AOS-W 8.11.0.1 Release Notes

Alcatel·Lucent

Enterprise

Copyright Information

The Alcatel-Lucent name and logo are trademarks of Nokia used under license by ALE. To view other trademarks used by affiliated companies of ALE Holding, visit: www.al-enterprise.com/en/legal/trademarks-copyright. All other trademarks are the property of their respective owners. The information presented is subject to change without notice. Neither ALE Holding nor any of its affiliates assumes any responsibility for inaccuracies contained herein.

Open Source Code

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

Contents

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 01	Initial release.

This AOS-W release notes includes the following topics:

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

Important

The factory-default image of APs introduced in AOS-W 8.9.0.0 or later versions use **aruba-conductor** as the host name instead of **aruba-master** to identify a target managed device or stand-alone switch during DNS discovery. However, the factory-default image of APs that were introduced prior to AOS-W 8.9.0.0 still use **aruba-master** during DNS discovery. The usage of **aruba-conductor** is to align with the Inclusive Language Initiative.

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 Conductor Licensing Guide*
- *Alcatel-Lucent Virtual Appliance Installation Guide*
- *Alcatel-Lucent AP Software Quick Start Guide*

Supported Browsers

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

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

Terminology Change

As part of advancing Alcatel-Lucent Enterprise's commitment to racial justice, we are taking a much-needed step in overhauling ALE engineering terminology to reflect our belief system of diversity and inclusion. Some legacy

products and publications may continue to include terminology that seemingly evokes bias against specific groups of people. Such content is not representative of our ALE culture and moving forward, ALE will replace racially insensitive terms and instead use the following new language:

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

Contacting Support

Table 2: *Contact Information*

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

There are no new features or enhancements introduced in this release.

Behavioral Changes

This release does not introduce any changes in AOS-W behaviors, resources, or support that would require you to modify the existing system configurations after updating to 8.11.0.1.

This chapter describes the platforms supported in this release.

Mobility Conductor Platforms

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

Table 3: *Supported Mobility Conductor Platforms*

Mobility Conductor Family	Mobility Conductor Model
Hardware Mobility Conductor	MCR-HW-1K, MCR-HW-5K, MCR-HW-10K
Virtual Mobility Conductor	MCR-VA-50, MCR-VA-500, MCR-VA-1K, MCR-VA-5K, MCR-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*

OmniAccess Mobility Controller Family	OmniAccess Mobility Controller Model
OAW-40xx Series OmniAccess Mobility Controllers	OAW-4005, OAW-4008, OAW-4010, OAW-4024, OAW-4030
OAW-4x50 Series OmniAccess Mobility Controllers	OAW-4450, OAW-4550, OAW-4650, OAW-4750, OAW-4750XM, OAW-4850
OAW-41xx Series OmniAccess Mobility Controllers	OAW-4104, 9012
9200 Series OmniAccess Mobility Controllers	9240
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*

AP Family	AP Model
OAW-AP300 Series	OAW-AP304, OAW-AP305
OAW-AP303 Series	OAW-AP303, OAW-AP303P

Table 5: *Supported AP Platforms*

AP Family	AP Model
OAW-AP303H Series	OAW-AP303H, OAW-303HR
OAW-AP310 Series	OAW-AP314, OAW-AP315
OAW-AP318 Series	OAW-AP318
OAW-AP360 Series	OAW-AP365, OAW-AP367
OAW-AP370 Series	OAW-AP374, OAW-AP375, OAW-AP377
OAW-AP370EX Series	OAW-AP375EX, OAW-AP377EX, OAW-AP375ATEX
OAW-AP500 Series	OAW-AP504, OAW-AP505
OAW-AP500H Series	OAW-AP503H, OAW-AP503HR, OAW-AP505H, OAW-AP505HR
OAW-AP510 Series	OAW-AP514, OAW-AP515, OAW-AP518
OAW-AP518 Series	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
OAW-AP580 Series	OAW-AP584, OAW-AP585, OAW-AP585EX, OAW-AP587, OAW-AP587EX
OAW-AP610 Series	OAW-AP615
OAW-AP630 Series	OAW-AP635
OAW-AP650 Series	OAW-AP655

Deprecated APs

The following APs are no longer supported from AOS-W 8.11.0.0 onwards.

Table 6: *Deprecated AP Platforms*

AP Family	AP Model
OAW-AP200 Series	OAW-AP204, OAW-AP205
OAW-AP203H Series	OAW-AP203H
OAW-AP203R Series	OAW-AP203R, OAW-AP203RP

Table 6: *Deprecated AP Platforms*

AP Family	AP Model
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-AP320 Series	OAW-AP324, OAW-AP325
OAW-AP330 Series	OAW-AP334, OAW-AP335
OAW-AP340 Series	OAW-AP344, OAW-AP345
OAW-AP387	OAW-AP387

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

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

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

The following DRT file version is part of this release:

- DRT-1.0_85483

This chapter describes the resolved issues in this release.

Table 7: *Resolved Issues in AOS-W 8.11.0.1*

New Bug ID	Description	Reported Version
AOS-235820	The **wms** process crashed on Mobility Conductors running AOS-W 8.10.0.2 or later versions. This issue occurred when the **wms** process exceeded the virtual memory limit of 2 GB. The fix ensures that the Mobility Conductors work as expected.	AOS-W 8.10.0.2
AOS-236242	The **apmove** command did not work as expected when the APs were connected to the backup LMS switches. The fix ensures that the **apmove** command works as expected. This issue was observed in managed devices running AOS-W 8.6.0.0 or later versions.	AOS-W 8.7.1.9
AOS-237372	A few OAW-AP610 Series access points running AOS-W 8.11.0.0 or later versions used the 6 GHz radio to connect to Wi-Fi uplink although the 6 GHz radio was disabled using the **apoot** command. The fix ensures that the APs do not use the 6 GHz radio to connect to Wi-Fi uplink when the 6 GHz radio is disabled.	AOS-W 8.11.0.0
AOS-237473 AOS-238104	The core files of the **nanny** process were not collected by the Mobility Conductor. The fix ensures that the Mobility Conductor collects the core files of the **nanny** process. This issue was observed in Mobility Conductor running AOS-W 8.7.1.9 or later versions.	AOS-W 8.7.1.9
AOS-237815	Mobility Conductors running AOS-W 8.6.0.19 or later versions did not have sufficient free flash space. This issue occurred when the AP image files consumed excessive flash space. The fix ensures that the Mobility Conductors work as expected.	AOS-W 8.6.0.19
AOS-238218	The mongo database took up a lot of flash space. This issue was observed in Mobility Conductors running AOS-W 8.9.0.3 or later versions. The fix ensures that the Mobility Conductors work as expected.	AOS-W 8.9.0.3
AOS-238298	Configuration changes that were made to the BLE UUID and the advertising interval parameters of the BLE service profile, were not updated on the Mobility Conductor. The fix ensures that the changes are updated correctly on the Mobility Conductor. This issue was observed in Mobility Conductors running AOS-W 8.10.0.2 or later versions.	AOS-W 8.10.0.2
AOS-238456 AOS-238906	Some stand-alone switches failed to perform IKE fragmentation for VIA clients. This issue occurred when VIA clients used EAP-MSCHAPv2 for authentication. The fix ensures that the switches perform IKE fragmentation for VIA clients. This issue was observed in stand-alone switches running AOS-W 8.7.1.11 or later versions.	AOS-W 8.7.1.11

Table 7: *Resolved Issues in AOS-W 8.11.0.1*

New Bug ID	Description	Reported Version
AOS-238578 AOS-238575 AOS-238576	The **halt** command did not save the audit-trail logs of the stand-alone switches. As a result, the **show audit-trail history** command did not display the configuration changes done before a reboot. The fix ensures that the **halt** command saves the audit-trail logs of the switches. This issue was observed in stand-alone switches running AOS-W 8.10.0.3 or later versions.	AOS-W 8.10.0.3
AOS-238589 AOS-239319	The **impystart** process crashed on Mobility Conductor Virtual Appliances running AOS-W 8.10.0.2 or later versions. The fix ensures that the Mobility Conductor Virtual Appliances work as expected.	AOS-W 8.10.0.2
AOS-238848	Some managed devices running AOS-W 8.10.0.2 or later versions displayed an error message, **Different SNMP hosts should not have same engine-id value**, while configuring the SNMPv3 trap host. This issue occurred when the same SNMP engine-id was configured for multiple SNMPv3 trap hosts. The fix ensures that the managed devices work as expected.	AOS-W 8.10.0.2
AOS-238921	Some OAW-4750XM switches running AOS-W 8.10.0.2 or later versions crashed and rebooted unexpectedly. The log files listed the reason for the event as **Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2)**. This issue occurred when IPv6 DNS response was received. The fix ensures that the switches work as expected.	AOS-W 8.10.0.2
AOS-238954	Clients that used machine and user authentication were unable to connect to SSIDs. This issue was observed when WPA3 encryption was used. The fix ensures seamless connectivity. This issue was observed in OAW-AP515 access points running AOS-W 8.6.0.18 or later versions.	AOS-W 8.6.0.18
AOS-238960	Some stand-alone switches running AOS-W 8.7.1.8 or later versions crashed and rebooted unexpectedly. The log files listed the reason for the event as **Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2)**. The fix ensures that the stand-alone switches work as expected.	AOS-W 8.7.1.8
AOS-239260	Some OAW-AP505 access points running AOS-W 8.6.0.18 or later versions crashed and rebooted unexpectedly. The log files listed the reason for the event as **BadPtr:00000294 PC:tun_recv_esp2_prep+0x10c/0x15c Warm-reset**. The fix ensures that the APs work as expected.	AOS-W 8.6.0.18

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

Limitations

Following are the limitations observed in this release.

Spectrum Analysis Support for OAW-AP615

The Spectrum Analysis feature is not supported on OAW-AP615 access points.

UNII-4 Channel Support for OAW-AP615

OAW-AP615 access points do not support UNII-4 channel.

OAW-40xx Series and OAW-4x50 Series Controllers

The **cpboot** command does not upgrade the AOS-W software version of OAW-40xx Series and OAW-4x50 Series controllers.

Known Issues

Following are the known issues observed in this release.

Table 8: *Known Issues in AOS-W 8.11.0.1*

New Bug ID	Description	Reported Version
AOS-151022 AOS-188417	The output of the **show datapath uplink** command displays an incorrect session count. This issue is observed in managed devices running AOS-W 8.1.0.0 or later versions. Old Bug ID: 185176	AOS-W 8.1.0.0
AOS-156661 AOS-224890	The authentication survivability feature does not work as expected when the uplink is down. This issue is observed in managed devices running AOS-W 8.2.2.2 or later versions.	AOS-W 8.2.2.2

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 the user role is in trunk mode. This issue is observed in OAW-4005 switches running AOS-W 8.4.0.0.
	Workaround:
	Perform the following steps to resolve the issue:
	    1.Remove web category from the ACL rules and apply **any any any permit** policy.
	    2. Disable WebCC on the user role.
	    3. Change the VLAN of user role from trunk mode to access mode.
		AOS-W 8.4.0.0

Table 8: *Known Issues in AOS-W 8.11.0.1*

New Bug ID	Description	Reported Version
AOS-195434	Some APs crash and reboot 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 or later versions.	AOS-W 8.5.0.2
AOS-216536 AOS-220630	Some managed devices running AOS-W 8.5.0.11 or later versions are unable to come up on the Mobility Conductor. This issue occurs when the managed devices receive the branch IP address as the switch IP address in a VPNC deployment.	AOS-W 8.5.0.11
AOS-218161	The output of the **show running-config** command displays the error message, **An internal system error has occurred at file amapi_ common.c function deserializeCommandList line 940 error sxdr_ read_u32_safe &numEntries failed**. This issue is observed in Mobility Conductors running AOS-W 8.9.0.0 or later versions.	AOS-W 8.9.0.0
AOS-219315	Some OAW-4104 switches running AOS-W 8.7.1.10 or later versions crash and reboot unexpectedly. The log files list the reason for the event as **Reboot Cause: Kernel Panic (Intent:cause: 86:50)**. Duplicates: AOS-223786, AOS-223787, AOS-240010, AOS-234981, and AOS-220422	AOS-W 8.7.1.10
AOS-223221 AOS-237950	Some OAW-AP514 and OAW-AP515 access points running AOS-W 8.7.1.4 or later versions generate the error logs, **CPU: 1 PID: 1979 at ../../../../soft - ap/broadcom/esdk6/main/src/wl/../../src/wl/sys/wlc.c:22608 wlc_ calc_frame_time+0x12c/0x410 [wl_v6]()**.	AOS-W 8.7.1.4
AOS-227306	Some managed devices respond to the ARP probe frames with the SRC MAC address of the clients that are not connected to the network. This issue is observed in managed devices running AOS-W 8.7.1.5 or later versions.	AOS-W 8.7.1.5
AOS-228799 AOS-238163	Some managed devices running AOS-W 8.6.0.16 or later versions crash and reboot unexpectedly. The log files list the reason for the event as **Datapath timeout (Fpapps Initiated)**.	AOS-W 8.6.0.16
AOS-229190 AOS-229798	The **Dashboard** > **Overview** > **Clients** page of the WebUI does not display active and standby switch information. This issue is observed in Mobility Conductors running AOS-W 8.10.0.0 or later versions.	AOS-W 8.10.0.0
AOS-231473	The **Dashboard > Overview > Wired Clients** page of the WebUI does not display the details of the APs to which the clients are connected. This issue occurs in a pure IPv6 deployment. This issue is observed in Mobility Conductors running AOS-W 8.8.0.2 or later versions.	AOS-W 8.8.0.2
AOS-232970	The AP MAC address is not present in the calling station ID of the RADIUS accounting packets and hence, the RADIUS accounting requests are discarded. This issue is observed in managed devices running AOS-W 8.7.1.6 or later versions in a cluster setup.	AOS-W 8.7.1.6

Table 8: *Known Issues in AOS-W 8.11.0.1*

New Bug ID	Description	Reported Version
AOS-233809	Users are unable to add GRE tunnels to a tunnel group and an incorrect error message, **Error: Tunnel is already part of a different tunnel-group** is displayed. This issue is observed in managed devices running AOS-W 8.6.0.8 or later versions.	AOS-W 8.6.0.8
AOS-234265 AOS-232356	Enet port flapping is observed on a few APs that are connected to the Cisco 9300 switches. As a result, the APs reboot and clients experience connectivity issues. This issue is observed in OAW-AP535 access points running AOS-W 8.6.0.14 or later versions.	AOS-W 8.6.0.14
AOS-234480	The **apflash ap31x-ap32x backup partition** command does not upgrade the backup partition of OAW-AP315 access points running AOS-W 8.7.1.9 or later versions in a cluster setup.	AOS-W 8.7.1.9
AOS-234627	Some managed devices running AOS-W 8.6.0.17-FIPS or later versions crash unexpectedly. This issue occurs after issuing the **aaa test-server** command for a Radsec server.	AOS-W 8.6.0.17-FIPS
AOS-234782	A few OAW-AP505H access points running AOS-W 8.10.0.0 or later versions crash and reboot unexpectedly. The log file lists the reason for the event as **skb double free detected!" at ("file-name/line-number/function-name"**) net/core/skbuff.c:1849/consume_skb().	AOS-W 8.10.0.0
AOS-235242 AOS-235777	The **auth** process crashes and an error message, **auth module busy** is displayed. This issue occurs when the **show run** command is issued. This issue is observed in managed devices running AOS-W 8.6.0.17 or later versions.	AOS-W 8.6.0.17
AOS-235744 AOS-235752	Some managed devices are unable to receive any configuration from the Mobility Conductor. This issue occurs when changes to a few group names are not synchronized on the standby Mobility Conductor before a reboot. This issue is observed in Mobility Conductors running AOS-W 8.6.0.17 or later versions.	AOS-W 8.6.0.17
AOS-236174 AOS-236270 AOS-238242	The deep sleep mode is enabled even when the Green AP feature is not enabled. Also, ports are down and heartbeats are missed on the managed devices. This issue is observed in APs running AOS-W 8.7.1.2 or later versions.	AOS-W 8.7.1.2
AOS-236445	Some users are unable to add or allocate licenses using the WebUI. This issue is observed in Mobility Conductors running AOS-W 8.10.0.2 or later versions.	AOS-W 8.10.0.2
AOS-236577	Some APs running AOS-W 8.7.1.9 or later versions display the error log, **wlc_dpc: 43 callbacks suppressed.**	AOS-W 8.7.1.9
AOS-236841 AOS-238400	The **Configuration > Services > Clusters >Add Controller** page of the WebUI does not display the list of **VRRP VLANs**. This issue is observed in managed devices running AOS-W 8.7.1.9 or later versions.	AOS-W 8.7.1.9
AOS-237050	A few users experience poor upstream network performance. This issue is observed in APs running AOS-W 8.7.1.9 or later versions.	AOS-W 8.7.1.9

Table 8: *Known Issues in AOS-W 8.11.0.1*

New Bug ID	Description	Reported Version
AOS-237052 AOS-208508	The HTTP traffic is incorrectly redirected by the captive portal for some users. This issue occurs when the ACL changes are not updated on the APs. This issue is observed in APs running AOS-W 8.10.0.2 or later versions.	AOS-W 8.10.0.2
AOS-237112	A mismatch of syslog messages is observed for clients connected to bridge mode and tunnel mode SSIDs. This issue is observed in managed devices running AOS-W 8.10.0.0 or later versions.	AOS-W 8.10.0.0
AOS-237113	High latency and jitter are observed on stand-alone switches running AOS-W 8.7.1.9 or later versions.	AOS-W 8.7.1.9
AOS-237203	Some stand-alone switches with IAP-VPN tunnels generate multiple error logs. This issue is observed in stand-alone switches running AOS-W 8.10.0.2 or later versions.	AOS-W 8.10.0.2
AOS-237348	Some OAW-AP535 access points running AOS-W 8.9.0.3 or later versions crash and reboot unexpectedly. The log files list the reason for the reboot as **Reboot caused by kernel panic: Take care of the TARGET ASSERT first at whal_recv.c:1656 Assertion.**	AOS-W 8.9.0.3
AOS-237510	Some WPA3-SAE opmode clients are unable to download user roles from ClearPass Policy Manager after a successful MAC authentication. The log file lists the reason for the event as **Cannot be assigned downloadable role, role is in error state**. This issue is observed in managed devices running AOS-W 8.6.0.18 or later versions.	AOS-W 8.6.0.18
AOS-237619	The **Dashboard > Overview > Wireless Clients** page of the WebUI displays an incorrect number of clients. This issue occurs due to a race condition. This issue is observed in Mobility Conductors running AOS-W 8.10.0.2 or later versions. Duplicates: AOS-239654, AOS-239801, AOS-239880, AOS-239883, and AOS-240051	AOS-W 8.10.0.2
AOS-237851	Some OAW-AP535 access points running AOS-W 8.10.0.2 or later versions crash and reboot unexpectedly. The log files list the reason for the event as **Reboot caused by kernel panic: Take care of the TARGET ASSERT first (phyrf_ani.c:718).**	AOS-W 8.10.0.2
AOS-237873 AOS-239428 AOS-238122	Some managed devices are stuck in the **DISCONNECTED-FROM-SELF-CONNECTED-FROM-PEERS** state. This issue occurs when heartbeats are missed on managed devices. This issue is observed in managed devices running AOS-W 8.7.1.10 or later versions in a cluster setup.	AOS-W 8.7.1.10
AOS-237897	The WebCC logs are stored in an invalid message format and as a result, the syslog server reports incorrect data. This issue is observed in managed devices running AOS-W 8.0.0.0 or later versions.	AOS-W 8.7.1.9
AOS-237975	Some users incorrectly fall back to the 802.1X initial role. This issue is observed in managed devices running AOS-W 8.7.1.9 or later versions.	AOS-W 8.7.1.9

Table 8: *Known Issues in AOS-W 8.11.0.1*

New Bug ID	Description	Reported Version
AOS-238147 AOS-239823	Some APs powered up using POE-AT incorrectly come up with **r** flag and are unable to broadcast SSIDs. This issue is observed in APs running AOS-W 8.6.0.0 or later versions.	AOS-W 8.7.1.10
AOS-238150	Users that are connected through IAP-VPN are not listed in the SNMP table. This issue is observed in switches running AOS-W 8.0.0.0 or later versions.	AOS-W 8.0.0.0
AOS-238249	The IPv6 mDNS data packets are dropped unexpectedly. This issue occurs when OpenFLow is enabled. This issue is observed in managed devices running AOS-W 8.10.0.3 or later versions.	AOS-W 8.10.0.3
AOS-238410 AOS-238939 AOS-238564 AOS-238487	The **httpd** process crashes on Mobility Conductors and managed devices running AOS-W 8.6.0.17 or later versions. This issue occurs when a specific type of curl request is sent to the switches.	AOS-W 8.10.0.3
AOS-238500	Some clients are unable to connect to a few APs. This issue occurs when the tunnel between the AP and the managed device in a cluster is down. This issue is observed in APs running AOS-W 8.7.1.9 or later versions.	AOS-W 8.7.1.9
AOS-238511	The information of wired clients connected to a port channel is not sent to OmniVista 3600 Air Manager. This issue is observed in managed devices running AOS-W 8.10.0.3 or later versions.	AOS-W 8.10.0.3
AOS-238701 AOS-238934 AOS-239570	The **authmgr, httpd, fwvisibility, ctamon**, and **ucm** processes are stuck in **NOT_RESPONDING** or I**NITIALIZING** state. This issue is observed in managed devices running AOS-W 8.6.0.19 or later versions in a cluster setup.	AOS-W 8.6.0.19
AOS-238768	WebUI takes a long time to display the AP and client information. This issue is observed in Mobility Conductors running AOS-W 8.10.0.2 or later versions.	AOS-W 8.10.0.2
AOS-238836	Clients that use machine and user authentication are unable to connect to SSIDs. This issue is observed when WPA3 encryption is used. This issue is observed in APs running AOS-W 8.6.0.18 or later versions.	AOS-W 8.6.0.18
AOS-239010	Some users experience poor upstream network performance. This issue is observed in OAW-AP635 access points running AOS-W 8.10.0.2 or later versions.	AOS-W 8.10.0.2
AOS-239202	The **ble_daemon** process consumes high memory and data packets are also dropped. This issue occurs when the BLE operation mode is enabled on the APs. This issue is observed in APs running AOS-W 8.10.0.2 or later versions.	AOS-W 8.10.0.2
AOS-239289	The output of the **show datapath cluster details** command displays an incorrect time stamp. This issue occurs when the managed devices are up for more than 49 days. This issue is observed in managed devices running AOS-W 8.10.0.2 or later versions in a cluster setup.	AOS-W 8.10.0.2

Table 8: *Known Issues in AOS-W 8.11.0.1*

New Bug ID	Description	Reported Version
AOS-239487	The PCAP files of an AP are incorrectly sent to the default folder of the dump server and not to the user-defined folder. This issue is observed in APs running AOS-W 8.10.0.4 or later versions.	AOS-W 8.10.0.4
AOS-239498	Some OAW-AP515 access points running AOS-W 8.6.0.19 or later versions crash and reboot unexpectedly. The log files list the reason for the event as **AP Reboot reason: BadPtr:0000000f PC:wlc_get_ txh_info+0x118/0x210 [wl_v6] Warm-rese**t.	AOS-W 8.6.0.19
AOS-239872	WebUI does not allow users to live upgrade a cluster. However, the CLI allows users to upgrade a cluster. This issue occurs when the name of the cluster contain spaces. This issue is observed in managed devices running AOS-W 8.5.0.0 or later versions.	AOS-W 8.10.0.4
AOS-240549	The managed devices are unable to copy AOS-W images from the SCP server and hence, the upgrade fails on IPv4 clusters. This issue occurs when the file server is not reachable through the management interface. This issue is observed in managed devices running AOS-W 8.11.0.1 in a cluster setup. **Workaround**: Ensure that the file server is reachable via OOB if OOB is configured for platforms that support the OOB Management port.	AOS-W 8.11.0.1

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 Conductor, managed device, or stand-alone switch.

Important Points to Remember

To upgrade your managed device or Mobility Conductor:

- 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 Conductor Licensing Guide*.
- With the introduction of the Long Supported Release (LSR) and Short Supported Release (SSR) terminology in AOS-W 8.10.0.0, a Mobility Conductor running an LSR release supports managed devices running the same release and the three preceding releases. This is considered as N-3 support. This allows a customer to run the latest LSR, the previous SSRs and the previous LSR simultaneously. A Mobility Conductor running an SSR release supports managed devices running the same release and the two preceding releases. This would be considered N-2 support and is the same behavior as the pre-AOS-W 8.10.0.0 MultiVersion support.
- Only for the AOS-W 8.10.0.0 LSR release, AOS-W 8.6.0.0 is treated as an LSR despite being beyond N-3. As such a Mobility Conductor running AOS-W 8.10.0.0 supports managed devices running AOS-W 8.10.0.0, AOS-W 8.9.0.0, AOS-W 8.8.0.0, AOS-W 8.7.0.0 and AOS-W 8.6.0.0.

Memory Requirements

All Alcatel-Lucent managed devices store critical configuration data on an onboard compact flash memory module. Ensure that there is always free flash space on the managed device. Loading multiple large files such as JPEG images for RF Plan can consume flash space quickly. Following are best practices for memory management:

- Do not proceed with an upgrade unless 100 MB of free memory is available. Execute the **show memory** command to identify the available free memory. To recover memory, reboot the managed device. After the managed device comes up, upgrade immediately.

- Do not proceed with an upgrade unless the minimum flash space 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 24 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 24 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 24 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 Conductor, navigate to **Diagnostic > Technical Support > Delete Files** and remove any aging log files or redundant backups.

In the CLI

```
(host) #delete filename <filename>
```

Low Free Flash Memory

Sometimes, after extended use, the flash memory might get used up for logs and other files. The AOS-W image has increased in size and this may cause issues while upgrading to newer AOS-W images without cleaning up the flash memory.

Prerequisites

Before you proceed with the freeing up the flash memory:

- Ensure to always backup the configuration and flash memory. Issue the **backup configuration** and **backup flash** commands to backup the configuration and flash.
- Copy the **flashbackup.tar.gz** and **configbackup.tar.gz** files out of the switch. Then delete the **flashbackup.tar.gz** and **configbackup.tar.gz** files from the flash memory of the switch.
- Use only one partition for the upgrade activity and keep the other partition unchanged.

If you use the WebUI to perform an upgrade, a banner on the **Maintenance** page provides the following reminder to have sufficient free flash memory before initiating an upgrade.

For a healthy and stable system it requires free space of 360 MB for AOS v8.3 and 8.5, 570 MB for AOS 8.6 and 8.7 and 450 MB for AOS 8.8 and higher version in the /flash directory. Please make sure minimum required memory is available in /flash before upgrading to newer version.

Freeing up Flash Memory

The following steps describe how to free up the flash memory before upgrading:

1. Check if the available memory in **/flash** is greater than the limits listed in Table 9 for all supported switch models:

Table 9: *Flash Memory Requirements*

Upgrading from	Upgrading to	Minimum Required Free Flash Memory Before Initiating an Upgrade
8.3.x	8.11.x	360 MB
8.5.x	8.11.x	360 MB
8.6.x	8.11.x	570 MB
8.7.x	8.11.x	570 MB
8.8.x	8.11.x	450 MB
8.9.x	8.11.x	450 MB
8.10.x	8.11.x	450 MB

To check the available free flash memory, issue the **show storage** command. Following is the sample output from a switch with low free flash memory:

```
(host) [mynode] #show storage
Filesystem              Size      Available      Use       %      Mounted on
/dev/usb/flash3         1.4G      1014.2M        386.7M    72%     /flash
```

2. If the available free flash memory is less than the limits listed in Table 9, issue the following commands to free up more memory.
   - **tar crash**
   - **tar clean crash**
   - **tar clean logs**
   - **tar clean traces**

3. Issue the **show storage** command again to check if the available space in **/flash** is more than the minimum space required for AOS-W upgrade as listed in Table 9

4. **If you are unable to free up sufficient flash memory, contact Technical Support. Do not reboot the switch.**

5. If sufficient flash memory is available, proceed with the standard AOS-W upgrade. See Upgrading AOS-W.

6. If a reboot was performed, you may see some of the following errors. Follow the directions below:

   - Upgrade using standard procedure. You may see some of the following errors:

     Error upgrading image: Ancillary unpack failed with tar error (tar: Short header).

     Please clean up the /flash and try upgrade again.

     Error upgrading image: Ancillary unpack failed with tar error (tar: Invalid tar magic).

     Please clean up the /flash and try upgrade again.

     Error upgrading image: Need atleast XXX MB space in /flash for image upgrade, please clean up the /flash and try upgrade again.

     Failed updating: [upgradeImageNew.c] extractAncTar (dev: /dev/usb/flash1 imgLoc: /flash/config/ArubaOS_70xx_8.8.0.0-mm-dev_78066

   - If any of the above errors occur, issue the **show image version** command to check for the default boot partition. The partition which was upgraded should become the default partition. Following is the sample output of the **show image version** command:

```
(host) [mynode] #show image version
-------------------------------
Partition                  : 0:0 (/dev/usb/flash1) **Default boot**
Software Version            : AOS-W 8.9.0.0 (Digitally Signed SHA1/SHA256 - Production
Build)
Build number               : 81046
Label                      : 81046
Built on                   : Thu Aug 5 22:54:49 PDT 2021
-------------------------------
Partition                  : 0:1 (/dev/usb/flash2)
Software Version            : AOS-W 8.7.0.0-2.3.1.0 (Digitally Signed SHA1/SHA256 -
Developer/Internal Build)
Build number               : 0000
Label                      : arpitg@sdwan-2.3_arpitg-3-ENG.0000
Built on                   : Tue Aug 10 15:02:15 IST 2021
```

   - If the default boot partition is not the same as the one where you performed the upgrade, change the default boot partition. Issue the **boot system partition <part_number>** command to change the default boot partition. Enter **0** or **1** for **part_number** representing partition 0:0 or partition 0:1, respectively.

   - Reload the switch. If any of the errors listed in step 4 were observed, the following errors might occur while booting AOS-W 8.9.0.0.

```
Sample error:
[03:17:17]:Installing ancillary FS                [ OK ]
Performing integrity check on ancillary partition 1   [ FAIL : Validating new
ancillary partition 1...Image Integrity check failed for file
/flash/img1/mswitch/sap/arm32.ari. Digest Mismatch]
Extracting Webui files..tar: Short read
chown: /mswitch/webui/*: No such file or directory
chmod: /mswitch/webui/wms/wms.cgi: No such file or directory
```

   - After the switch reboots, the login prompt displays the following banner:

```
****************************************************************
* WARNING:  An additional image upgrade is required to complete the *
* installation of the AP and WebUI files. Please upgrade the boot   *
* partition again and reload the controller.                       *
****************************************************************
```

- Repeat steps 1 through 5. If sufficient free flash memory is available, proceed with the standard AOS-W upgrade procedure. See Upgrading AOS-W.
- If sufficient free flash memory is not available, issue the **dir** and **dir flash** commands to identify large files occupying the flash memory.

> ⚠ **CAUTION**
> Exercise caution while deleting files. Contact Technical Support if you are not sure which large files in the **/flash** directory could be safely deleted to free up the required space.

- Issue the **delete filename <filename>** command to delete large files to free more flash memory.
- Check if sufficient flash memory is free as listed in Table 9.
- Proceed with the standard AOS-W upgrade procedure in the same partition. See Upgrading AOS-W.

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 Conductor 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 Conductor or managed device. For details, see Memory Requirements on page 21.

> **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.

> **NOTE**
>
> The AOS-W image file is digitally signed and is verified using RSA2048 certificates preloaded at the factory. The Mobility Conductor or managed device will not load a corrupted AOS-W image.

4. Log in to the AOS-W WebUI from the Mobility Conductor.

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.

N O T E The upgrade does not take effect until reboot. If you chose to reboot after upgrade, the Mobility Conductor 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 Conductor.

3. Execute the **ping** command to verify the network connection between the Mobility Conductor 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 Conductor.

```
(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 Conductor 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 24 for information on creating a backup.

In the CLI

The following steps describe how to verify that the Mobility Conductor 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 24 for information on creating a backup.

Downgrading AOS-W

A Mobility Conductor or managed device has two partitions, 0 and 1. If the upgrade fails on one of the partitions, you can reboot the Mobility Conductor or managed device from the other partition.

Pre-requisites

Before you reboot the Mobility Conductor or managed device with the pre-upgrade AOS-W version, perform the following steps:

1. Back up your Mobility Conductor or managed device. For details, see Backing up Critical Data on page 24.

2. Verify that the control plane security is disabled.

3. Set the Mobility Conductor or managed device to boot with the previously saved configuration file.

4. Set the Mobility Conductor 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 Conductor 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 Conductor 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 Conductor 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 Conductor or managed device reboots after the countdown period.

4. When the boot process is complete, verify that the Mobility Conductor 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 Conductor 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 Conductor 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 Conductor or managed device.

```
(host) # reload
```

6. When the boot process is complete, verify that the Mobility Conductor 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.