AOS-W 6.5.4.22

Alcatel·Lucent
Enterprise

Release Notes

Contents

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

Revision History

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

Table 1: *Revision History*

Revision	Change Description
Revision 01	Initial release.

This AOS-W release notes includes the following topics:

For the list of terms, refer Glossary.

Supported Browsers

The following browsers are officially supported for use with 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://businessportal.al-enterprise.com
Email	ebg_global_supportcenter@al-enterprise.com

Contact Center Online	
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 introduced in AOS-W 6.5.4.22 release.

This chapter contains the regulatory updates in AOS-W 6.5.4.22.

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.

The following DRT file version is part of this release.

- DRT-1.0_82868

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 support.esd.alcatel-lucent.com.

This software release supports the channel requirements described in *ALE Support Advisory SA-N0033*, available for download from the support.esd.alcatel-lucent.com site.

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 3: *Resolved Issues in AOS-W 6.5.4.22*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-229991	–	**Symptom:** Clients were unable to connect to SSIDs that had the 802.11r option enabled. During this period, commands run in the CLI returned the error message, **Module AP STM Low Priority is busy**. **Please try later**. The fix ensures that SSIDs configured with 802.11r option service the client as expected. **Scenario:** This issue was observed in APs running AOS-W 6.5.4.21 or later versions. **Duplicates:** AOS-230192, AOS-230290, AOS-230554, AOS-230604, AOS-230721, AOS-230871, AOS-229972, AOS-230416, and AOS-230725	Station Management	All platforms	AOS-W 6.5.4.21

This chapter describes the known issues identified 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 4: *Known Issues in AOS-W 6.5.4.22*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-127982 AOS-145349	154887 177271	**Symptom:** Some APs display incorrect IPv6 addresses when checked using SNMP. **Scenario:** This issue is observed in APs running AOS-W 6.5.1.9 or later versions. **Workaround:** None.	SNMP	All platforms	AOS-W 6.5.1.9
AOS-128831 AOS-147829 AOS-148994	155936 180912 182485	**Symptom:** A switch does not respond to the PPP LCP echo request messages from a PPPoE server making the PPPoE link unusable. **Scenario:** This issue is observed in switches running AOS-W 6.5.1.2 or later versions. **Workaround:** None.	PPPoE	All platforms	AOS-W 6.5.1.2
AOS-130510 AOS-177783	158149 176715	**Symptom:** The BLE scanning in an AP is slow and fewer BLE devices are reported. **Scenario:** This issue is observed in OAW-AP207 access points running AOS-W 6.5.2.0 or later versions. **Workaround:** None.	BLE	OAW-AP207 access points	AOS-W 6.5.2.0
AOS-133222	161655	**Symptom:** Some high-frequency radio statistics like Tx time, Rx time, and Rx clear are not collected correctly per beacon period in an AP. **Scenario:** This issue is observed in APs running AOS-W 6.5.2.0 or later versions. **Workaround:** None.	AP-Platform	All platforms	AOS-W 6.5.2.0

Table 4: *Known Issues in AOS-W 6.5.4.22*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-133616 AOS-144468 AOS-144501	162140 176047 176088	**Symptom:** The BLE devices connected to an AP display the value of the output as **Ineligible** for the **show ap debug ble-update-status ap-name** command. **Scenario:** This issue is observed in APs running AOS-W 6.5.3.3 or later versions. **Workaround:** None.	IoT	All platforms	AOS-W 6.5.3.3
AOS-134588	163341	**Symptom:** Some clients stop sending data traffic after every three hours approximately. **Scenario:** This issue occurs due to broken L3 connectivity. This issue is observed in APs running AOS-W 6.5.1.5 or later versions. **Workaround:** None.	AP-Wireless	All platforms	AOS-W 6.5.1.5
AOS-137064 AOS-140141	166426 167050 170409	**Symptom:** A master switch and a standby switch reboot unexpectedly. The log file lists the reason for this event as **Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:60)**. **Scenario:** This issue occurs when clients send A-MSDU traffic to switches. This issue is observed in OAW-40xx Series switches running AOS-W 6.5.1.9 or later versions in a master-standby topology. **Workaround:** None.	Switch-Datapath	OAW-40xx Series switches	AOS-W 6.5.1.9
AOS-137371 AOS-142604	166800 173645	**Symptom:** False detections of type-5 radars are triggered in the FCC domain. **Scenario:** This issue is observed in OAW-AP200 Series and OAW-AP220 Series access points running AOS-W 6.5.1.5 or later versions. **Workaround:** None.	AP-Wireless	OAW-AP200 Series and OAW-AP220 Series access points	AOS-W 6.5.1.5
AOS-138939	168789	**Symptom:** An AP with 802.1X supplicant configuration fails to boot. **Scenario:** This issue occurs when an ACL denies a DNS response from the DNS server. This issue is observed in APs running AOS-W 6.5.4.0 or later versions. **Workaround:** None.	AP-Platform	All platforms	AOS-W 6.5.4.0

Table 4: *Known Issues in AOS-W 6.5.4.22*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-139580	169622	**Symptom:** A syslog server displays the error message, **aruba_ change_channel 512 channel 6 mode 3 not found** for some APs. **Scenario:** This issue is observed in OAW-AP314 and OAW-AP315 access points running AOS-W 6.5.1.5. **Workaround:** None.	AP-Wireless	OAW-AP314 and OAW-AP315 access points	AOS-W 6.5.1.5
AOS-139880 AOS-139898	170037 170055	**Symptom:** An AP does not discover a master switch through ADP. **Scenario:** This issue occurs when a static IP address is configured in an AP and the ACL denies ADP packets. This issue is observed in APs running AOS-W 6.5.4.2 or later versions. **Workaround:** None.	AP-Platform	All platforms	AOS-W 6.5.4.2
AOS-140642	171103	**Symptom:** A switch crashes and reboots unexpectedly. The log file lists the reason for this event as **Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2)**. **Scenario:** This issue is observed in switches running AOS-W 6.5.1.9 or later versions. **Workaround:** None.	Switch-Datapath	All platforms	AOS-W 6.5.1.9
AOS-141091	171726	**Symptom:** A switch crashes and reboots unexpectedly. The log lists the reason for the event as **Datapath timeout (SOS Assert) (Intent: cause:register 54:86:50:2)**. **Scenario:** This issue is observed in OAW-4650 switches running AOS-W 6.5.3.3. **Workaround:** None.	Switch-Datapath	OAW-4650 switches	AOS-W 6.5.3.3
AOS-141528	172305	**Symptom:** A switch sends multiple SNMP error messages, **snmp [21466]: PAPI_Send: To: 7f000001:8419 Type:0x4 Timed out**. **Scenario:** This issue is observed in switches running AOS-W 6.5.1.9 or later versions. **Workaround:** None.	SNMP	All platforms	AOS-W 6.5.1.9
AOS-141755	172593	**Symptom:** ACLs are not displayed in the output of the **show datapath acl ap-name** command because acl entry parameters (d->index and d->entry.flags) are not set correctly on little endian APs. **Scenario:** This issue is observed in AOS-W 6.5.1.9 or later versions. **Workaround:** None.	Captive Portal	All platforms	AOS-W 6.51.9

Table 4: *Known Issues in AOS-W 6.5.4.22*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-142093	172987	**Symptom:** A switch crashes and reboots unexpectedly. The log file lists the reason for the event as **Kernel panic: Fatal exception**. **Scenario:** This issue is observed in OAW-4550 switches running AOS-W 6.5.3.3 or later versions. **Workaround:** None.	Switch-Datapath	OAW-4550 switches	AOS-W 6.5.3.3
AOS-142230	173168	**Symptom:** AppRF does not block Hotspot-Shield traffic in a switch. **Scenario:** This issue is observed in switches running AOS-W 6.5.1.9 or later versions. **Workaround:** None.	Switch-Datapath	All platforms	AOS-W 6.5.1.9
AOS-142392	173359	**Symptom:** A switch crashes and reboots unexpectedly. The log file lists the reason for this event as **Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2)**. **Scenario:** This issue is observed in OAW-4750 switches running AOS-W 6.5.3.3 or later versions. **Workaround:** None.	Switch-Datapath	OAW-4750 switches	AOS-W 6.5.3.3
AOS-142474	173465	**Symptom:** A switch crashes and reboots unexpectedly. The log file lists the reason for the event as **Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2)**. **Scenario:** This issue is observed in OAW-4650 switches running AOS-W 6.5.4.3 or later versions. **Workaround:** None.	Switch-Datapath	OAW-4650 switches	AOS-W 6.5.4.3
AOS-143005	174150	**Symptom:** A switch crashes and reboots unexpectedly. The log file lists the reason for this event as **Datapath crash**. **Scenario:** This issue is observed in7280 switches running AOS-W 6.5.4.2 or later versions. **Workaround:** None.	Switch-Datapath	7280 switches	AOS-W 6.5.4.2
AOS-143252	174473	**Symptom:** A switch crashes and reboots unexpectedly. The log file lists the reason for the event as **Datapath crash**. **Scenario:** This issue is observed in7280 switches running AOS-W 6.5.4.0 or later versions. **Workaround:** None.	Switch-Datapath	7280 switches	AOS-W 6.5.4.0

Table 4: *Known Issues in AOS-W 6.5.4.22*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-143457	174743	**Symptom:** A switch crashes and reboots unexpectedly. The log file lists the reason for the event as **Datapath crash**. **Scenario:** This issue is observed in7280 switches running AOS-W 6.5.4.0 or later versions. **Workaround:** None.	Switch-Datapath	7280 switches	AOS-W 6.5.4.0
AOS-143904	175340	**Symptom:** The AP logs for a Remote AP displays the error message, **connect-debounce failed, port 1 disabled**. **Scenario:** This issue is observed in Remote Access Points running AOS-W 6.5.3.1 or later versions. **Workaround:** None.	AP-Platform	OAW-RAP3WNP access points	AOS-W 6.5.3.1
AOS-144022	175493	**Symptom:** A controller crashes and reboots unexpectedly. The log file lists the reason for the event as **Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2)**. **Scenario:** This issue is observed in a OAW-4750 switches running AOS-W 6.5.3.3 or later versions. **Workaround:** None.	Switch-Datapath	OAW-4750 switches	AOS-W 6.5.3.3
AOS-144689	176344	**Symptom:** A switch does not retain the cached ACR license. **Scenario:** This issue is observed in switches running AOS-W 6.5.3.3-FIPS version. **Workaround:** None.	Licensing	All platforms	AOS-W 6.5.3.3-FIPS
AOS-144882	176622	**Symptom:** The UCC data export function is missing from the AOS-W 6.5.1.9 version running in a switch. **Scenario:** This issue is observed in switches running AOS-W 6.5.1.9 or later versions. **Workaround:** None.	UCC	All platforms	AOS-W 6.5.1.9
AOS-145636	177651	**Symptom:** Some Windows 64-bit clients detected 32-bit version of VIA while trying to download it using Microsoft Edge browser. **Scenario:** This issue is observed in OAW-AP225 access points running AOS-W 6.5.1.4 or later versions. **Workaround:** None.	AP-Wireless	OAW-AP225 access points	AOS-W 6.5.1.4

Table 4: *Known Issues in AOS-W 6.5.4.22*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-145876 AOS-156159 AOS-157877	177969 192218 194648	**Symptom:** On a 2.4 GHz radio, channel utilization is very low for a few APs. **Scenario:** This issue is observed in OAW-AP203R, OAW-AP207, and OAW-AP315 access points running AOS-W 6.5.4.0 or later versions. **Workaround:** None.	AP-Wireless	OAW-AP203R, OAW-AP207, and OAW-AP315 access points	AOS-W 6.5.4.9
AOS-146105 AOS-179536	185354	**Symptom:** An AP crashes and reboots unexpectedly. The log file lists the reason for this event as **rebooted caused by external watchdog reset**. **Scenario:** This issue occurs in the driver when multicast or DMO performance test is done either in bridge mode or tunnel mode. This issue is observed in OAW-AP203H, OAW-AP203R, and OAW-AP207 access points running AOS-W 6.5.4.8 or later versions. **Workaround:** None.	AP-Wireless	OAW-AP203H, OAW-AP203R, and OAW-AP207 access points	AOS-W 6.5.4.8
AOS-146948	179408	**Symptom:** A switch log file displays **|localdb| |wl-sync| Skipping db_sync** messages. **Scenario:** This issue is observed in OAW-4650 switches running AOS-W 6.5.3.4 or later versions. **Workaround:** None.	802.1X	OAW-4650 switches	AOS-W 6.5.3.4
AOS-147232 AOS-158495 AOS-184142	179942 195511	**Symptom:** A client is unable to send or receive traffic to or from an AP. **Scenario:** This issue occurs when the station management process in an AP sends a PAPI message to the AAC instead of the UAC. This issue is observed in switches in a cluster topology running AOS-W 6.4.4.22 with 802.11r enabled. **Workaround:** None.	Station Management	All platforms	AOS-W 6.4.4.22
AOS-147309	180094	**Symptom:** The console output of an AP shows **asap_user_set_acl: no name for id 0** message with the MAC address of the associated clients. **Scenario:** This issue is observed in APs running AOS-W 6.5.3.6 or later versions. **Workaround:** None.	Authentication	All platforms	AOS-W 6.5.3.6

Table 4: *Known Issues in AOS-W 6.5.4.22*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-148146 AOS-180312	181354	**Symptom:** Some clients experience ping loss while pinging a switch. **Scenario:** This issue occurs when the switch is connected to a mesh point. This issue is observed in switches running AOS-W 6.5.4.8 or later versions. **Workaround:** None.	Mesh	All platforms	AOS-W 6.5.4.8
AOS-148329	181606	**Symptom:** The output of the **show ap debug log** command displays the **Bridge entry insertion failure** error message. **Scenario:** This issue is observed in OAW-AP225 and OAW-AP335 access points running AOS-W 6.5.4.5 or later versions. **Workaround:** None.	AP Datapath	OAW-AP225 and OAW-AP335 access points	AOS-W 6.5.4.5
AOS-149135	182683	**Symptom:** The redirect page is blank and displays only **URL=** for WISPR clients. **Scenario:** This issue occurs when CPU utilization is high. This issue is observed in switches running AOS-W 6.5.1.6 or later versions. **Workaround:** None.	WISPR Interoperability	All platforms	AOS-W 6.5.1.6
AOS-151814	186224	**Symptom:** Clients are unable to connect to a bridge mode virtual AP after a VLAN assignment failure. **Scenario:** This issue occurs when the VLAN in a switch is removed, causing subsequent deauthentication of all the clients associated with the virtual APs. This issue is observed in switches running AOS-W 6.5.4.6 or later versions. **Workaround:** None.	Station Management	All platforms	AOS-W 6.5.4.6
AOS-152338	186981	**Symptom:** The SNMP polling displays **incorrect privacy password** mismatch error though the credentials are correct. **Scenario:** This issue is observed in switches running AOS-W 6.5.3.6 or later versions. **Workaround:** None.	SNMP	All platforms	AOS-W 6.5.3.6

Table 4: *Known Issues in AOS-W 6.5.4.22*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-153087	188021	**Symptom:** A switch generates the console error message, **|snmp| An internal system error has occurred at file ../unix/aruba_ main.c function snmpRequestProcessing line 704 error Cannot send snmp response**. **Scenario:** This issue is observed in switches running AOS-W 6.5.4.6 or later versions. **Workaround:** None.	SNMP	All platforms	AOS-W 6.5.4.6
AOS-153844	189017	**Symptom:** A few 802.11b clients are unable to pass traffic. **Scenario:** This issue is observed in OAW-AP305 access points running AOS-W 6.5.4.0 or later versions. **Workaround:** None.	AP-Wireless	OAW-AP305 access points	AOS-W 6.5.4.6
AOS-154191	189490	**Symptom:** Some APs send AMON messages such as **CL_HT_ MODE** with incorrect values displaying 0, 9, and 255. **Scenario:** This issue is observed in APs running AOS-W 6.5.4.7 or later versions. **Workaround:** None.	Station Management	All platforms	AOS-W 6.5.4.7
AOS-154324	189646	**Symptom:** Some clients using Fing mobile software are able to discover some wireless devices connected to the same AP. **Scenario:** This issue is not restricted to any specific switch model or AOS-W release version. **Workaround:** None.	Multicast	All platforms	AOS-W 6.5.4.8
AOS-154460	189816	**Symptom:** The WebUI of a switch does not display the certificate information in the **Configuration** > **Management** tab. **Scenario:** This issue is observed in switches running AOS-W 6.5.4.8 or later versions. **Workaround:** None.	WebUI	All platforms	AOS-W 6.5.4.8
AOS-154965	190482	**Symptom:** The global timers in the **Configuration** > **Security** > **Authentication** > **Advanced** tab cannot be configured. **Scenario:** This issue is observed in switches running AOS-W 6.5.4.9 or later versions. **Workaround:** None.	WebUI	All platforms	AOS-W 6.5.4.9

Table 4: *Known Issues in AOS-W 6.5.4.22*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-155267	190912	**Symptom:** The **show datapath bridge ap-name** and **show ap mesh debug forwarding-table ap-name** commands run into an infinite loop and display the **Warning: Not enough memory to complete this operation** error message. **Scenario:** This issue occurs when the AP is configured as a Remote AP with PPPoE enabled. This issue is observed in switches running AOS-W 6.5.4.9 or later versions. **Workaround:** None.	RAP-NG	All platforms	AOS-W 6.5.4.9
AOS-156027	192034	**Symptom:** An AP stops broadcasting on 2.4 GHz radios. **Scenario:** This issue is observed in AP-105 access points connected to switches running AOS-W 6.5.3.4 or later versions. **Workaround:** None. **Duplicates:** **New ID:** AOS-157576, AOS-158392, AOS-158580, AOS-182796, AOS-183992, AOS-184344 **Old ID:** 194197, 195377, 195607	AP-Wireless	AP-105 access points	AOS-W 6.5.3.4
AOS-156223	192294	**Symptom:** Some BSSIDs are classified as interfering instead of being classified as **suspected-rogue**. **Scenario:** This issue occurs when **rules_match_mask** does not reset while resetting the Remote AP attributes. This issue is observed in APs running AOS-W 6.5.1.10 or later versions. **Workaround:** None.	Air Management-IDS	All platforms	AOS-W 6.5.1.10
AOS-187337	–	**Symptom:** The WebUI allows access to pages which are inaccessible to administrators. **Scenario:** This issue is observed in switches running AOS-W 6.5.4.12 or later versions. **Workaround:** None.	WebUI	All platforms	AOS-W 6.5.4.12
AOS-190911 AOS-192857	–	**Symptom:** The **fw_visibility** process crashes in a 4-node cluster after an upgrade. **Scenario:** This issue is observed in switches running AOS-W 6.5.4.8 or later versions. **Workaround:** None.	Firewall Visibility	All platforms	AOS-W 6.5.4.8

Table 4: *Known Issues in AOS-W 6.5.4.22*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-190927 AOS-192132 AOS-216689	–	**Symptom:** A few switches are unresponsive without console access. **Scenario:** This issue occurs due to memory leak in STM process. This issue is observed in switches running AOS-W 6.5.4.17 or later versions. **Workaround:** None.	Switch Platform	All platforms	AOS-W 6.5.4.17
AOS-193751	–	**Symptom:** Some switches do not display certificate information in the WebUI. **Scenario:** This issue occurs when the account type is read-only. This issue is observed in switches running AOS-W 6.5.4.8 or later versions. **Workaround:** None.	WebUI	All platforms	AOS-W 6.5.4.8
AOS-194739	–	**Symptom:** A switch crashes and reboots unexpectedly. The log file lists the reason for this event as **Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:0:20)**. **Scenario:** This issue is observed in 7280 switches running AOS-W 6.5.4.13 or later versions. **Workaround:** None.	Switch-Datapath	7280 switches	AOS-W 6.5.4.13
AOS-194919 AOS-195565 AOS-205648 AOS-206010	–	**Symptom:** The **HTTPD** process in a switch crashes unexpectedly. The log files list the reason for the event as **Reboot Cause: User reboot (Intent:cause: 86:50)**. **Scenario:** This issue occurs when the switch is scanned for security vulnerabilities. This issue is observed in switches running AOS-W 6.5.4.0 or later versions. **Workaround:** None.	Web Server	All platforms	AOS-W 6.5.4.0
AOS-198003	–	**Symptom:** Network firewall drops fragmented packets and hence, clients face connectivity issues. **Scenario:** This issue is observed in switches running AOS-W 6.5.4.9 or later versions. **Workaround:** None.	Switch-Datapath	All platforms	AOS-W 6.5.4.9

Table 4: *Known Issues in AOS-W 6.5.4.22*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-200084 AOS-204429	–	**Symptom:** A few APs crash and reboot unexpectedly. The log file lists the reason for the event as **Kernel panic - not syncing: Rebooting the AP because of FW ASSERT**. **Scenario:** This issue was observed in OAW-AP305 access points running AOS-W 6.5.4.13 or later versions. **Workaround:** None.	AP-Wireless	OAW-AP305 access points	AOS-W 6.5.4.13
AOS-200762	–	**Symptom:** Disabling **Prohibit IP spoofing** in the firewall does not work as expected. This is because the ARP request frame is getting flooded as a broadcast instead of unicast. **Scenario:** This issue is observed in switches running AOS-W 6.5.4.14 or later versions. **Workaround:** None.	Switch-Datapath	All platforms	AOS-W 6.5.4.14
AOS-200993	–	**Symptom:** Active IP goes missing when a switch is reloaded after the next hop is configured with the IPsec map. **Scenario:** This issue is observed in switches running AOS-W 6.5.4.16 or later versions. **Workaround:** None.	Switch-Datapath	All platforms	AOS-W 6.5.4.16
AOS-203139	–	**Symptom:** The user table does not list the entire list of available users. **Scenario:** This issue occurs when BCMC optimization is enabled. This issue is observed in switches running AOS-W 6.5.4.13 or later versions. **Workaround:** None.	Base OS Security	All platforms	AOS-W 6.5.4.13

Table 4: *Known Issues in AOS-W 6.5.4.22*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-212300	–	**Symptom:** The **show processes** command displays defunct entries. **Scenario:** This issue is observed in switches running AOS-W 6.5.4.17 or later versions. **Workaround:** None.	Switch-Platform	All platforms	AOS-W 6.5.4.17
AOS-196042 AOS-217995 AOS-221263	–	**Symptom:** The **show ucc dns-ip-learning** command displays **Unknown** for **Service Provider**. **Scenario:** This issue is observed in switches running AOS-W 6.5.4.12 or later versions. **Workaround:** None.	UCC	All platforms	AOS-W 6.5.4.12
AOS-219177	–	**Symptom:** Some switches crash and reboot unexpectedly. The log file lists the reason for the event as **Reboot Cause: Soft Watchdog reset (Intent:cause:register de:86:70:2).** **Scenario:** This issue is observed in switches running AOS-W 6.5.4.18 or later versions. **Workaround:** None.	Switch-Platform	All platforms	AOS-W 6.5.4.18

This chapter details the 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 switch.

Topics in this chapter include:

Upgrade Caveats

- OAW-AP120 Series access points, OAW-4306 Series, OAW-4x04 Series, OAW-S3, and OAW-6000 switches are not supported in AOS-W 6.5.x. Do not upgrade to AOS-W 6.5.x if your deployment contains a mix of these switches in a master-local setup.
- If your switch is running AOS-W 6.4.0.0 or later versions, do not use a Windows-based TFTP server to copy the AOS-W image to the nonboot partition of the switch for upgrading or downgrading. Use FTP or SCP to copy the image.
- Starting from AOS-W 6.4.x, you cannot create redundant firewall rules in a single ACL. AOS-W will consider a rule redundant if the primary keys are the same. The primary key is made up of the following variables:
  - source IP or alias
  - destination IP or alias
  - proto-port or service

If you are upgrading from AOS-W 6.1 or earlier and your configuration contains an ACL with redundant firewall rules, upon upgrading, only the last rule will remain.

For example, in the following ACL, both ACE entries could not be configured in AOS-W 6.4.x. When the second ACE is added, it overwrites the first.

```
(host)(config) #ip access-list session allowall-laptop
(host)(config-sess-allowall-laptop) #any any any permit time-range test_range
(host)(config-sess-allowall-laptop) #any any any deny
(host)(config-sess-allowall-laptop) #!
(host)(config) #end
(host) #show ip access-list allowall-laptop

ip access-list session allowall-laptop
allowall-laptop
---------------
Priority        Source  Destination     Service Action  TimeRange
--------        ------  -----------     ------- ------  ---------
1               any     any             any     deny
```

- When upgrading the software in a multi-switch network (one that uses two or more Alcatel-Lucent switches), upgrade all the switches in the proper sequence listed in Upgrading in a Multi-switch Network on page 29.

AOS-W 6.5.0.0-FIPS Upgrade Failure

Customers upgrading from any FIPS version of AOS-W prior to AOS-W 6.5.0.0-FIPS to AOS-W 6.5.0.0-FIPS or later version may experience symptoms that indicate an upgrade failure. Symptoms may include loss of configuration or administrative access to the switch, and/or hostname reset of the switch to default value.

This condition is caused by a change in the FIPS requirement for the strength of the hashing algorithm that is used to protect the configuration file from outside tampering. Starting from AOS-W 6.5.0.0-FIPS, all versions of AOS-W are changed to use stronger hashing algorithm to meet FIPS requirements. This change is known to create a challenge when upgrading or downgrading a switch between AOS-W 6.4.0.0-FIPS version and AOS-W 6.5.0.0-FIPS version. In some instances, the new stronger hash value may be missing or incorrect. This may disrupt switch reboot.

The most common scenario is:

1. When a switch running any version of AOS-W 6.5.0.0-FIPS or later version is downgraded to any version of AOS-W 6.4.0.0-FIPS or prior version
2. Switch is upgraded to AOS-W 6.5.0.0- FIPS or later version.

To restore service, roll back to the previous AOS-W version:

1. Connect an administrative terminal to the console port of the switch.
2. Reboot the switch.
3. On the administrative terminal, interrupt the boot process when prompted to enter the cpboot bootloader.
4. Execute the **osinfo** command to display the versions of AOS-W hosted on partition 0 and partition 1.
5. Execute the **def_part 0** or **def_part 1** command depending on which partition hosts the AOS-W 6.4.0.0-FIPS or later version.

6. Execute the **reset** or **bootf** to reboot the switch.

This restores the switch configuration and the previous AOS-W version. Contact Alcatel-Lucent support for instructions to upgrade.

GRE Tunnel-Type Requirements

This section describes the important points to remember when configuring an L2 GRE tunnel:

- AOS-W 6.5.4.22 continues to support L2 GRE tunnel type zero, but it is recommended to use a non-zero tunnel type.
- If both L2 and L3 tunnels are configured between endpoint devices, you must use a non-zero tunnel type for L2 GRE tunnels.

Important Points to Remember and Best Practices

To upgrade your switch:

- 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 switch? Verify this information by navigating to the **Monitoring > NETWORK > All Access Points** page in the WebUI, or by executing the **show ap active** or **show ap database** commands.
  - How are those APs discovering the switch (DNS, DHCP Option, Broadcast)?
  - What version of AOS-W runs on your switch?
  - Are all switch running the same version of AOS-W?
  - What services are used on your switch (employee wireless, guest access, Remote AP, wireless voice)?
- Resolve any existing issues (consistent or intermittent) before you upgrade.
- If possible, use FTP to load AOS-W images to the switch. 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 to the “Software Licenses” chapter in the *AOS-W 6.5.x User Guide*.

Memory Requirements

All Alcatel-Lucent Switches store critical configuration data on an onboard compact flash memory module. Ensure that there is always free flash space on the switch. 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 60 MB of free memory is available for an upgrade using the WebUI or execute the **show memory** command to confirm that there is at least 40 MB of free memory available for an upgrade using the CLI. To recover memory, reboot the switch. After the switch comes up, upgrade immediately.
- Do not proceed with an upgrade unless 75 MB of flash space is available for an upgrade using WebUI or execute the **show storage** command to confirm that there is at least 60 MB of flash space available for an upgrade using the CLI. 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 switch to a desired location. Delete the following files from the switch 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 27 to copy the **crash.tar** file to an external server, and then execute the **tar clean crash** command to delete the file from the switch.
  - **Flash Backups:** Use the procedures described in Backing up Critical Data on page 27 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 switch.
  - **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 27 to copy the **logs.tar** file to an external server. Execute the **tar clean logs** command to delete the file from the switch.

In certain situations, a reboot or a shutdown could cause the switch 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.

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. Click **Configuration**.
2. Click **Save Configuration**.
3. Navigate to the **Maintenance > File > Backup Flash** page.
4. Click **Create Backup** to back up the contents of the flash memory to the **flashbackup.tar.gz** file.
5. 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 **Maintenance > File > Copy Files** page.
6. To restore the backup file to the flash memory, navigate to the **Maintenance > File > Restore Flash** 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 tar relevant files from flash...
   Please wait while we compress the tar file...
   Checking for free space on flash...
   Copying file to flash...
   File flashbackup.tar.gz created successfully on flash.
   ```
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
   ```

Upgrading in a Multi-switch Network

In a multi-switch network, upgrade the switch based on the switch type (master or local). Backup your switch before upgrading as described in Backing up Critical Data on page 27.

All switches in the network must be upgraded with the same version of AOS-W software. Ensure that the switch model is the same for redundant environments such as VRRP.

To upgrade a multi-switch:

1. Load the AOS-W image on all switches (including redundant master switches).
2. If all the switches cannot be upgraded and rebooted simultaneously, use the following guidelines:
   a. Upgrade the software image on all the switches.
   b. Reboot the master switch.
   c. After the master switch reboots, reboot the local switches simultaneously.
   d. Ensure that the master and local switches are upgraded to the AOS-W version.

Installing AOS-W 6.5.x-FIPS Version

Before you install AOS-W-FIPS version on a switch that is currently running a non-FIPS version, perform the following steps:

If you are currently running a AOS-W-FIPS version on the switch, do not execute the **write erase** command.

1. Download the AOS-W-FIPS image from the customer support site.
2. Install the AOS-W-FIPS image on the switch.
3. Execute the **write erase** command to reset the configuration to the factory default.
4. Reboot the switch by executing the **reload** command.

Upgrading AOS-W

Upgrade AOS-W using the WebUI and the CLI.

Ensure that there is enough free memory and flash space on your switch. For details, see Memory Requirements on page 27.

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

In the WebUI

The following steps describe how to upgrade AOS-W from one of these versions using local file:

- AOS-W 3.4.4.1 or later
- AOS-W 5.0.3.1 or later
- AOS-W 6.0.1.0 or later

When upgrading from an existing AOS-W 6.4.x release, it is required to set AMON packet size manually to a desired value. However, the packet size is increased to 32K by default for fresh installations of AOS-W 6.4.3.9.

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

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

4. Log in to the AOS-W WebUI from the PC or workstation.
5. Navigate to the **Maintenance > Controller > Image Management** page.
   a. Select the **Local File** option.
   b. Click **Browse** to navigate to the saved image file on your PC or workstation.
6. Select the downloaded image file.
7. Choose the non-boot partition from the **Partition to Upgrade**.
8. Choose **Yes** in the **Reboot Controller After Upgrade** to automatically reboot. Choose **No**, if you do not want the switch to reboot immediately.

The upgrade will not take effect until reboot.

9. Choose **Yes** in the **Save Current Configuration Before Reboot**.
10. Click **Upgrade**.

    When the software image is uploaded to the switch, the **Changes were written to flash successfully** message is displayed.
11. Click **OK**.

    The switch reboots automatically based on your selection in step 8.

Verifying the AOS-W Upgrade

The following steps describe how to verify that the switch is functioning as expected.

1. Log in to the WebUI to verify all your switches are up after the reboot.
2. Navigate to the **Monitoring > NETWORK > Network Summary** page to determine if your APs are up and ready to accept clients.
3. Verify that the number of APs and clients are what you would expect.
4. Verify that the number of access points 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 27 for information on creating a backup.

In the CLI

The following steps describe how to upgrade AOS-W from one of these versions using the CLI:

- AOS-W 3.4.4.1 or later
- AOS-W 5.0.3.1 or the latest version of AOS-W 5.0.x
- AOS-W 6.0.1.0 or later version of AOS-W 6.x

1. Download AOS-W from the customer support site.
2. Open an SSH session on the switch.
3. Execute the **ping** command to verify the network connection between the switch 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 images 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**.

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>
```

The USB option is available on the OAW-40xx Series and OAW-4x50 Seriesswitches.

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

```
(host)# reload
```

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

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

Verifying the AOS-W Upgrade

The following steps describe how to verify that the switch is functioning as expected.

1. Log in to the CLI to verify that all your switches 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 27 for information on creating a backup.

Downgrading AOS-W

A switch has two partitions, 0 and 1. If the upgrade fails on one of the partitions, you can reboot the switch from the other partition.

Database versions are not compatible between different AOS-W releases.

If you do not downgrade to a previously saved pre-6.1 configuration, some parts of your deployment may not work as they previously did. For example, when downgrading from AOS-W 6.5.4.22 to 5.0.3.2, changes made to WIPS in AOS-W 6.x prevent the new predefined IDS profile assigned to an AP group from being recognized by the older version of AOS-W. This unrecognized profile can prevent associated APs from coming up, and can trigger a profile error.
These new IDS profiles begin with *ids-transitional* while older IDS profiles do not include *transitional*. If you have encountered this issue, execute the **show profile-errors** and **show ap-group** commands to view the IDS profile associated with the AP group.

When reverting the switch software, use the previous version used on the switch.

Prerequisites

Before you reboot the switch with the pre-upgrade AOS-W version, perform the following steps:

1. Back up your switch. For details, see Backing up Critical Data on page 27.
2. Verify that the control plane security is disabled.
3. Set the switch to boot with the previously saved configuration file.
4. Set the switch 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, switch 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 switch. 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 switch by navigating to the **Maintenance > File > Copy Files** page.
   a. For **Source Selection**, 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. For **Destination Selection**, enter a file name (other than default.cfg) for Flash File System.

2. Set the switch to boot with your pre-upgrade configuration file by navigating to the **Maintenance > Controller > Boot Parameters** page.
   a. Select the saved pre-upgrade configuration file from the **Configuration File** drop-down list.
   b. Click **Apply**.
3. Determine the partition on which the previous AOS-W image is stored by navigating to the **Maintenance > Controller > Image Management** page. If there is no previous AOS-W image stored on the system partition, load it to 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. Click **Upgrade**.
4. Navigate to the **Maintenance > Controller > Boot Parameters** page.
   a. Select the system partition that contains the pre-upgrade image file as the boot partition.
   b. Click **Apply**.
5. Navigate to the **Maintenance > Controller > Reboot Controller** page and click **Continue**.
   The switch reboots after the countdown period.
6. After the switch reboots, log in to the WebUI and navigating to the **Maintenance > Controller > Image Management** page to verify the AOS-W version.

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 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.

```
#show image version
```

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

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

5. Reboot the switch.

```
(host) # reload
```

6. When the boot process is complete, verify that the switch is using the correct AOS-W version.

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

Before You Call 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.