, AOS-211247, AOS-211252, AOS-211715, AOS-211774, AOS-212111, AOS-212235, AOS-212557, AOS-212741, AOS-212930, AOS-212961, and AOS-214656	AOS-W 8.6.0.4

Table 7: *Known Issues in AOS-W 8.7.1.1*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-208337 AOS-209348 AOS-212655 AOS-213442	—	The **airmatch_recv** process crashes on Mobility Controller Virtual Appliances running AOS-W 8.5.0.7 or later versions.	AOS-W 8.5.0.7
AOS-208420	—	Users are unable to log in to CLI of a switch. This issue occurs when the password has special characters, < and/or >. This issue is observed in switches running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.5
AOS-208421	—	Some managed devices running AOS-W 8.5.0.10 crash and reboot unexpectedly. The log file lists the reason for the event as **Reboot Cause: Soft Watchdog reset**. **Duplicates:** AOS-209367, AOS-209509, AOS-209606, AOS-211577, AOS-211772, AOS-211879, and AOS-212502.	AOS-W 8.5.0.10
AOS-208597	—	The **show ap mesh monitor stats** command returns 0 for output. This issue is observed in Mobility Masters running AOS-W 8.7.0.0 or later versions.	AOS-W 8.7.0.0
AOS-208696	—	The **profmgr** process crashes after configuring LACP and the error message, **Module profmgr is busy** is displayed. This issue is observed in Mobility Masters running AOS-W 8.6.0.4 or later versions.	AOS-W 8.6.0.4
AOS-209069	—	The control plane security configuration, **auto-cert-allowed-addrs** pushed from a Mobility Master to the managed devices is not visible in the **Configuration > System > CPSec** page of the WebUI. This issue is observed in managed devices running AOS-W 8.5.0.9 or later versions.	AOS-W 8.5.0.9
AOS-209130	—	Stale user entries are not removed from the user-table and hence, new users cannot connect to the managed device. This issue is observed in managed devices running AOS-W 8..6.0.4 or later versions.	AOS-W 8..6.0.4
AOS-209323	—	The **Server Group Match Rules** option for **Internal** server in the **Authentication > Auth Servers** page of the WebUI is not available in Mobility Masters running AOS-W 8.7.0.0 or later versions.	AOS-W 8.7.0.0
AOS-209352	—	Some managed devices terminating VIA connection display the error message, **httpd[30106]: Reached session limit: 64**. This issue is observed in managed devices running AOS-W 8.6.0.5 or later versions.	AOS-W 8.6.0.5
AOS-209545	—	MAC authentication is not initialized when IPv6 is globally disabled. This issue is observed in managed devices running AOS-W 8.3.0.13.	AOS-W 8.3.0.13
AOS-209626	—	A few clients experience connectivity issue. This issue is observed in managed device running AOS-W 8.6.0.4 or later versions.	AOS-W 8.6.0.4

Table 7: *Known Issues in AOS-W 8.7.1.1*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-209640	—	A few clients are unable to receive IP addresses from the VLAN configured on LLDP-MED network policy profile. This issue is observed in managed devices running AOS-W 8.5.0.9 or later versions.	AOS-W 8.5.0.9
AOS-209797	—	Some Mobility Master Hardware Appliances running AOS-W 8.6.0.4 or later versions intermittently return high values for SNMP walk for OID **ifOutDiscards.**	AOS-W 8.6.0.4
AOS-209977	—	SNMP query with an incorrect string fails to record the offending IP address in the trap or log information. This issue is observed in managed devices running AOS-W 8.5.0.10 or later versions.	AOS-W 8.5.0.10
AOS-209996	—	Some APs running AOS-W 8.5.0.9 or later versions crash and reboot unexpectedly. The log file lists the reason for the event as **Reboot caused by kernel panic: __bug**.	AOS-W 8.5.0.9
AOS-210065	—	A few users are unable to connect to an AP. This issue is observed in APs running AOS-W 8.5.0.10 or later versions.	AOS-W 8.5.0.10
AOS-210122	—	Clients are unable to receive the IP addresses from their respective VLANs. This issue occurs when clients are connected to a OAW-RAP. This issue is observed in managed devices running AOS-W 8.7.0.0 or later versions.	AOS-W 8.7.0.0
AOS-210342	—	The VRRP authentication password is not encrypted in the output of the **show running config** command. This issue is observed in managed devices running AOS-W 8.5.0.10 or later versions.	AOS-W 8.5.0.10
AOS-210404	—	The **Pending Changes** option does not appear in the WebUI. This issue occurs there are too many unsaved nodes and the **show configuration unsaved-nodes** command has on output of more than 1024 characters. This issue is observed in Mobility Masters running AOS-W 8.3.0.7 or later versions.	AOS-W 8.3.0.7
AOS-210416 AOS-210480	—	The **show ap client trail-info** command display incorrect **VLAN(s)** values. This issue is observed in Mobility Masters running AOS-W 8.5.0.8 or later versions.	AOS-W 8.5.0.8
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-210484	—	Some managed devices running AOS-W 8.0.0.0 or later versions do not display the 802.11k measurements from clients.	AOS-W 8.3.0.6
AOS-210638	—	The **ARM** process crashes on managed devices running AOS-W 8.6.0.5 or later versions.	AOS-W 8.6.0.5
AOS-210896	—	Hotspot 2.0 IEs are not present in beacons frames. This issue is observed in APs running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.0

Table 7: *Known Issues in AOS-W 8.7.1.1*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-210922	—	The **auth** process crashes on stand-alone switches and APs reboot unexpectedly. The log file lists the reason for the reboot as **Unable to set up IPSec tunnel, Error:RC_ERROR_IKEV2_TIMEOUT.** This issue is observed in stand-alone switches running AOS-W 8.5.0.10 or later versions.	AOS-W 8.5.0.10
AOS-210990	—	Some managed devices send BPDUs when STP is globally disabled. This issue is observed in managed devices running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.4
AOS-211256	—	The SFP J8177D, JD089B, and Cisco GLC-TE transceivers do not work with OAW-4450 switches running AOS-W 8.6.0.3.	AOS-W 8.6.0.3
AOS-211448	—	Some APs running AOS-W 8.7.0.0 or later versions crash and reboot unexpectedly. The log file lists the reason for the reboot as **BadPtr:00000028 PC:anul_aon_buf_release+0x14/0x70 [anul] Warm-reset.**	AOS-W 8.7.0.0
AOS-211472	—	Captive portal fails to send mails to guest accounts. This issue occurs when the SMTP server fails to validate the host. This issue is observed in stand-alone switches running AOS-W 8.7.0.0 or later versions.	AOS-W 8.7.0.0
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-211730	—	Users are unable to a map server certificate as switch certificate on a secondary Mobility Master running AOS-W 8.5.0.10 or later versions.	AOS-W 8.5.0.10
AOS-211782	—	Users are unable to delete a policy assigned to a role and the error message, **No Changes Done** is displayed. This issue is observed in Mobility Masters running AOS-W 8.7.0.0 or later versions.	AOS-W 8.7.0.0
AOS-211863	—	Some APs do not come up on managed devices. This issue occurs when ■ the forwarding mode is changed to bridge mode. ■ the name of the ACL is 64 bytes. This issue is observed in managed devices running AOS-W 8.6.0.5 or later versions.	AOS-W 8.6.0.5
AOS-211878 AOS-214377	—	Some APs fail to come up as OAW-RAPs. This issue occurs when the MTU size is not adjusted automatically. This issue is observed in APs running AOS-W 8.6.0.5 or later versions.	AOS-W 8.6.0.5
AOS-212039	—	User debug logging information is not available in **Configuration > System > Logging > Logging Levels** page of the WebUI. This issue is observed in Mobility Masters running AOS-W 8.5.0.10 or later versions.	AOS-W 8.5.0.10
AOS-212063	—	Licenses get installed with incorrect dates in Mobility Masters running AOS-W 8.5.0.10 or later versions.	AOS-W 8.5.0.10

Table 7: *Known Issues in AOS-W 8.7.1.1*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-212123	—	The SNMP trap **wlsxNUserAuthenticationFailed** is not generated upon failed authentication in a termination-enabled dot1X configuration. This issue occurs in stand-alone switches running AOS-W 8.0.0.0 or later versions.	AOS-W 8.3.0.0
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-212486	—	L2TP IP address leak is observed and VLAN pool gets exhausted. This issue is observed in managed devices running AOS-W 8.5.0.11.	AOS-W 8.5.0.11
AOS-212554	—	VIA connection fails and high **ISAKMP CPU** usage is observed. This issue is observed in managed devices running AOS-W 8.6.0.6.	AOS-W 8.6.0.6
AOS-212576	—	Some APs running AOS-W 8.6.0.5 or later versions crash and reboot unexpectedly. The log file lists the reason for the event as **Kernel panic - not syncing: rcu_sched detected stalls (pc is at __schedule+0x78/0x360).**	AOS-W 8.6.0.5
AOS-212591	—	Some managed devices running AOS-W 8.7.1.0 crash and reboot unexpectedly. The log file lists the reason for the event as **Reboot Cause: Kernel Panic (Intent:cause:register 12:86:b0:2)**.	AOS-W 8.7.1.0
AOS-212599 AOS-211699 AOS-212564 AOS-212567	—	Some APs running AOS-W 8.6.0.5 or later versions crash and reboot unexpectedly. The log file lists the reason for the event as **Kernel panic - not syncing: jiffies stall (pc is at __schedule+0x78/0x360).**	AOS-W 8.6.0.5
AOS-212707	—	Some Mobility Masters running AOS-W 8.5.0.10 log the error message, **Fri Oct 16 23:58:53 2020, 0, 0, 0, 0, 0, 0, 0.**	AOS-W 8.5.0.10
AOS-212843	—	A few clients in bridge mode are randomly assigned the default role instead of the derived role. This issue is observed in managed devices running AOS-W 8.0.0.0 or later versions.	AOS-W 8.6.0.4
AOS-212991	—	The **use-ip-for-calling-station** parameter of the **aaa authentication-server radius** command does not work as expected for VIA clients. This issue is observed in stand-alone switches running AOS-W 8.6.0.6.	AOS-W 8.6.0.6
AOS-213089 AOS-213044 AOS-213295 AOS-214238 AOS-214431	—	Some managed devices running AOS-W 8.3.0.0 or later versions crash and reboot unexpectedly. The log file lists the reason for the event as **Reboot Cause: Kernel Panic (Intent:cause:register 12:86:f0:2)**.	AOS-W 8.3.0.0

Table 7: *Known Issues in AOS-W 8.7.1.1*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-213099 AOS-214123	—	The **dpagent** process crashes on managed devices running AOS-W 8.5.0.10 or later versions.	AOS-W 8.5.0.10
AOS-213115	—	Some managed devices running AOS-W 8.5.0.10 crash and reboot unexpectedly. The log file lists the reason for the event as **Reboot caused by kernel panic: Take care of the HOST ASSERT first.**	AOS-W 8.5.0.10
AOS-213132	—	Users are unable to upload server certificates in PEM or DER format. This issue is observed in Mobility Masters running AOS-W 8.6.0.6-FIPS. **Workaround:** Temporarily upload root CA and intermediate CAs as trusted CA in /mm node. This accepts the server certificates in PEM/DER format in /md node. When server certificate configuration in /md path node is successful, CA certificates from /mm node can be removed.	AOS-W 8.6.0.6
AOS-213305 AOS-213310	—	Some OAW-AP515 access points running AOS-W 8.7.0.0 or later versions crash and reboot unexpectedly. The log file lists the reason for the event as **PC is at wlc_nar_dotxstatus+0x88/0x7d8: AOS-200674 instrumentation kicks in (wlc_nar_validate_cubby)**.	AOS-W 8.7.0.0
AOS-213308	—	Some OAW-AP515 access points running AOS-W 8.7.0.0 or later versions crash and reboot unexpectedly. The log file lists the reason for the event as **PC is at asap_ap_dev_xmit+0x118/0x4d0.**	AOS-W 8.7.0.0
AOS-213309	—	Some OAW-AP515 access points running AOS-W 8.7.0.0 or later versions crash and reboot unexpectedly. The log file lists the reason for the event as **PC is at wlc_ratesel_clr_cache+0x2c/0xa0.**	AOS-W 8.7.0.0
AOS-213558	—	Users are unable to add a new node to an existing cluster of eight nodes. This issue is observed in managed devices running AOS-W 8.5.0.6 or later versions.	AOS-W 8.5.0.6
AOS-214243	—	A managed device running AOS-W 8.7.1.0 or later versions crash and reboot unexpectedly. The log file lists the reason for the event as **Reboot Cause: Kernel Panic (Intent:cause:register 12:86:b0:2)**. This issue occurs due to a race condition.	AOS-W 8.7.1.0

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, 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 software 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 36 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 36 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 36 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.

Ensure that there is enough free memory and flash space on your Mobility Master or managed device. For details, see Memory Requirements on page 35.

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 36 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 36 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 36.
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
   ```

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.