

AOS-W 8.5.0.6



Copyright Information

Alcatel-Lucent and the Alcatel-Lucent Enterprise logo are trademarks of Alcatel-Lucent. To view other trademarks used by affiliated companies of ALE Holding, visit:

<https://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. (2020)

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	3
Revision History	5
Release Overview	6
Important Points Before Upgrading to AOS-W 8.5.0.0	6
Related Documents	7
Supported Browsers	7
Contacting Support	8
New Features and Enhancements	9
Supported Platforms	10
Mobility Master Platforms	10
OmniAccess Mobility Controller Platforms	10
AP Platforms	11
Regulatory Updates	13
Resolved Issues	14
Known Issues and Limitations	15
Upgrade Procedure	30
Migrating from AOS-W 6.x to AOS-W 8.x	30

Important Points to Remember and Best Practices	30
Memory Requirements	31
Backing up Critical Data	32
Upgrading AOS-W	34
Downgrading AOS-W	36
Before Calling Technical Support	38

Revision History

The following table provides the revision history of this document.

Table 1: *Revision History*

Revision	Change Description
Revision 01	Initial release.

This AOS-W release notes includes the following topics:



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

- [New Features and Enhancements on page 9](#)
- [Supported Platforms on page 10](#)
- [Regulatory Updates on page 13](#)
- [Resolved Issues on page 14](#)
- [Known Issues and Limitations on page 15](#)
- [Upgrade Procedure on page 30](#)

For the list of terms, refer [Glossary](#).

Important Points Before Upgrading to AOS-W 8.5.0.0

DPI classification is not initialized after a switch is upgraded from AOS-W 8.4.0.0, 8.4.0.1, or 8.4.0.2 to AOS-W 8.5.0.0. The affected platforms are OAW-4x50 Series switches.

An additional reboot of the affected platform is required to initialize DPI classification.

To check the status of DPI classification after upgrading an affected platform from AOS-W 8.4.0.0, 8.4.0.1, or 8.4.0.2 to AOS-W, 8.5.0.0, issue the **show firewall | include dpi** command. In the following example, DPI classification is disabled:

```
(host) #show firewall | include dpi
DPI Classification      Disabled [Cfg: enabled, PEF license: installed]
```

If DPI classification is enabled, further action is not needed. However, if DP classification is disabled, issue the **show datapath utilization** and check if the DPI classification CPUs are initialized. In the following example, the DPI classification CPUs are disabled:

```
(host) #show datapath utilization

Datapath CPU Allocation Summary
Slow Path (SP) : 1,   Slow Path Gateway (SPGW) : 1
Fast Path (FP) : 17,  Fast Path Gateway (FPGW) : 1
DPI : 0, Crypto (CRYP) : 0
Slow Path Spare (SPSPARE) : 0
```

If the DPI classification CPUs are not initialized, reboot the affected platform by:

- Issuing the **reload** command.
- Power cycling the switch.

Related Documents

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

- *AOS-W Getting Started Guide*
- *AOS-W User Guide*
- *AOS-W CLI Reference Guide*
- *AOS-W Migration Guide*
- *AOS-W API Guide*
- *Alcatel-Lucent Mobility Master Licensing Guide*
- *Alcatel-Lucent Virtual Appliance Installation Guide*
- *Alcatel-Lucent Mobility Master Hardware Appliance Installation Guide*

Supported Browsers

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

- Microsoft Internet Explorer 11 on Windows 7 and Windows 8
- Microsoft Edge (Microsoft Edge 38.14393.0.0 and Microsoft EdgeHTML 14.14393) on Windows 10
- Mozilla Firefox 58 or later on Windows 7, Windows 8, Windows 10, and macOS
- Apple Safari 9.0 or later on macOS
- Google Chrome 67 or later on Windows 7, Windows 8, Windows 10, and macOS

Contacting Support

Table 2: *Contact Information*

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

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

Default Value of host-ageout-time Parameter

The default value of the Openflow switch's **host-ageout-time** parameter is changed from 300 seconds to 3600 seconds.

Execute the following command to view the value of the **ofc host-ageout-time** parameter:

```
(host) [mynode] #show openflow-controller
```

```
Openflow-controller
-----
Parameter                Value
-----
ofc state                 Enabled
ofc host-ageout-time      3600 sec
ofc mode                  passive
ofc certificate-file      none
ofc key-file              none
ofc ca-certificate-file   none
ofc tls                   Disabled
ofc port                  6633
ofc topology-discovery    Disabled
ofc auxiliary-channel-port 6633
```

This chapter describes the platforms supported in this release.

Mobility Master Platforms

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

Table 3: *Supported Mobility Master Platforms in AOS-W 8.5.0.6*

Mobility Master Family	Mobility Master Model
Hardware Mobility Master	MM-HW-1K, MM-HW-5K, MM-HW-10K
Virtual Mobility Master	MM-VA-50, MM-VA-500, MM-VA-1K, MM-VA-5K, MM-VA-10K

OmniAccess Mobility Controller Platforms

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

Table 4: *Supported OmniAccess Mobility Controller Platforms in AOS-W 8.5.0.6*

OmniAccess Mobility Controller Family	OmniAccess Mobility Controller Model
OAW-40xx Series Hardware OmniAccess Mobility Controllers	OAW-4005, OAW-4008, OAW-4010, OAW-4024, OAW-4030
OAW-4x50 Series Hardware OmniAccess Mobility Controllers	OAW-4450, OAW-4550, OAW-4650, OAW-4750, OAW-4750XM, OAW-4850
OAW-41xx Series Hardware OmniAccess Mobility Controllers	OAW-4104
MC-VA-xxx Virtual OmniAccess Mobility Controllers	MC-VA-50, MC-VA-250, MC-VA-1K

AP Platforms

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

Table 5: *Supported AP Platforms in AOS-W 8.5.0.6*

AP Family	AP Model
OAW-AP100 Series	OAW-AP104, OAW-AP105
OAW-AP103 Series	OAW-AP103
OAW-AP110 Series	OAW-AP114, OAW-AP115
OAW-AP130 Series	OAW-AP134, OAW-AP135
OAW-AP 170 Series	OAW-AP175AC, OAW-AP175AC-F1, OAW-AP175DC, OAW-AP175DC-F1, OAW-AP175P, OAW-AP175P-F1
OAW-AP200 Series	OAW-AP204, OAW-AP205
OAW-AP203H Series	OAW-AP203H
OAW-AP205H Series	OAW-AP205H
OAW-AP207 Series	OAW-AP207
OAW-AP203R Series	OAW-AP203R, OAW-AP203RP
OAW-AP210 Series	OAW-AP214, OAW-AP215
OAW-AP 220 Series	OAW-AP224, OAW-AP225
228 Series	OAW-AP228
OAW-AP270 Series	OAW-AP274, OAW-AP275, OAW-AP277
OAW-AP300 Series	OAW-AP304, OAW-AP305
OAW-AP303 Series	OAW-AP303
OAW-AP303H Series	OAW-AP303H

Table 5: Supported AP Platforms in AOS-W 8.5.0.6

AP Family	AP Model
OAW-AP310 Series	OAW-AP314, OAW-AP315
OAW-AP318 Series	OAW-AP210AP-318
OAW-AP320 Series	OAW-APAP-324, OAW-AP325
OAW-AP330 Series	OAW-AP334, OAW-AP335
OAW-AP340 Series	OAW-AP344, OAW-AP345
OAW-AP360 Series	OAW-AP365, OAW-AP367
OAW-AP370 Series	OAW-AP374, OAW-AP375, OAW-AP377
OAW-AP387	OAW-AP387
OAW-AP510 Series	OAW-AP514, OAW-AP515
OAW-AP530 Series	OAW-AP534, OAW-AP535
OAW-AP550 Series	OAW-AP555
OAW-RAP3 Series	OAW-RAP3WN, OAW-RAP3WNP
OAW-RAP100 Series	OAW-RAP108, OAW-RAP109
OAW-RAP155 Series	OAW-RAP155, OAW-RAP155P

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

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

The following DRT file version is part of this release:

- DRT-1.0_73798

This chapter describes the issues resolved in this release.



We have migrated to a new defect tracking tool. Some bugs are listed with the new bug ID, which is prefixed by AOS.

Table 6: Resolved Issues in AOS-W 8.5.0.6

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-196457	—	Symptom: High radio noise floor was observed in APs. Enhancements to the wireless driver resolved this issue. Scenario: This issue was observed in OAW-AP515 access points running AOS-W 8.5.0.2 or later versions.	AP-Wireless	OAW-AP515 access points	AOS-W 8.5.0.2
AOS-197665	—	Symptom: The SNMP walk for an MIB displayed both IPv4 address and IPv6 address in the user-table entries. The fix ensures that the SNMP walk displays only IPv6 address in the user-table. Scenario: This issue was observed in managed devices running AOS-W 8.3.0.8 or later versions.	Base OS Security	All platforms	AOS-W 8.3.0.8
AOS-198232	—	Symptom: A managed device was unable to forward RADIUS server statistics through SNMP walk. This issue was resolved by combining the RADIUS server statistics of 802.1X and authentication processes. Scenario: This issue was observed in managed devices running AOS-W 8.4.0.0 or later versions.	802.1X	All platforms	AOS-W 8.5.0.5
AOS-198927	—	Symptom: A few clients were unable to pass traffic on APs. Enhancements to the wireless driver resolved this issue. Scenario: This issue was observed in OAW-AP515 access points running AOS-W 8.5.0.3 or later versions.	AP-Wireless	OAW-AP515 access points	AOS-W 8.5.0.3

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



We have migrated to a new defect tracking tool. Some bugs are listed with the new bug ID, which is prefixed by AOS.

Limitation

Zero Touch Provisioning and multi-version support for OAW-4104 switches are currently not supported.



It is recommended to have the Mobility Master and managed device running the same AOS-W version.

Known Issues

Following are the known issues observed in this release.

Table 7: Known Issues in AOS-W 8.5.0.6

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-131325 AOS-146748	159222 179137	<p>Symptom: Incorrect number of clients are displayed in the active-standby IP field under Wireless Clients table on the Dashboard > Overview > Clients page in the WebUI.</p> <p>Scenario: This issue occurs due to a cluster failover causing race condition. This issue is observed in Mobility Masters running AOS-W 8.1.0.0 or later versions.</p> <p>Workaround: None.</p>	Base OS Security	All platforms	AOS-W 8.1.0.0
AOS-145410 AOS-146962	177352 179430	<p>Symptom: A managed device crashes and reboots with the following error message: Atleast 2000 MB free flash is recommended to keep system stable. Please clean up your flash file.</p> <p>Scenario: This issue occurs when a managed device receives IP packets larger than one segment. This issue is observed in managed devices running AOS-W 8.2.0.2 or later versions.</p> <p>Workaround: None.</p>	switch-Platform	All platforms	AOS-W 8.2.0.2
AOS-145566	177559	<p>Symptom: A Mobility Master is unable to forward the traffic that is sourced from an IP interface in the gateway.</p> <p>Scenario: This issue occurs when netdestinations are used in the routing ACL rule. This issue is observed in Mobility Masters running AOS-W 8.0.1.0 or later versions.</p> <p>Workaround: None.</p>	Policy-Based Routing	All platforms	AOS-W 8.0.1.0
AOS-151022 AOS-188417	185176	<p>Symptom: The output of the show datapath uplink command displays incorrect session count.</p> <p>Scenario: This issue is observed in managed devices running AOS-W 8.1.0.0 or later versions.</p> <p>Workaround: None.</p>	switch-Datapath	All platforms	AOS-W 8.1.0.0
AOS-151355	185602	<p>Symptom: A few managed devices are unable to pass traffic to the nexthop VPN concentrator (VPNC) using policy-based routing.</p> <p>Scenario: This issue is observed in managed devices running AOS-W 8.0.1.0 or later versions.</p> <p>Workaround: None.</p>	Policy-Based Routing	All platforms	AOS-W 8.0.1.0

Table 7: Known Issues in AOS-W 8.5.0.6

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-153185	188148	<p>Symptom: The Dashboard > Security > Active rogue > Locate option in the WebUI does not function.</p> <p>Scenario: This issue is observed in Mobility Masters running AOS-W 8.3.0.1 or later versions.</p> <p>Workaround: None.</p>	WebUI	All platforms	AOS-W 8.3.0.1
AOS-155037	190571	<p>Symptom: A OAW-RAP fails to boot up.</p> <p>Scenario: This issue occurs in a OAW-RAP with EST key type X9.62/SECG curve. This issue is observed in OAW-AP303H access points running AOS-W 8.3.0.3 or later versions.</p> <p>Workaround: None.</p>	CPsec	OAW-AP303H access points	AOS-W 8.3.0.3
AOS-155801	191726	<p>Symptom: The SNMP walk performed from OmniVista 3600 Air Manager does not produce correct results.</p> <p>Scenario: This issue is observed in managed devices running AOS-W 8.3.0.3.</p> <p>Workaround: None.</p>	SNMP	All platforms	AOS-W 8.3.0.3
AOS-156085 AOS-157704	192119 194393	<p>Symptom: A few managed devices are unable to obtain the switch-IP address during boot up after an upgrade.</p> <p>Scenario: This issue is observed in managed devices running AOS-W 8.1.0.0 or later versions.</p> <p>Workaround: None.</p>	Configuration	All platforms	AOS-W 8.1.0.0
AOS-156742 AOS-156977	193031 193319	<p>Symptom: After pushing a complete configuration via API, the user is unable to make any change to IP Probe configuration.</p> <p>Scenario: This issue is observed in managed devices running AOS-W 8.0.1.0.</p> <p>Workaround: None.</p>	Configuration	All platforms	AOS-W 8.0.1.0
AOS-157492	194064	<p>Symptom: VRRP authentication fails in a managed device.</p> <p>Scenario: This issue is observed in managed devices running AOS-W 8.2.1.0.</p> <p>Workaround: None.</p>	VRRP	All platforms	AOS-W 8.2.1.0

Table 7: Known Issues in AOS-W 8.5.0.6

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-157795	194516	<p>Symptom: A few managed devices are unable to process two APN usb-init strings using the uplink cellular apn command with Huawei E3372 modem.</p> <p>Scenario: This issue is observed in managed devices running AOS-W 8.3.0.0 or later versions.</p> <p>Workaround: None.</p>	switch-Platform	All platforms	AOS-W 8.3.0.6
AOS-182073 AOS-183743	—	<p>Symptom: An AP crashes and reboots unexpectedly. The log files lists the reason for the event as Reboot caused by kernel panic: Rebooting the AP because of FW ASSERT.</p> <p>Scenario: This issue is observed in OAW-AP315 access points running AOS-W 8.3.0.5.</p> <p>Workaround: None.</p>	IPsec	OAW-AP315 access points	AOS-W 8.3.0.5
AOS-183669 AOS-190457 AOS-192089 AOS-194012	—	<p>Symptom: The system LED blinks with a green light after a OAW-RAP connects to the managed device and boots up.</p> <p>Scenario: This issue is observed in OAW-RAPs running AOS-W 8.5.0.0 or later versions.</p> <p>Workaround: None.</p>	Air Management - IDS	All platforms	AOS-W 8.4.0.0
AOS-183998 AOS-183999	—	<p>Symptom: A few users are unable to configure the PPPoE password when they provision a OAW-RAP in the Configuration > Access Points > Remote APs page of the WebUI.</p> <p>Scenario: This issue occurs because the Retype password field for PPPoE is missing from the Uplink option in the provisioning page of the WebUI. This issue is observed in OAW-RAPs running AOS-W 8.2.2.0 or later versions.</p> <p>Workaround: None.</p>	WebUI	All platforms	AOS-W 8.3.0.6
AOS-184135	—	<p>Symptom: A few users are unable to download applications from Google Play Store.</p> <p>Scenario: This issue occurs when the YouTube application is blocked. This issue is observed in stand-alone switches running AOS-W 8.4.0.0 or later versions.</p> <p>Workaround: None.</p>	switch-Datapath	All platforms	AOS-W 8.4.0.0

Table 7: Known Issues in AOS-W 8.5.0.6

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-184801	—	<p>Symptom: A few managed devices crash and reboot unexpectedly. The log files list the reason for the event as Datapath exception.</p> <p>Scenario: This issue is observed in managed devices running AOS-W 8.4.0.0.</p> <p>Workaround: None.</p>	switch -Datapath	All platforms	AOS-W 8.4.0.0
AOS-184977 AOS-188242 AOS-188378	—	<p>Symptom: The output of basic commands such as show version, show clock, and show image version are unable to display any information and the default gateway details are missing in a managed device.</p> <p>Scenario: This issue occurs when the /tmp directory runs out of memory because of too many logs from the Policy Manager. This issue is observed in managed devices running AOS-W 8.4.0.0 or later versions.</p> <p>Workaround: None.</p>	Routing	All platforms	AOS-W 8.4.0.0
AOS-186133	—	<p>Symptom: A few managed devices display abnormally high multicast traffic in Performance Summary > All Radios monitoring page.</p> <p>Scenario: This issue is observed in OAW-AP320 Series access points running AOS-W 8.3.0.6.</p> <p>Workaround: None.</p>	AP-Wireless	OAW-AP320 Series access points	AOS-W 8.3.0.6
AOS-186411	—	<p>Symptom: A few users are unable to remove a VLAN from port channel trunk.</p> <p>Scenario: This issue is observed in Mobility Masters running AOS-W 8.3.0.0 or later versions.</p> <p>Workaround: Execute the switchport trunk allowed vlan 1-4094 command to add the allowed VLAN range (1-4094). Then, execute the switchport trunk allowed vlan remove 259 command to remove the VLAN from the port channel trunk.</p>	Interface	All platforms	AOS-W 8.3.0.0
AOS-186774	—	<p>Symptom: When the show memory cfm command is executed, a large memory allocation is displayed in the output of the command.</p> <p>Scenario: This issue is observed in managed devices running AOS-W 8.3.0.0 or later versions.</p> <p>Workaround: None.</p>	Configuration	All platforms	AOS-W 8.3.0.6

Table 7: Known Issues in AOS-W 8.5.0.6

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-186860	—	<p>Symptom: RADIUS authentication requests are sent in IP address of the managed device though they are configured to go through the loopback IP address.</p> <p>Scenario: This issue is observed in managed devices running AOS-W 8.4.0.0 or later versions.</p> <p>Workaround: None.</p>	IPsec	All platforms	AOS-W 8.4.0.1
AOS-187268 AOS-196356	—	<p>Symptom: A few APs crash and reboot unexpectedly. The log files list the reason for the event as Reboot caused by kernel panic: Fatal exception.</p> <p>Scenario: This issue occurs when 802.11w standard is enabled in the APs. This issue is observed in APs running AOS-W 8.3.0.0 or later versions.</p> <p>Workaround: None.</p>	AP-Wireless	All platforms	AOS-W 8.3.0.0
AOS-187422 AOS-189258	—	<p>Symptom: The output of show log all and show audit-trail commands displays the unencrypted password entered for non-profile commands such as aaa test-server command.</p> <p>Scenario: This issue is observed in a Mobility Master Virtual Appliance running AOS-W 8.3.0.5.</p> <p>Workaround: None.</p>	Configuration	All platforms	AOS-W 8.3.0.5
AOS-187479 AOS-188428	—	<p>Symptom: The authentication server configuration details are not forwarded from the primary Mobility Master to the secondary Mobility Master in Layer-3 redundancy configuration.</p> <p>Scenario: This issue is observed in a Mobility Master Virtual Appliance running AOS-W 8.4.0.0 or later versions.</p> <p>Workaround: None.</p>	Configuration	All platforms	AOS-W 8.4.0.2
AOS-187820	—	<p>Symptom: The output of the show cpuload per-cpu command displays the same CPU load statistics for each processor.</p> <p>Scenario: This issue occurs after a switch reboot. This issue is observed in managed devices running AOS-W 8.4.0.0 or later versions.</p> <p>Workaround: None.</p>	switch-Platform	All platforms	AOS-W 8.4.0.0

Table 7: Known Issues in AOS-W 8.5.0.6

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-187834	—	<p>Symptom: A few APs do not send Port VLAN IDs in an LLDP packet although the native-vlan-id parameter is set using the ap system-profile command.</p> <p>Scenario: This issue is observed in APs running AOS-W 8.2.2.0 or later versions.</p> <p>Workaround: None.</p>	AP-Platform	All platforms	AOS-W 8.2.2.5
AOS-187911	—	<p>Symptom: The Wireless Clients section of the Dashboard > Overview page in the WebUI displays incorrect client usage values.</p> <p>Scenario: This issue is observed in Mobility Masters running AOS-W 8.4.0.0 or later versions.</p> <p>Workaround: Add a tooltip over the usage tab to mention that the current client usage value accounts for the last 15 min.</p>	WebUI	All platforms	AOS-W 8.4.0.0
AOS-188002 AOS-195453	—	<p>Symptom: The OFA process crashes in a managed device unexpectedly.</p> <p>Scenario: This issue occurs due to a memory leak. This issue is observed in managed devices running AOS-W 8.2.2.0 or later versions.</p> <p>Workaround: None.</p>	SDN	All platforms	AOS-W 8.4.0.3
AOS-188285	—	<p>Symptom: A mesh portal reboots continuously because the wpa_hex_key value exceeds more than 132 bytes string in the ap mesh-recovery-profile cluster <cluster_id> wpa-hexkey <wpa_hex_key> command. The log files list the reason for the event as AP rebooted Tue Jun 11 10:40:01 CDT 2019; Critical process /aruba/bin/meshd [pid 2450] DIED, process marked as RESTART.</p> <p>Scenario: This issue is observed in APs running AOS-W 8.3.0.7 as a mesh portal.</p> <p>Workaround:</p> <ul style="list-style-type: none"> ■ Modify mesh-recovery-profile by using mesh-recovery-generate command. ■ Reboot the mesh portal and issue the setenv mesh_role 0 command on apboot in the console port of the AP. ■ Reprovision the AP to mesh portal. 	Mesh	All platforms	AOS-W 8.3.0.7
AOS-188467	—	<p>Symptom: The AMON messages from a peer cluster display wrong value for cl_cluster_incompatible_reason.</p> <p>Scenario: This issue occurs when the incompatible reason is not reset after an incompatibility with a peer cluster member is resolved and the cluster is re-formed. This issue is observed in managed devices running AOS-W 8.3.0.6 in a cluster topology.</p> <p>Workaround: None.</p>	Cluster-Manager	All platforms	AOS-W 8.3.0.6

Table 7: Known Issues in AOS-W 8.5.0.6

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-188478	—	<p>Symptom: The OAW-RAP whitelist file does not contain the first MAC address entry.</p> <p>Scenario: This issue occurs when the user executes the show whitelist-db rap export-css <filename> command to export the OAW-RAP whitelist file to the switch directory. This issue is observed in stand-alone switches running AOS-W 8.3.0.5 or later versions.</p> <p>Workaround: None.</p>	Local Database	All platforms	AOS-W 8.3.0.5
AOS-188485 AOS-193638	—	<p>Symptom: The <ofald 237504> <ERRS> AP 32438@172.16.4.151 ofald sdn ERRS ofald_datapath_msg_rcv_cb:274 Invalid message type 126 error message is displayed every second in APs.</p> <p>Scenario: This issue is observed in APs running AOS-W 8.4.0.0-FIPS in a Mobility Master-Managed Device topology.</p> <p>Workaround: None.</p>	SDN	All platforms	AOS-W 8.4.0.0
AOS-188490 AOS-189847 AOS-192747 AOS-197045	—	<p>Symptom: A Mobility Master crashes and reboots unexpectedly. The log file lists the reason for the event as Datapath timeout (SOS Assert) (Intent:cause:register 54:86:0:20).</p> <p>Scenario: This issue is observed in Mobility Masters running AOS-W 8.3.0.0 or later versions.</p> <p>Workaround: None.</p>	switch-Datapath	All platforms	AOS-W 8.3.0.0
AOS-188897	—	<p>Symptom: An AP crashes unexpectedly. The log files list the reason for the event as Internal error: Oops: 96000004 [#1] SMP.</p> <p>Scenario: This issue is observed in APs running AOS-W 8.3.0.6 or later versions.</p> <p>Workaround: None.</p>	AP-Wireless	All platforms	AOS-W 8.3.0.6
AOS-189194	—	<p>Symptom: The 5 GHz and 2.4 GHz antenna values are swapped after AP provisioning rules configuration is committed in the Configuration > Access Points > Provisioning Rules page of the WebUI.</p> <p>Scenario: This issue occurs when the user selects the Set Antenna Gain for Dual Band mode option from the Actions drop-down list in the Configuration > Access Points > Provisioning Rules page, and enters the 5 GHz and 2.4 GHz field values in the WebUI. This issue is observed in Mobility Master Virtual Appliances running AOS-W 8.4.0.3 or later versions.</p> <p>Workaround: None.</p>	WebUI	All platforms	AOS-W 8.5.0.0

Table 7: Known Issues in AOS-W 8.5.0.6

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-189913 AOS-193777	—	<p>Symptom: A stand-alone switch fails to establish communication with the Activate server during ZTP.</p> <p>Scenario: This issue occurs when the database synchronization fails between stand-alone switches in L2 redundancy. As a result, the output of the show database synchronize command displays the Standby switch did not acknowledge the WMS database restore request message. This issue is observed in OAW-4850 switches running AOS-W 8.5.0.0 or later versions.</p> <p>Workaround: None.</p>	switch-Platform	OAW-4850 switches	AOS-W 8.5.0.2
AOS-189977	—	<p>Symptom: A managed device crashes and reboots unexpectedly. The log file lists the reason for the event as Reboot Cause: Datapath timeout (Fpapps Initiated) (Intent:cause:register 51:86:50:2).</p> <p>Scenario: This issue is observed in managed devices running AOS-W 8.3.0.0 or later versions.</p> <p>Workaround: None.</p>	switch-Datapath	All platforms	AOS-W 8.3.0.7
AOS-190071 AOS-190372	—	<p>Symptom: A few users are unable to access the websites when WebCC is enabled on the user role.</p> <p>Scenario: This issue occurs in a Per User Tunnel Node (PUTN) setup when the VLAN of user role is in trunk mode. This issue is observed in OAW-4005 switches running AOS-W 8.4.0.0.</p> <p>Workaround:</p> <ul style="list-style-type: none"> ■ Remove web category from the ACL rules and apply any any any permit policy. ■ Disable WebCC on the user role. ■ Change the VLAN of user role from trunk mode to access mode. 	WebCC	OAW-4005 switches	AOS-W 8.4.0.0
AOS-190230 AOS-194760	—	<p>Symptom: A few OAW-RAPs fail to come up on the managed device after reboot of the APs, and get the same inner IP address which has already been assigned to other OAW-RAPs.</p> <p>Scenario: This issue occurs because most of the OAW-RAP whitelist database entries are removed from the Mobility Master. This issue is observed in APs running AOS-W 8.4.0.0 or later versions.</p> <p>Workaround: Purge the OAW-RAP whitelist database entries on the Mobility Master and managed device, and add them again.</p>	CPsec	All platforms	AOS-W 8.4.0.0
AOS-190240 AOS-192168	—	<p>Symptom: The SNMP OIDs provide incorrect result in a cluster setup.</p> <p>Scenario: This issue is observed in managed devices running AOS-W 8.3.0.0 or later versions.</p> <p>Workaround: None.</p>	SNMP	All platforms	AOS-W 8.3.0.0

Table 7: Known Issues in AOS-W 8.5.0.6

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-190380 AOS-196361	—	<p>Symptom: A few users are unable to connect to VIA server from the guest account.</p> <p>Scenario: This issue occurs because PBR is not applied to data packets from UDP 4500 port. As a result, the client traffic is not forwarded correctly. This issue is observed in managed devices running AOS-W 8.0.0.0 or later versions.</p> <p>Workaround: None.</p>	switch-Datapath	All platforms	AOS-W 8.0.1.0
AOS-190836	—	<p>Symptom: The output of the show interface gigabitethernet 0/0/0 transceiver command displays the Error reading Transceiver ID Prom on 0/0/0 message when the Small Form-factor Pluggable transceiver (SFP module) is connected to the Mobility Master.</p> <p>Scenario: This issue is observed in Mobility Masters running AOS-W 8.5.0.0 or later versions.</p> <p>Workaround: None.</p>	switch-Platform	All platforms	AOS-W 8.5.0.1
AOS-191317 AOS-194342	—	<p>Symptom: A few High Efficiency 802.11ax Intel clients are unable to pass traffic.</p> <p>Scenario: This issue occurs when the clients are configured with OFDMA and Medium Power Save mode, which results in delay or packet drop to other clients. This issue is observed in OAW-AP510 Series access points running AOS-W 8.5.0.6 or later versions.</p> <p>Workaround:</p> <ul style="list-style-type: none"> ■ Issue the wlan he-ssid-profile command to disable MU-OFDMA in HE-SSID profile . ■ Move the client in wireless adaptor in Maximum Performance mode. 	AP-Wireless	OAW-AP510 Series access points	AOS-W 8.6.0.0
AOS-191539	—	<p>Symptom: The configuration synchronization fails and the status of the synchronization displays as CONFIG Failure in a managed device. The log files list the Error: Tunnel is an L2 GRE Tunnel, Delete the Vlans, before changing the mode." executing "tunnel mode gre 2048 error message.</p> <p>Scenario: This issue occurs when tunnel number 2048 is set for the interface tunnel. This issue is observed in managed devices running AOS-W 8.4.0.0 or later versions in a Mobility Master-Managed Device topology.</p> <p>Workaround: None.</p>	Interface	All platforms	AOS-W 8.4.0.1

Table 7: Known Issues in AOS-W 8.5.0.6

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-191565	—	<p>Symptom: A Mobility Master Virtual Appliance displays high memory utilization.</p> <p>Scenario: This issue is observed in Mobility Master Virtual Appliances running AOS-W 8.4.0.0 or later versions.</p> <p>Workaround: None.</p>	Firewall Visibility	All platforms	AOS-W 8.4.0.0
AOS-191579 AOS-195733	—	<p>Symptom: A few users are unable to connect to the wireless network.</p> <p>Scenario: This issue occurs when the authentication process crashes unexpectedly in a managed device. This issue is observed in managed devices running AOS-W 8.3.0.0 or later versions.</p> <p>Workaround: None.</p>	Base OS Security	All platforms	AOS-W 8.3.0.0
AOS-191820	—	<p>Symptom: The output of the show datapath dns-cache counter command does not display any information.</p> <p>Scenario: This issue is observed in managed devices running AOS-W 8.5.0.1 or later versions.</p> <p>Workaround: None.</p>	switch-Datapath	All platforms	AOS-W 8.5.0.1
AOS-192568 AOS-192736	—	<p>Symptom: A few clients are unable to connect to APs even though High Efficiency was disabled on all the SSID profiles of the APs.</p> <p>Scenario: This issue is observed in OAW-AP515 access points running AOS-W 8.5.0.0 or later versions.</p> <p>Workaround: None.</p>	DDS	OAW-AP515 access points	AOS-W 8.5.0.1
AOS-192841	—	<p>Symptom: The STM process crashes on a managed device and the APs are unable to communicate with the managed device.</p> <p>Scenario: This issue is observed in managed devices running AOS-W 8.3.0.1 or later versions.</p> <p>Workaround: None.</p>	AP-Platform	All platforms	AOS-W 8.0.0.0
AOS-193083	—	<p>Symptom: The cluster upgrade fails on a 2 node cluster because the AP platform capacity of the managed device is only 4 and the hash table size is calculated as zero.</p> <p>Scenario: This issue is observed in Mobility Controller Virtual Appliances running AOS-W 8.5.0.0 or later versions.</p> <p>Workaround: None.</p>	Cluster-Manager	All platforms	AOS-W 8.5.0.0

Table 7: Known Issues in AOS-W 8.5.0.6

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-193188	—	<p>Symptom: The Reclassify Detected Radios pop-up window displays action commands for a specific SSID in the Dashboard > Security > Detected Radios page of the WebUI.</p> <p>Scenario: This issue occurs when apostrophe and quotation are added to the ESSID of a stand-alone switch. This issue is observed in OAW-4550 switches running AOS-W 8.4.0.0 or later versions.</p> <p>Workaround: None.</p>	WebUI	OAW-4550 switches	AOS-W 8.5.0.1
AOS-193775 AOS-194581	—	<p>Symptom: A mismatch of AP count and client count is observed between the Mobility Master and the managed device.</p> <p>Scenario: This issue is observed in Mobility Masters running AOS-W 8.3.0.0 or later versions.</p> <p>Workaround: None.</p>	Monitoring	All platforms	AOS-W 8.5.0.2
AOS-194052	—	<p>Symptom: A few clients are unable to obtain IP addresses.</p> <p>Scenario: This issue occurs when High Efficiency is enabled on the WPA2-PSK SSID profile of the APs. This issue is observed in Mobility Controller Virtual Appliances running AOS-W 8.5.0.0 or later versions.</p> <p>Workaround: Disable High Efficiency on the WPA2-PSK SSID profile of the APs.</p>	switch-Platform	All platforms	AOS-W 8.5.0.2
AOS-194146	—	<p>Symptom: A managed device does not display any warning message when the cluster profile name contains more than 32 characters.</p> <p>Scenario: This issue is observed in managed devices running AOS-W 8.5.0.2 or later versions in a cluster setup.</p> <p>Workaround: None.</p>	Cluster-Manager	All platforms	AOS-W 8.5.0.2
AOS-194325 AOS-194579	—	<p>Symptom: The datapath process in a managed device crashes multiple times.</p> <p>Scenario: This issue is observed in managed devices running AOS-W 8.3.0.0 or later versions in a Mobility Master-Managed Device topology.</p> <p>Workaround: None.</p>	switch-Datapath	All platforms	AOS-W 8.3.0.7
AOS-194370	—	<p>Symptom: High memory utilization is observed in the cluster manager process of managed devices.</p> <p>Scenario: This issue is observed in managed devices running AOS-W 8.4.0.2 or later versions in a cluster setup.</p> <p>Workaround: None.</p>	Cluster-Manager	All platforms	AOS-W 8.4.0.2

Table 7: Known Issues in AOS-W 8.5.0.6

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-194390	—	<p>Symptom: The SAPD process crashes in a managed device unexpectedly. The log files lists the reason for this event as RF Client failed: No such file or directory Message Code 1005 Sequence Num is 18119 Aug 29 10:35:21 sapd[2905]: RF Client failed: No such file or directory Message Code 1003 Sequence Num is 18112.</p> <p>Scenario: This issue is observed in managed devices running AOS-W 8.3.0.0 or later versions.</p> <p>Workaround: None.</p>	AP-Platform	All platforms	AOS-W 8.3.0.8
AOS-194706	—	<p>Symptom: A managed device crashes and reboots unexpectedly. The log files list the reason for the event as Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:4).</p> <p>Scenario: This issue is observed in managed devices running AOS-W 8.3.0.7 or later versions in a Mobility Master-Managed Device topology.</p> <p>Workaround: None.</p>	switch-Datapath	All platforms	AOS-W 8.5.0.2
AOS-194727	—	<p>Symptom: An AP sends RTS requests continuously to one client only and this results in delay or packet drop to other clients.</p> <p>Scenario: This issue is observed in OAW-AP340 Series access points running AOS-W 8.3.0.7 or later versions.</p> <p>Workaround: None.</p>	AP-Wireless	OAW-AP340 Series access points	AOS-W 8.3.0.7
AOS-194925 AOS-195413	—	<p>Symptom: A Branch office managed device is unable to failover to a secondary VPNC managed device.</p> <p>Scenario: This issue occurs because the secondary VPNC's MAC address is not updated on the running configuration of the managed device. This issue is observed in Mobility Master Virtual Appliances and Branch office managed devices running AOS-W 8.5.0.2 or later versions.</p> <p>Workaround: None.</p>	Configuration	All platforms	AOS-W 8.5.0.2
AOS-194964	—	<p>Symptom: A few users are unable to clone the configuration from an existing group to a new group in a Mobility Master.</p> <p>Scenario: This issue is observed in Mobility Masters running AOS-W 8.4.0.1 or later versions.</p> <p>Workaround: Execute the rf dot11a-radio-profile <profile name> command to change the operating mode of the AP from am-mode to ap-mode.</p>	Configuration	All platforms	AOS-W 8.5.0.2

Table 7: Known Issues in AOS-W 8.5.0.6

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-195000	—	Symptom: A few APs crash unexpectedly. The log files list the reason for the event as Kernel panic: softlockup - hung tasks . Scenario: This issue is observed in OAW-AP515 access points running AOS-W 8.5.0.1 or later versions. Workaround: None.	AP-Wireless	OAW-AP515 access points	AOS-W 8.5.0.1
AOS-195036	—	Symptom: The authentication process in a managed device crashes unexpectedly. Scenario: This issue is observed in managed devices running AOS-W 8.3.0.0 or later versions. Workaround: None.	802.1X	All platforms	AOS-W 8.3.0.6
AOS-195162	—	Symptom: The WebUI is unresponsive and the licenses are not visible in the Mobility Master > Configuration > Licenses page in the WebUI. Scenario: This issue occurs when 29 non-default pools are configured and enabled. This issue is observed in Mobility Masters running AOS-W 8.5.0.1 or later versions. Workaround: None.	Licensing	All platforms	AOS-W 8.5.0.1
AOS-195228	—	Symptom: The device status is always displayed as inactive when SNMP walk is performed. Scenario: This issue is observed in stand-alone switches running AOS-W 8.5.0.2 or later versions. Workaround: None.	SNMP	All platforms	AOS-W 8.5.0.2
AOS-195265	—	Symptom: A managed device crashes and reboots unexpectedly. The log files list the reason for the event as Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2) . Scenario: This issue occurs due to ACL corruption. This issue is observed in managed devices running AOS-W 8.5.0.0 or later versions. Workaround: None.	SDN	All platforms	AOS-W 8.5.0.3

Table 7: *Known Issues in AOS-W 8.5.0.6*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-195434	—	<p>Symptom: An AP crashes and reboots unexpectedly. The log files list the reason for the event as Reboot caused by kernel panic: Fatal exception.</p> <p>Scenario: This issue is observed in APs running AOS-W 8.5.0.0 o or later versions in a Mobility Master-Managed Device topology.</p> <p>Workaround: None.</p>	AP-Wireless	All platforms	AOS-W 8.5.0.2
AOS-195677 AOS-196311	—	<p>Symptom: The airmatch_recv process crashes unexpectedly in a Mobility Master.</p> <p>Scenario: This issue is observed in Mobility Masters running AOS-W 8.3.0.0 or later versions in a Mobility Master-Managed Device topology.</p> <p>Workaround: None.</p>	AirMatch	All platforms	AOS-W 8.3.0.7
AOS-196729	—	<p>Symptom: An AP crashes and reboots unexpectedly. The log files list the reason for the event as Unable to set up IPsec tunnel, Error:RC_ERROR_IKEV2_TIMEOUT.</p> <p>Scenario: This issue is observed in OAW-AP340 Series access points running AOS-W 8.5.0.3 or later versions.</p> <p>Workaround: None.</p>	AP-Wireless	OAW-AP340 Series access points	AOS-W 8.5.0.3

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



CAUTION

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

Topics in this chapter include:

- [Migrating from AOS-W 6.x to AOS-W 8.x on page 30](#)
- [Important Points to Remember and Best Practices on page 30](#)
- [Memory Requirements on page 31](#)
- [Backing up Critical Data on page 32](#)
- [Upgrading AOS-W on page 34](#)
- [Downgrading AOS-W on page 36](#)
- [Before Calling Technical Support on page 38](#)

Migrating from AOS-W 6.x to AOS-W 8.x

Use the interactive migration tool provided on the customer support site to migrate any AOS-W 6.x deployments to one of the following AOS-W 8.x deployments:

- Master-Local setup to Mobility Master
- All-Master setup to Mobility Master
- Master-Local setup to Master switch Mode in AOS-W 8.x
- Stand-alone switch running AOS-W 8.x

For more information, refer to the *AOS-W 8.x Migration Guide*.



Licenses are not migrated by the migration tool from any of the devices to Mobility Master. However, the licenses are preserved when migrating to AOS-W 8.x Master switch Mode or stand-alone switches. For more information on License migration, refer to *Alcatel-Lucent Mobility Master Licensing Guide*.

Important Points to Remember and Best Practices

To upgrade your managed device or Mobility Master:

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

Memory Requirements

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

- Do not proceed with an upgrade unless 100 MB of free memory is available. Execute the **show memory** command to identify the available free memory. To recover memory, reboot the managed device. After the managed device comes up, upgrade immediately.
- Do not proceed with an upgrade unless 150 MB of flash space is available. Execute the **show storage** command to identify the available flash space. If the output of the **show storage** command indicates that there is insufficient flash memory, free some used memory. Copy any log files, crash data, or flash backups from your managed device to a desired location. Delete the following files from the managed device to free some memory:
 - **Crash data:** Execute the **tar crash** command to compress crash files to a file named **crash.tar**. Use the procedures described in [Backing up Critical Data on page 32](#) 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 32](#) to back up the flash directory to a file named **flash.tar.gz**. Execute the **tar clean flash** command to delete the file from the managed device.
- **Log file:** Execute the **tar logs** command to compress log files to a file named **logs.tar**. Use the procedures described in [Backing up Critical Data on page 32](#) to copy the **logs.tar** files to an external server. Execute the **tar clean logs** command to delete the file from the managed device.



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

Deleting a File

You can delete a file using the WebUI or the CLI.

In the WebUI

From the Mobility Master, navigate to **Diagnostic > Technical Support > Delete Files** and remove any aging log files or redundant backups.

In the CLI

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

Backing up Critical Data

It is important to frequently back up all critical configuration data and files on the flash memory to an external server or mass storage device. You should include the following files in these frequent backups:

- Configuration data
- WMS database
- Local user database
- Licensing database
- Custom captive portal pages
- x.509 certificates
- Logs
- Flashbackup

Backing up and Restoring Flash Memory

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

In the WebUI

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

1. In the Mobility Master node hierarchy, navigate to the **Maintenance > Configuration Management > Backup** page.
2. Click **Create Backup** to backup the contents of the flash memory to the **flashbackup.tar.gz** file.
3. Click **Copy Backup** to copy the file to an external server.
You can copy the backup file from the external server to the flash memory using the file utility in the **Diagnostics > Technical Support > Copy Files** page.
4. To restore the backup file to the Compact Flash file system, navigate to the **Maintenance > Configuration Management > Restore** page and click **Restore**.

In the CLI

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

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

```
(host) #write memory
```
2. Execute the following command to back up the contents of the flash memory to the **flashbackup.tar.gz** file.

```
(host) #backup flash
Please wait while we take the flash backup.....
File flashbackup.tar.gz created successfully on flash.
Please copy it out of the controller and delete it when done.
```
3. Execute the following command to transfer the flash backup file to an external server or storage device.

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

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

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

- ```
(host) #copy tftp: <tftphost> <filename> flash: flashbackup.tar.gz
(host) #copy usb: partition <partition-number> <filename> flash: flashbackup.tar.gz
```
4. Execute the following command to untar and extract the **flashbackup.tar.gz** file to the compact flash file system.  

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

## Upgrading AOS-W

Upgrade AOS-W using the WebUI or CLI.



CAUTION

---

Ensure that there is enough free memory and flash space on your Mobility Master or managed device. For details, see [Memory Requirements on page 31](#).

---



NOTE

---

When you navigate to the **Configuration** tab in the WebUI, the managed device might display the **Error getting information: command is not supported on this platform** message. This message occurs when you upgrade using the WebUI and navigate to the **Configuration** tab after the managed device reboots. This message disappears after clearing the Web browser cache.

---

### In the WebUI

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

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



NOTE

---

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

---

4. Log in to the AOS-W WebUI from the Mobility Master.
5. Navigate to the **Maintenance > Software Management > Upgrade** page.
  - a. Select the **Local File** from the **Upgrade using** drop-down list.
  - b. Click **Browse** from **Image file name** to navigate to the saved image file on your PC or workstation.
6. Select the downloaded image file.
7. Choose the partition from the **Partition to Upgrade** option.
8. Enable the **Reboot Controller After Upgrade** toggle switch to automatically reboot after upgrading. If you do not want to reboot immediately, disable this option.



NOTE

---

The upgrade does not take effect until reboot. If you chose to reboot after upgrade, the Mobility Master or managed device reboots automatically.

---

9. Select **Save Current Configuration**.

10. Click **Upgrade**.
11. Click **OK** when the **Changes were written to flash successfully** message is displayed.

## In the CLI

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

1. Download AOS-W image from the customer support site.
2. Open an SSH session to your Mobility Master.
3. Execute the **ping** command to verify the network connection between the Mobility Master and the SCP server, FTP server, or TFTP server.  

```
(host)# ping <ftphost>
```

or

```
(host)# ping <tftphost>
```

or

```
(host)# ping <scphost>
```
4. Execute the **show image version** command to check if the AOS-W image is loaded on the flash partitions. The partition number appears in the **Partition** row; **0:0** is partition 0, and **0:1** is partition 1. The active boot partition is marked as **Default boot**.  

```
(host) #show image version
```
5. Execute the **copy** command to load the new image to the non-boot partition.  

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

or

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

or

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

or

```
(host)# copy usb: partition <partition-number> <image filename> system: partition <0|1>
```
6. Execute the **show image version** command to verify that the new image is loaded.  

```
(host)# show image version
```
7. Reboot the Mobility Master.  

```
(host)# reload
```

## Verifying the AOS-W Upgrade

Verify the upgrade using the WebUI or CLI.

### In the WebUI

Log in to the WebUI and navigate to the **Dashboard > WLANs** page to verify the AOS-W image version.

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

1. Log in to the WebUI to verify if all the managed devices are up after the reboot.
2. Navigate to the **Dashboard > Access Points** page to determine if your APs are up and ready to accept clients.
3. Verify that the number of access points and clients are as expected.
4. Test a different type of client in different locations, for each access method used.
5. Complete a backup of all critical configuration data and files on the flash memory to an external server or mass storage facility. See [Memory Requirements on page 31](#) for information on creating a backup.

### In the CLI

Execute the **show version** command to verify the AOS-W image version. The following steps describe how to verify that the Mobility Master is functioning as expected:

1. Log in to the CLI to verify that all your managed devices are up after the reboot.
2. Execute the **show ap active** command to determine if your APs are up and ready to accept clients.
3. Execute the **show ap database** command to verify that the number of APs and clients are as expected.
4. Test a different type of client in different locations, for each access method used.
5. Complete a backup of all critical configuration data and files on the flash memory to an external server or mass storage facility. See [Backing up Critical Data on page 32](#) for information on creating a backup.

## Downgrading AOS-W

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

### Pre-requisites

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

1. Back up your Mobility Master or managed device. For details, see [Backing up Critical Data on page 32](#).
2. Verify that the control plane security is disabled.
3. Set the Mobility Master or managed device to boot with the previously saved AOS-W configuration file.
4. Set the Mobility Master or managed device to boot from the system partition that contains the pre-upgrade AOS-W version.  
When you specify a boot partition or copy an image file to a system partition, Mobility Master or managed device checks if the AOS-W version is compatible with the configuration file. An error message is displayed if the boot parameters are incompatible with the AOS-W version and configuration files.
5. After switching the boot partition, perform the following steps:
  - Restore pre-upgrade flash backup from the file stored on the Mobility Master or managed device. Do not restore the AOS-W flash backup file.

- Do not import the WMS database.
- If the RF plan was changed before switching the boot partition, the changed RF plan does not appear in the downgraded AOS-W version.
- If any new certificates were added in the upgraded AOS-W version, reinstall these certificates in the downgraded AOS-W version.

Downgrade AOS-W version using the WebUI or CLI.

## In the WebUI

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

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




---

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

---

- a. Enter the FTP or TFTP server address and image file name.
  - b. Select the backup system partition.
  - c. Enable **Reboot controller after upgrade**.
  - d. Click **Upgrade**.
3. Navigate to the **Maintenance > Software Management > Reboot** page. Select **Save configuration before reboot** option and click **Reboot**. The Mobility Master or managed device reboots after the countdown period.
  4. When the boot process is complete, verify that the Mobility Master or managed device is using the correct AOS-W version by navigating to the **Maintenance > Software Management > About** page.

## In the CLI

The following section describes how to downgrade the AOS-W version.

1. If the saved pre-upgrade configuration file is on an external FTP/TFTP server, use the following command to copy it to the switch:

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

or

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

2. Set the switch to boot with your pre-upgrade configuration file.

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

3. Execute the **show image version** command to view the partition on which your pre-upgrade AOS-W version is stored. You cannot load a new image into the active system partition (the default boot).

```
#show image version
```

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

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

5. Reboot the Mobility Master or managed device.

```
(host) # reload
```

6. When the boot process is complete, verify that the Mobility Master or managed device is using the correct AOS-W version.

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

## Before Calling Technical Support

Provide the following information when you call Technical Support:

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