AOS-W 6.5.4.13

Alcatel·Lucent
Enterprise

Release Notes

Revision History

The following table provides the revision history of this document.

Table 1: *Revision History*

Revision	Change Description
Revision 01	Initial release.

The AOS-W 6.5.4.13 release notes includes the following topics:

- New Features describes the new features and enhancements introduced in this release.
- Regulatory Updates lists the regulatory updates in this release.
- Resolved Issues lists the issues resolved in this release.
- Known Issues lists the issues identified in this release.
- Upgrade Procedure describes the procedures for upgrading your WLAN network to the latest AOS-W release version.

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
- Firefox 58 and later on Windows 7, Windows 8, Windows 10, and macOS
- Apple Safari 9.0 or later on macOS
- Google Chrome 67 and 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	

Contact Center Online	
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

Chapter 2
New Features

There are no new features introduced in AOS-W 6.5.4.13 release.

Chapter 3
Regulatory Updates

This chapter describes the regulatory updates in AOS-W 6.5.4.13.

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 default Downloadable Regulatory Table (DRT) version is part of AOS-W 6.5.4.13:

- DRT-1.0_70855

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 AOS-W 6.5.4.13.

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 6.5.4.13*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-104987	126176	**Symptom:** LLDP requests from multiple clients triggered unnecessary wired authentication requests that failed. The fix ensures that unnecessary wired authentication requests are blocked. **Scenario:** This issue occurred when wired authentication was linked with MAC authentication. This issue was observed in switches running AOS-W 6.4.2.4 or later versions.	LLDP	All platforms	AOS-W 6.4.2.4
AOS-128555	—	**Symptom:** A memory leak was found as a result of using a script to query the switch Monitoring Dashboard. The fix ensures that there is no memory leak. **Scenario:** This issue occurred when certain Monitoring Dashboard queries were run either using a script or the WebUI, where memory relating to the query **filter** strings were not freed. This issue was observed in switches running AOS-W 6.4.0.0 or later versions.	Monitoring	All platforms	AOS-W 6.5.4.11
AOS-135373 AOS-158456	164342 195462	**Symptom:** Some clients were unable to associate with an AP. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue occurred when the AP denied clients that crossed the configured **deny-time-range** value. This issue was observed in OAW-AP105 access points running AOS-W 6.5.1.0 or later versions.	Base OS Security	OAW-AP105 access points	AOS-W 6.5.1.3

Table 3: *Resolved Issues in AOS-W 6.5.4.13*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-140282 AOS-158227	195138	**Symptom:** The **tx-power** did not get recalculated when the **tx-chain** numbers changed. The fix ensures that the **tx-power** gets recalculated. **Scenario:** This issue was observed in OAW-AP225 access points running AOS-W 6.5.4.0 or later versions.	AP-Platform	OAW-AP225 access points	AOS-W 6.5.4.0
AOS-140500	170916	**Symptom:** The DNS server IP address was reserved as master candidate, and it was displayed as HA standby even though HA was disabled. The fix ensures that the resolved IP addresses are taken as master candidate and HA standby is displayed only when HA is enabled and standby IP configuration is pushed from the switch. **Scenario:** This issue was observed in switches running AOS-W 6.5.4.0 or later versions.	AP-Platform	All platforms	AOS-W 6.5.4.0
AOS-142382 AOS-184956	—	**Symptom:** Some APs were transmitting only 3 CSA beacons when the CSA count was set to 4. The fix ensures that the correct number of CSA beacons are transmitted. **Scenario:** This issue was observed in OAW-AP305 access points running AOS-W 6.5.3.4 or later versions.	AP-Wireless	OAW-AP305 access points	AOS-W 6.5.3.4
AOS-142387	173353	**Symptom:** The **TM** column (time used by MGMT frames) in the output of the **show ap radio-summary dot11g** command always displayed 100. The fix ensures that the actual value is displayed. **Scenario:** This issue was observed in access points running AOS-W 6.5.3.0 or later versions.	AP-Platform	All platforms	AOS-W 6.5.3.4
AOS-142612 AOS-157142	193536	**Symptom:** Radius Access / Accounting Request packet did not have the correct AP-mac address. Copying the AP-mac address instead of the BSSID fixes this issue. **Scenario:** This issue occurred when the **called-station-id**, **auth-modified**, and **acct-modified** parameters in the **aaa authentication-server radius** command had AP-mac address related configurations. This issue was observed in switches running AOS-W 6.5.4.0 or later versions.	Base OS Security	All platforms	AOS-W 6.5.4.7

Table 3: *Resolved Issues in AOS-W 6.5.4.13*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-143093 AOS-157338	193794	**Symptom:** A VIA client was unable to establish VPN tunnel with the switch. The log file listed the reason for this event as **Dropping VPN session because we have exceeded the VPN license-limit of 4096**. This issue is resolved by not incrementing the VPN license count for VPN tunnels. **Scenario:** This issue occurred when the VPN license was incorrectly incremented. This issue was observed in switches running AOS-W 6.4.3.9 or later versions.	IPsec	All platforms	AOS-W 6.4.3.9
AOS-143398 AOS-146422	174670 178706	**Symptom:** An LACP port channel received multiple warning messages, **LACP: Disabling Collection and Distribution on port 0/0/0 LAG 0.** The fix ensures that the LACP port channel does not receive these error messages. **Scenario:** This issue occurred when the port channel was in trusted mode and the trusted VLAN list for the port channel did not have the default VLAN in its list. This issue was observed in switches running AOS-W 6.5.3.5.	Port-Channel	All platforms	AOS-W 6.5.3.5
AOS-144310	173353	**Symptom:** A switch displayed the **Save failed: Module Authentication is busy. Please try later** error when the user attempted to save the configuration. The fix ensures that user can save the configuration changes in the switch. **Scenario:** This issue was observed in switches running AOS-W 6.5.3.0 or later versions.	Base OS Security	All platforms	AOS-W 6.5.3.3
AOS-144781 AOS-146209 AOS-146254 AOS-146858 AOS-147590	176490 178459 178407 178469 179289	**Symptom:** Clients were unable to send packets that were larger than 978 bytes over an IPsec tunnel. The fix ensures that the clients are able to send packets that are larger than 978 bytes over an IPsec tunnel. **Scenario:** This issue was observed in OAW-AP315 and OAW-AP320 Series access points running AOS-W 6.5.4.0 or later versions.	AP Datapath	OAW-AP315 and OAW-AP320 Series access points	AOS-W 6.5.4.0
AOS-144984 AOS-145169	176774 177016	**Symptom:** An AP crashed and rebooted unexpectedly. The log file listed the reason for the event as **Kernel panic - not syncing: Fatal exception in interrupt**. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue was observed in OAW-AP225 access points running AOS-W 6.5.1.4 or later versions.	AP-Wireless	OAW-AP225 access points	AOS-W 6.5.1.4

Table 3: *Resolved Issues in AOS-W 6.5.4.13*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-145170	177017	**Symptom:** An AP crashed and rebooted unexpectedly. The log file listed the reason for this event as **Kernel panic - not syncing: Fatal exception in interrupt**. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue was observed in OAW-AP225 access points running AOS-W 6.5.1.4 or later versions.	AP-Wireless	OAW-AP225 access points	AOS-W 6.5.1.4
AOS-145304	177205	**Symptom:** The **Station Management** process in a switch crashed and the switch rebooted unexpectedly. The log file listed the reason for this event as **unexpected stm (Station management) runtime error at data_path_handler, 1324, data_path_handler: recv - Network is down**. The fix ensures that the switch works as expected. **Scenario:** This issue was observed in OAW-4650 switches running AOS-W 6.5.3.4 or later versions.	Station Management	OAW-4650 switches	AOS-W 6.5.3.4
AOS-145463	177420	**Symptom:** The HSTS Security header was missing in the HTTP response from the switch WebUI. The fix ensures that the HSTS header is included in the HTTP response. **Scenario:** This issue was not limited to any specific switch model or AOS-W release version.	Web Server	All platforms	AOS-W 6.5.4.0
AOS-145651 AOS-147206 AOS-180623	177671 179906 190477 193836	**Symptom:** An AP crashed and rebooted unexpectedly. The log file listed the reason for this event as **Reboot caused by kernel panic: Take care of the HOST ASSERT first**. Enhancements to the wireless driver resolved the issue. **Scenario:** This issue was observed in OAW-AP300 Series, OAW-AP310 Series, OAW-AP320 Series, and OAW-AP330 Series access points running AOS-W 6.5.4.0 or later versions.	AP-Wireless	OAW-AP300 Series, OAW-AP310 Series, OAW-AP320 Series, and OAW-AP330 Series access points	AOS-W 6.5.4.0
AOS-146331 AOS-183502 AOS-184796 AOS-185200	178574	**Symptom:** The **Datapath** process crashed in a switch. The fix ensures that the switch works as expected. **Scenario:** This issue was observed in 7280 switches running AOS-W 6.5.4.0 or later versions.	Switch-Datapath	7280 switches	AOS-W 6.5.0.0

Table 3: *Resolved Issues in AOS-W 6.5.4.13*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-146375	178633	**Symptom:** An AP console displayed the **fsl_dpa ethernet.17 eth0: Err FD status = 0x00000020** error message. The fix ensures that the AP works as expected. **Scenario:** This issue occurred when the AP received bad checksum uplink packets. This issue was observed in OAW-AP335 access points running AOS-W 6.5.4.0 or later versions.	AP Datapath	OAW-AP335 access points	AOS-W 6.5.4.0
AOS-146670 AOS-152310 AOS-157311 AOS-182295 AOS-184295	179034 193759	**Symptom:** Clients experience poor performance with OAW-AP300 Series access points. Enhancements to the wireless driver resolved this issue. **Scenario:** The issue was observed in OAW-AP300 Series access points running AOS-W 6.5.4.0 or later versions.	AP-Wireless	OAW-AP300 Series access points	AOS-W 6.5.4.0
AOS-147036 AOS-155499 AOS-158444	179623 191227 195448	**Symptom:** A switch crashed and rebooted unexpectedly. The log file listed the reason for this event as **Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:0:20).** The fix ensures that the switch works as expected. **Scenario:** This issue occurred due to a race condition while upgrading the hardware caches. This issue was observed in switches running AOS-W 6.5.4.0 or later versions.	Switch-Datapath	All platforms	AOS-W 6.5.4.0
AOS-147223 AOS-153842 AOS-185358	179928 189015	**Symptom:** Clients were unable to connect to the 2.4 GHz or 5 GHz radio on some APs. The fix ensures that the clients are connected to the 2.4 GHz or 5 GHz radio. **Scenario:** This issue was observed in OAW-AP300 Series access points running AOS-W 6.5.4.5 or later versions.	Station Management	OAW-AP300 Series access points	AOS-W 6.5.4.5
AOS-147062	1179696	**Symptom:** A mismatch of MTU value was observed between the AP and the switch. The issue is resolved by changing the default value of the **rap-gre-mtu** parameter from 1200 bytes to 1300 bytes under the **ap system-profile <profile_name>** command. **Scenario:** This issue occurred when the AP was rebooted after setting the default value of the **rap-gre-mtu** parameter. This issue was observed in OAW-AP305 and OAW-AP315 access points running AOS-W 6.5.4.0 or later versions.	AP-Platform	OAW-AP305 and OAW-AP315 access points	AOS-W 6.5.4.0

Table 3: *Resolved Issues in AOS-W 6.5.4.13*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-147231 AOS-148250	179939 181520	**Symptom:** A user was unable to configure the **radius-interim-accounting** parameter using the **aaa profile** command. The fix ensures that the user can configure the parameter. **Scenario:** This issue occurred when the **dhcp-option-12** parameter in the **aaa derivation-rules** command and the **enforce-dhcp** parameter in the **aaa profile** command were enabled. This issue was observed in switches running AOS-W 6.5.3.7 or later versions.	Base OS Security	All platforms	AOS-W 6.5.3.7
AOS-147232 AOS-158495 AOS-184142	179942 195511	**Symptom:** Some clients did not send or receive traffic to or from an AP. The fix ensures that the clients can send and receive traffic. **Scenario:** This issue occurred when the station management process in an AP sent PAPI message to the AAC instead of the UAC. This issue was observed in switches running AOS-W 6.5.4.5 or later versions.	Station Management	All platforms	AOS-W 6.5.4.5
AOS-147914	181043	**Symptom:** An AP crashed and rebooted unexpectedly. The fix ensures that the AP works as expected. **Scenario:** This issue occurred because of retransmitted PAPI messages. This issue was observed in OAW-AP225 access points running AOS-W 6.5.1.9 or later versions.	Station Management	OAW-AP225 access points	AOS-W 6.5.1.9
AOS-147991 AOS-148924	181147	**Symptom:** The Datapath core dump was incomplete and did not have traceback for some CPUs. The fix ensures that the core dump is completed. **Scenario:** This issue was observed in OAW-4750 and OAW-40xx Series switches running AOS-W 6.5.4.0 or later versions.	Switch-Platform	OAW-4750 and OAW-40xx Series switches	AOS-W 6.5.4.0
AOS-148169 AOS-153101 AOS-156712	181401 188037	**Symptom:** A mesh AP came up with **ML** (unlicensed) flags. The fix ensures that the mesh AP works as expected. **Scenario:** This issue occurred after a VRRP failover. This issue was observed in access points running AOS-W 6.4.4.17 as a mesh portal.	AP-Platform	All platforms	AOS-W 6.4.4.17
AOS-148675 AOS-158300	182073 195240	**Symptom:** An AP crashed and rebooted unexpectedly. The log file listed the reason for this event as **Kernel panic - not syncing: Rebooting the AP because of FW ASSERT: rcRateFind+229; ratectrl_11ac.c:2394**. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue was observed in OAW-AP315 access points running AOS-W 6.5.4.0 or later versions.	AP-Wireless	OAW-AP315 access points	AOS-W 6.5.4.0

Table 3: *Resolved Issues in AOS-W 6.5.4.13*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-149285	182878	**Symptom:** IDS tarpit containment was inconsistent in APs. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue occurred when APs were configured in AM mode with tarpit containment enabled in **deauth-only** mode. This issue was observed in OAW-AP305 access points running AOS-W 6.5.4.7 or later versions.	Air Management - IDS	OAW-AP305 access points	AOS-W 6.5.4.7
AOS-149456	183100	**Symptom:** OID did not provide IPv6 address of an AP when clients tried to get SNMP. The fix ensures that the OID provides both IPv4 and IPv6 addresses. **Scenario:** This issue occurred because the OID did not exist. This issue was observed in access points running AOS-W 6.5.4.7 or later versions.	SNMP	All platforms	AOS-W 6.5.4.7
AOS-149657	183358	**Symptom:** A switch crashed and rebooted unexpectedly. The log file listed the reason for this event as **Reboot Cause: Nanny rebooted machine - fpapps process died (Intent:cause:register 34:86:50:2)**. The fix ensures that the switch works as expected. **Scenario:** This issue was observed in switches running AOS-W 6.5.3.6 or later versions.	Switch-Datapath	All platforms	AOS-W 6.5.3.6
AOS-150599 AOS-187306		**Symptom:** Some switches failed to do a full kernel coredump though it was configured and flash storage was cleared. The fix ensures that the switch works as expected. **Scenario:** This issue was observed in OAW-4x50 Series switches running AOS-W 6.5.4.12 or later versions.	Switch-Platform	OAW-4x50 Series switches	AOS-W 6.5.4.12
AOS-150879	184966	**Symptom:** A switch crashed and rebooted unexpectedly. The log file listed the reason for this event as **Master Initiated Reboot**. The fix ensures that the switch works as expected. **Scenario:** This issue occurred when a branch office switch failed over and the license was changed in the master switch before the failover. This issue was observed in switches running AOS-W 6.5.2.0 or later versions in branch office setup.	Branch Office Switch	All platforms	AOS-W 6.5.2.0

Table 3: *Resolved Issues in AOS-W 6.5.4.13*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-151413 AOS-152871 AOS-153240 AOS-153948 AOS-153981 AOS-155577 AOS-185348	185679 187734 188214 189144 189191 191414	**Symptom:** An AP crashed and rebooted unexpectedly. The fix ensures that the AP works as expected. **Scenario:** This issue was observed in APs running AOS-W 6.5.3.7 or later versions.	AP-Platform	All platforms	AOS-W 6.5.3.7
AOS-151509 AOS-183260	—	**Symptom:** When the PBR policy **any user any route next-hop-list next-hop1** was attached to the user role, traffic initiated from the user worked properly but traffic from the server to the user did not hit the reverse PBR. This issue is resolved by applying reverse PBR to user based rules, when the traffic is initiated by the server. **Scenario:** This issue was observed in switches running AOS-W 6.5.4.0 or later versions.	PBR	All platforms	AOS-W 6.5.4.9
AOS-152750 AOS-186035	187572	**Symptom:** Alcatel-Lucent switches were sending OSPF LSA with '00' in LSA checksum field which was causing upstream routers to log OSPF errors. With the fix, Alcatel-Lucent switches send OSPF LSA with calculated checksum. **Scenario:** This issue occurred when the switch established OSPF neighbour relationship with routers other than Alcatel-Lucent routers. This issue was observed in switches running AOS-W 6.5.4.2 or later versions.	OSPF	All platforms	AOS-W 6.5.4.2
AOS-152880 AOS-154088 AOS-155582 AOS-157371 AOS-156758	187744 189352 191419 193868	**Symptom:** Some APs crashed and rebooted unexpectedly. The log files for the event listed the reason as **Reboot caused by kernel panic: Fatal exception**. The fix ensures that the AP works as expected. **Scenario:** This issue occurred when EIRP table was not sent to the AP when either 2G or 5G channel list was empty. This issue was observed in access points running AOS-W 6.5.4.0 or later versions.	AP Regulatory	All platforms	AOS-W 6.5.4.0
AOS-152872	187735	**Symptom:** The configured MTU value of an AP was incorrect in the switch. The fix ensures that the correct MTU value is reflected in the switch. **Scenario:** This issue occurred when the AP was rebooted after configuring the SAP MTU in the AP system-profile. This issue was observed in access points running AOS-W 6.5.4.0 or later versions.	Mesh	All platforms	AOS-W 6.5.4.0

Table 3: *Resolved Issues in AOS-W 6.5.4.13*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-153019	187939	**Symptom:** The **authentication** process in a switch leaked memory and generated a crash report. Improvements to memory management resolved this issue. **Scenario:** This issue occurred when the 802.1X authentication load was high. This issue was observed in switches running AOS-W 6.5.3.4 or later versions.	Authentication	All platforms	AOS-W 6.5.3.4
AOS-153169 AOS-184045 AOS-184530	—	**Symptom:** An AP crashed and rebooted unexpectedly. The log files listed the reason for the event as **kernel panic: softlockup: hung tasks**. The fix ensures that only 32 packets are processed in one batch. **Scenario:** This issue occurred because the firewall processed too many packets in one batch. This issue was observed in OAW-AP303H access points running AOS-W 6.5.4.0 or later versions.	AP Datapath	OAW-AP303H access points	AOS-W 6.5.4.10
AOS-153315	188313	**Symptom:** An AP deauthenticated a client unexpectedly. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue occurred because of an unexpected internal ageout and long connection delay. This issue was observed in OAW-AP300 Series, OAW-AP310 Series, OAW-AP320 Series, OAW-AP330 Series, and OAW-AP360 Series access points running ArubaOS 6.5.4.0 or later versions.	AP-Wireless	OAW-AP300 Series, OAW-AP310 Series, OAW-AP320 Series, OAW-AP330 Series, and OAW-AP360 Series access points	AOS-W 6.5.4.0
AOS-153478	188517	**Symptom:** Multiple APs crashed and rebooted unexpectedly. The fix ensures that the APs work as expected. **Scenario:** This issue was observed in APs running AOS-W 6.5.4.0 or later versions.	AP-Wireless	All platforms	AOS-W 6.5.4.0
AOS-153533 AOS-179571 AOS-181276 AOS-181402 AOS-184537	188590 185520 192894 193585	**Symptom:** Incorrect memory corruption was detected during fast recovery process of an AP. Enhancements to wireless driver resolved the issue. **Scenario:** This issue occurred when an AP crashed and rebooted unexpectedly due to a kernel panic. This issue was observed in OAW-AP305 access points running AOS-W 6.5.4.0 or later versions.	AP-Wireless	OAW-AP305 access points	AOS-W 6.5.4.0

Table 3: *Resolved Issues in AOS-W 6.5.4.13*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-153902	189090	**Symptom:** A client lost connectivity with an AP. The fix ensures that the client connectivity is restored. **Scenario:** This issue occurred when the client forwarded small bytes of packets but the switch padded it with 0 bytes. This issue was observed in switches running AOS-W 6.5.4.0 or later versions.	Switch-Datapath	All platforms	AOS-W 6.5.4.0
AOS-154735 AOS-187277	190181	**Symptom:** An AP crashed and rebooted unexpectedly. The log files listed the reason for this event as **kernel panic: softlockup: hung tasks**. Enhancements to the wireless driver resolved the issue. **Scenario:** This issue was observed in OAW-AP203H access points running AOS-W 6.5.4.9 or later versions.	AP-Wireless	OAW-AP203H access points	AOS-W 6.5.4.9
AOS-154994 AOS-183903	—	**Symptom:** Some clients got disconnected from an AP and the error message displayed the reason as **Requested authentication algorithm not supported** instead of displaying **Disassociated; Auth frame from STA that was already associated**. The fix ensures that the correct error message is displayed. **Scenario:** This issue was observed in access points running AOS-W 6.4.4.20 or later versions.	Station Management	All platforms	AOS-W 6.4.4.20
AOS-155275	190925	**Symptom:** A switch did not forward broadcast ARP packets to silent clients through GRE tunnels although the **no suppress-arp** parameter was set. The fix ensures that the **no suppress-arp** command overrides the **broadcast-filter arp** command to allow unknown broadcast ARP packets through GRE tunnels. **Scenario:** This issue was observed in switches running AOS-W 6.5.4.0 or later versions.	Switch-Datapath	All platforms	AOS-W 6.5.4.0
AOS-155352	191031	**Symptom:** Bandwidth contract was not getting applied when clients disconnected and reconnected to an AP. The fix ensures that the bandwidth contract gets applied even if the clients disconnect and reconnect. **Scenario:** This issue was observed in switches running AOS-W 6.5.4.0 or later versions.	Base OS Security	All platforms	AOS-W 6.5.4.0

Table 3: *Resolved Issues in AOS-W 6.5.4.13*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-155533	—	**Symptom:** A switch crashed and rebooted unexpectedly. The log file listed the reason for this event as **Reboot Cause: Kernel Panic (Intent:cause:register 12:86:0:20)**. The fix ensures that the switch works as expected. **Scenario:** This issue occurred due to a corrupt neighbor entry in the forwarding path. This issue was observed in 7280 switches running AOS-W 6.5.4.8 or later versions.	Switch-Platform	7280 switches	AOS-W 6.5.4.8
AOS-155667 AOS-182789 AOS-185224 AOS-186048 AOS-186473	—	**Symptom:** An AP crashed and rebooted unexpectedly. The log file listed the reason for this event as **Reboot caused by kernel panic: Fatal exception in interrupt**. The fix ensures that the access point works as expected. **Scenario:** This issue was observed in Remote access points running AOS-W 6.5.4.10 or later versions.	AP Datapath	All platforms	AOS-W 6.5.4.10
AOS-155877 AOS-184056	191816	**Symptom:** A switch crashed and rebooted unexpectedly. The log file listed the reason for this event as **Reboot Cause: Kernel Panic (Intent:cause:register 12:86:0:20)**. The fix ensures that the switch works as expected. **Scenario:** This issue was observed in OAW-40xx Series and OAW-4x50 Series switches running AOS-W 6.5.4.0 or later versions.	Switch-Platform	OAW-40xx Series and OAW-4x50 Series switches	AOS-W 6.5.4.0
AOS-156244 AOS-187898	192323	**Symptom:** A switch sent syslog packets with invalid facility levels. This issue is resolved by implementing a local logging facility. **Scenario:** This issue was observed in switches running AOS-W 6.5.4.0 or later versions.	Logging	All platforms	AOS-W 6.5.4.10
AOS-156282	192378	**Symptom:** Some clients were unable to connect to c switch. The fix ensures that the switch works as expected. **Scenario:** This issue occurred when the **enforce DHCP** feature was enabled. This issue was observed in switches running AOS-W 6.5.4.0 or later versions.	Switch-Datapath	All platforms	AOS-W 6.5.4.0
AOS-156840 AOS-157049 AOS-185234	193416	**Symptom:** The **halt** command did not work on a switch. The fix ensures that the command can be executed on the switch. **Scenario:** This issue occurred when **Initialization** process was killed during the execution of the **halt** command. This issue was observed in switches running AOS-W 6.5.4.0 or later versions.	Switch-Platform	All platforms	AOS-W 6.5.4.0

Table 3: *Resolved Issues in AOS-W 6.5.4.13*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-157205	193553	**Symptom:** The NTP server failed to synchronize after upgrading the switch to AOS-W 6.5.4.9 version. The fix ensures that the switch works as expected. **Scenario:** This issue was observed in switches running AOS-W 6.5.4.9 or later versions.	VLAN	All platforms	AOS-W 6.5.4.9
AOS-157205	193617	**Symptom:** High Availability on the backup LMS configuration was displayed as disabled when the **show ap debug system-status** was executed although High Availability was enabled on the switch. The fix ensures that High Availability is not displayed as disabled. **Scenario:** This issue was observed in OAW-4x50 Series switches running AOS-W 6.5.4.4 or later versions.	HA-Lite	OAW-4x50 Series switches	AOS-W 6.5.4.4
AOS-157357	193834	**Symptom:** Static link aggregation was not formed correctly when switchport mode and VLAN STP were disabled. Enhancements to the driver resolved this issue. **Scenario:** This issue was observed in stand-alone switches running AOS-W 6.5.4.0 or later versions.	Port-Channel	All platforms	AOS-W 6.5.4.8
AOS-157573	194193	**Symptom:** Wireless clients were unable to access internet through the APs configured in PPPoE and split-tunnel mode. The fix ensures that the wireless client is able to pass traffic and access internet. **Scenario:** This issue occurred because linux detected one timed out neighbor and deleted the corresponding route cache table. This issue was observed in OAW-AP305 access points running AOS-W 6.5.3.4 or later versions.	RAP+BOAP	OAW-AP305 access points	AOS-W 6.5.3.4
AOS-157610	194243	**Symptom:** Some scanners were unable to connect to static WEP SSID. The fix ensures that the scanners are connected to static WEP SSID. **Scenario:** This issue occurred when the static WEP SSID was configured with the key index value of 2 using the command, **wlan ssid-profile**. This issue was observed in OAW-AP305 access points running AOS-W 6.5.4.7 or later versions.	AP-Wireless	OAW-AP305 access points	AOS-W 6.5.4.7

Table 3: *Resolved Issues in AOS-W 6.5.4.13*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-157979	194788	**Symptom:** A memory leak was found in both **arci-cli-helper** and **STM** processes as a result of using a script to query the switch Monitoring Dashboard. The fix ensures that there is no memory leak. **Scenario:** This issue occurred when certain Monitoring Dashboard queries were run either using a script or the WebUI, where memory relating to the query **filter** strings were not freed. This issue was observed in switches running AOS-W 6.4.0.0 or later versions.	Monitoring	All platforms	AOS-W 6.5.4.11
AOS-158207	195111	**Symptom:** An incorrect redirected URL was displayed during an external captive portal authentication. The fix ensures that the correct redirected URL is displayed on the captive portal page. **Scenario:** This issue was observed in OAW-AP205 access points running AOS-W 6.4.4.0 or later versions.	Captive Portal	OAW-AP205 access points	AOS-W 6.4.4.20
AOS-158511	195528	**Symptom:** IAP wireless clients did not receive IP address from one particular slave IAP. The fix ensures that the IAP wireless clients receive IP addresses. **Scenario:** This issue occurred when the IAP cluster was upgraded to a higher version of ArubaOS. This issue was observed in switches running AOS-W 6.5.4.2 or later versions.	Switch-Datapath	All platforms	AOS-W 6.5.4.2
AOS-158599 AOS-182977	—	**Symptom:** A switch crashed and rebooted unexpectedly. The log file listed the reason for this event as **Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:4)**. The fix ensures that the switch works as expected. **Scenario:** This issue occurred when some wired client were sending malformed packets to the switch. This issue was observed in OAW-4650 switches running AOS-W 6.5.4.7 or later versions.	Switch-Datapath	OAW-4650 switches	AOS-W 6.5.4.7
AOS-182091 AOS-183253 AOS-183255 AOS-184627	—	**Symptom:** The **mDNS** process in a switch crashed unexpectedly. The fix ensures that the switch works as expected. **Scenario:** This issue occurred due to memory corruption. This issue was observed in switches running AOS-W 6.5.4.0 or later versions.	AirGroup	All platforms	AOS-W 6.5.4.7

Table 3: *Resolved Issues in AOS-W 6.5.4.13*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-183148 AOS-183454 AOS-183782 AOS-184700 AOS-185163 AOS-186657 AOS-187148	—	**Symptom:** Some APs crashed and rebooted unexpectedly. The log file lists the reason for this event as **Reboot reason: fatal exception in interrupt.** The fix ensures that the APs work as expected. **Scenario:** This issue was observed in OAW-AP214, OAW-AP215, and OAW-AP315 access points running AOS-W 6.5.4.0 or later versions.	AP-Platform	OAW-AP214, OAW-AP215, and OAW-AP315 access point	AOS-W 6.5.4.12
AOS-183601	—	**Symptom:** Some APs advertised incorrect protection flag in their beacons. Enhancements to the wireless driver resolved the issue. **Scenario:** This issue occurred when 802.11g, 802.11n, or 802.11ac clients were connected to 2.4 GHz radios and low rates of 1 Mbps were removed from the tx-rate of SSID profiles. This issue was observed in OAW-AP305 and OAW-AP315 access points running AOS-W 6.5.4.0 or later versions.	AP-Wireless	OAW-AP305 and OAW-AP315 access points	AOS-W 6.5.4.0
AOS-184032	—	**Symptom:** An AP crashed and rebooted unexpectedly. The log file listed the reason for this event as **Reboot caused by kernel panic: Fatal exception in interrupt**. Enhancements to the wireless driver resolved the issue. **Scenario:** This issue was observed in OAW-AP315 access points running AOS-W 6.5.4.0 or later versions.	AP-Wireless	OAW-AP315 access points	AOS-W 6.5.4.10
AOS-184051	—	**Symptom:** A switch was sending NTP sync packets every 15 minutes to the NTP server. The fix ensures that the switch works as expected. **Scenario:** This issue occurred due to upstream reachability that triggered sync packets from the switch. This issue was observed in switches running AOS-W 6.5.4.0 or later versions.	VLAN	All platforms	AOS-W 6.5.4.9
AOS-184208	—	**Symptom:** The **Dashboard** > **Traffic Analysis** > **AppRF** > **Roles** tab displayed **Unknown**. The fix ensures that the correct value is displayed. **Scenario:** This issue occurred after clients got authenticated, but the role was not updated. This issue was observed in OAW-4550 switches running AOS-W 6.5.4.0 or later versions.	Firewall Visibility	OAW-4550 switches	AOS-W 6.5.4.0

Table 3: *Resolved Issues in AOS-W 6.5.4.13*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-184545 AOS-187213	—	**Symptom:** An AP crashed and rebooted unexpectedly. The log file listed the reason for this event as **kernel panic: softlockup: hung tasks**. Reducing the batch size to 64 resolves this issue. **Scenario:** This issue occurred when the AP processed large batch files leading to lock stall detection and causing panic. This issue was observed in OAW-AP303H access points running AOS-W 6.5.4.0 or later versions.	AP Datapath	OAW-AP303H access points	AOS-W 6.5.4.12
AOS-184675	—	**Symptom: Datapath** process crashed in a switch during L3 mobility. The fix ensures that the switch works as expected. **Scenario:** This issue occurred when a client roamed to the switch. This issue was observed in switches running AOS-W 6.5.4.12.	Switch-Datapath	All platforms	AOS-W 6.5.4.12
AOS-184787 AOS-185375	—	**Symptom:** The **Authentication** process crashed in a controller. The fix ensures that the controller works as expected. **Scenario:** This issue occurred due to memory corruption. This issue was observed in OAW-4750 and OAW-4750XM switches running AOS-W 6.4.4.20 or later versions.	Base OS Security	OAW-4750 and OAW-4750XM switches	AOS-W 6.4.4.20
AOS-185920 AOS-185921	—	**Symptom:** A switch crashed and rebooted unexpectedly. The log file listed the reason for this event as **Nanny Rebooted Machine – fpapps process died and crashed on pubsub, cfgm, syslogdwrap, aaa and nanny module**. The fix ensures that the switch works as expected. **Scenario:** This issue occurred due to a memory leak. This issue was observed in switches running AOS-W 6.4.0.0 or later versions.	IPsec	All platforms	AOS-W 6.4.4.16
AOS-186386 AOS-186556	—	**Symptom:** Clients failed to obtain the IPv6 address from the external DHCPv6 servers. The fix ensures that the switch works as expected. **Scenario:** This issue occurred when **bc-mc optimization** was enabled. This issue was observed in switches running AOS-W 6.5.4.0 or later versions.	DHCP	All platforms	AOS-W 6.5.4.12

Table 3: *Resolved Issues in AOS-W 6.5.4.13*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-186422	—	**Symptom:** Some clients did not receive an IP address when connected to a Remote AP. The fix ensures that clients receive IP address. **Scenario:** This issue occurred when forwarding mode was set to Tunnel. This issue was observed in Remote OAW-AP205 access points running AOS-W 6.5.4.0 or later versions.	Switch-Datapath	Remote OAW-AP205 access points	AOS-W 6.5.4.0
AOS-186667 AOS-187118	—	**Symptom:** Some clients were unable to associate to an AP because the AP stops beaconing. The fix ensures that the APs work as expected. **Scenario:** This issue was observed in OAW-AP100 Series access points running AOS-W 6.5.4.12.	AP-Wireless	OAW-AP100 Series access points	AOS-W 6.5.4.12
AOS-187086	—	**Symptom:** Switch traffic from wired phones were unable to reach the call server via uplink VLAN 4092. The fix ensures that the switch egresses the traffic from the wired phones. **Scenario:** This issue occurred when lower priority uplink was used as higher priority next-hop. This issue was observed in switches running AOS-W 6.5.4.0 or later versions.	Switch-Datapath	All platforms	AOS-W 6.5.4.0

This chapter describes the known and outstanding issues identified in AOS-W 6.5.4.13.

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 6.5.4.13*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-127789 AOS-128792 AOS-128621 AOS-129208 AOS-130788 AOS-133333 AOS-140532 AOS-141083 AOS-142791 AOS-148054	154625 155709 156383 158536 161789 170955 171717 173885 181227	**Symptom:** The VRRP state changes although heartbeats are not missed. **Scenario:** This issue occurs when a standby switch inadvertently transitions to master state because the master switch delays the processing of VRRP advertisements. This issue is observed in switches running AOS-W 6.5.0.3 in a master-local topology. **Workaround:** Disable debug logs and syslog server. Increase the advertisement interval.	Switch-Platform	All platforms	AOS-W 6.5.0.3
AOS-127982 AOS-145349	177271	**Symptom:** Some APs display incorrect IPv6 addresses when checked using SNMP. **Scenario:** This issue is observed in access points 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. Hence, the PPPoE link is not usable. **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

Table 4: *Known Issues in AOS-W 6.5.4.13*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
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 access points running AOS-W 6.5.2.0. **Workaround:** None.	AP-Platform	All platforms	AOS-W 6.5.2.0
AOS-133616 AOS-144468 AOS-144501	176047 176088	**Symptom:** The output of the **show ap debug ble-update-status ap-name** command displays the number of ineligible beacons. **Scenario:** This issue is observed in switchesrunning AOS-W 6.5.4.0 or later versions. **Workaround:** None.	IoT	All platforms	AOS-W 6.5.4.3
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 access points running AOS-W 6.5.1.5 or later versions. **Workaround:** None.	AP-Wireless	All platforms	AOS-W 6.5.1.5
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 access points running AOS-W 6.5.1.9 or later versions. **Workaround:** None.	AP-Wireless	All platforms	AOS-W 6.5.1.9
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 DNS server. This issue is observed in access points 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 6.5.4.13*

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 or 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 access points running AOS-W 6.5.4.2. **Workaround:** None.	AP-Platform	All platforms	AOS-W 6.5.4.2
AOS-141528	172305	**Symptom:** A switch sends many 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-140141 AOS-137064	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-140642	171103	**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 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 or later versions. **Workaround:** None.	Switch-Datapath	OAW-4650 switches	AOS-W 6.5.3.3

Table 4: *Known Issues in AOS-W 6.5.4.13*

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 the 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 the event as **Datapath crash**. **Scenario:** This issue is observed in 7280 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 in 7280 switches running AOS-W 6.5.4.0. **Workaround:** None.	Switch-Datapath	7280 switches	AOS-W 6.5.4.0

Table 4: *Known Issues in AOS-W 6.5.4.13*

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 in 7280 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 observer in OAW-RAP3WNP 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-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 version running on 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-144984 AOS-145169	176774 177016	**Symptom:** An AP crashes and reboots unexpectedly. **Scenario:** This issue is observed in OAW-AP225 access points running AOS-W 6.5.1.4. **Workaround:** None.	AP-Wireless	OAW-AP225 access points	AOS-W 6.5.1.4
AOS-145603	177606	**Symptom:** The error **VLAN IP address conflict with another interface** is displayed while configuring a named VLAN under **Configure Controller** > **VLANs and IP Interfaces** > **Named VLANs** tab. **Scenario:** This issue is observed in OAW-4005 switches running AOS-W 6.5.1.4 or later versions. **Workaround:** None.	WebUI	OAW-4005 switches	AOS-W 6.5.1.4

Table 4: *Known Issues in AOS-W 6.5.4.13*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
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
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 with reason **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-146916	179360	**Symptom:** A switch displays the **Module L2TP is busy. Please try later** error message and does not provide the L2TP IP address. **Scenario:** This issue is observed in switches running AOS-W 6.5.2.0 or later versions. **Workaround:** None.	IPsec	All platforms	AOS-W 6.5.2.0
AOS-146948	179408	**Symptom:** A switch log file displays the **|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

Table 4: *Known Issues in AOS-W 6.5.4.13*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-147053	179656	**Symptom:** An AP crashes and reboots unexpectedly. The log file lists the reason for this event as **Kernel panic - not syncing: Fatal exception in interrupt**. **Scenario:** This issue occurs when the mesh role in the AP provisioning profile is set to mesh point. This issue is observed in OAW-AP300 Series access points running AOS-W 6.5.4.0 or later versions. **Workaround:** None.	AP-Wireless	OAW-AP300 Series access points	AOS-W 6.5.4.6
AOS-147255	179970	**Symptom:** The **flags** column in the output of the **show ap bss-table** displays wrong characters for wired clients. **Scenario:** This issue is observed in switches running AOS-W 6.5.4.7 or later versions. **Workaround:** None.	Station Management	All platforms	AOS-W 6.5.4.7
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 access points running AOS-W 6.5.3.6 or later versions. **Workaround:** None.	Authentication	All platforms	AOS-W 6.5.3.6
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-148564	181926	**Symptom:** A switch reboots unexpectedly. The log file lists the reason for the event as **Soft Watchdog reset (Intent:cause:register de:86:70:4)** **Scenario:** This issue is observed in OAW-4750 switches running AOS-W 6.5.4.2 or later versions. **Workaround:** None.	Switch-Platform	7280 switches	AOS-W 6.5.4.2
AOS-149285	182878	**Symptom:** IDS tarpit containment is inconsistent in APs. **Scenario:** This issue occurs when APs were configured in AM mode with tarpit containment enabled in **deauth-only** mode. This issue occurs in OAW-AP305 access points running AOS-W 6.5.4.7 or later versions. **Workaround:** None.	Air Management - IDS	OAW-AP305 access points	AOS-W 6.5.4.7

Table 4: *Known Issues in AOS-W 6.5.4.13*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
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. **Workaround:** None.	Station Management	All platforms	AOS-W 6.5.4.6
AOS-152338	186981	**Symptom:** The SNMP polling displays incorrect privacy password mis-match 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
AOS-153844	189017	**Symptom:** 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 access points 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:** 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-154965	190482	**Symptom:** The global timers under **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 6.5.4.13*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-157356	193833	**Symptom:** The cache for firewall **dns-name** is filling up and causing service interruptions. **Scenario:** This issue is observed in switches running AOS-W 6.5.4.10 or later versions. **Workaround:** Reboot the device.	Switch-Datapath	All platforms	AOS-W 6.5.4.10
AOS-157801	194522	**Symptom:** WebUI certificates are not getting pushed or reflected on the branch switch. **Scenario:** This issue occurs when the branch switch is mapped to Smart Config under a master switch. This issue is observed in switches running AOS-W 6.5.3.3 or later versions. **Workaround:** None.	Certificate Manager	All platforms	AOS-W 6.5.3.3
AOS-185238	—	**Symptom:** Under **Security** > **Access Control** > **User Roles** > **Firewall Policies** tab, users are unable to make changes to the ACL position. Other ACL positions are also getting disturbed while trying to change an ACL position. **Scenario:** This issue is observed in switches running AOS-W 6.5.4.10 or later versions. **Workaround:** None.	WebUI	All platforms	AOS-W 6.5.4.10
AOS-185745	—	**Symptom:** The output of the **show lldp neighbors** command displays incorrect remote interface information. **Scenario:** This issue is observed in switches running AOS-W 6.5.4.10 or later versions. **Workaround:** None.	LLDP	All platforms	AOS-W 6.5.4.10
AOS-186449	—	**Symptom:** A switch crashes and reboots unexpectedly. The log file lists the reason for this event as **Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:60)**. **Scenario:** This issue is observed in OAW-4030 switches running AOS-W 6.5.4.12 or later versions. **Workaround:** None.	Switch-Datapath	OAW-4030 switches	AOS-W 6.5.4.12
AOS-186649	—	**Symptom:** The word **Fragments** is misspelled in the **show datapath network ingress** command output. **Scenario:** This issue is not limited to any switch model or AOS-W release versions. **Workaround:** None.	Switch-Datapath	All platforms	AOS-W 6.5.4.12

Chapter 6
Upgrade Procedure

This chapter details the software upgrade procedures. Alcatel-Lucent best practices recommend that you schedule a maintenance window for upgrading your switches.

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 multiswitch network (one that uses two or more Alcatel-Lucent switches), special care must be taken to upgrade all the switches in the network and to upgrade them in the proper sequence. (See Upgrading in a Multiswitch Network on page 39.)

Failure to Upgrade to AOS-W 6.5.0.0-FIPS

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 the apparent loss of configuration, being unable to gain administrative access to the switch, and/or the hostname of the switch being set back to the 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 the 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 cause the switch to not boot normally.

The most common scenario is when a switch has been booted with any version of AOS-W 6.5.0.0-FIPS or later version, is subsequently downgraded to any version of AOS-W 6.4.0.0-FIPS or prior versions, and then at any point in the future is upgraded back to any version AOS-W 6.5.0.0-FIPS or later version.

To restore service, Alcatel-Lucent recommends to roll back the AOS-W to the previous version. This can be accomplished by:

1. Connect an administrative terminal to the console port of the switch.
2. Power cycle the switch to reboot it.
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 previous version AOS-W 6.4.0.0-FIPS or later version.

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

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

GRE Tunnel-Type Requirements

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

- AOS-W 6.5.4.13 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

Ensure a successful upgrade and optimize your upgrade procedure by taking the recommended actions provided in the following list. You should save this list for future use.

- 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 other 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 your 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** section of the WebUI, or by executing the **show ap active** and **show ap database** CLI commands.
  - How are those APs discovering the switch (DNS, DHCP Option, Broadcast)?
  - What version of AOS-W is currently on the switch?
  - Are all switches in a master-local cluster running the same version of software?
  - Which services are used on the switches (employee wireless, guest access, remote AP, wireless voice)?
- Resolve any existing issues (consistent or intermittent) before you upgrade.
- If possible, use FTP to load software 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 problems occur 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 should it be required.
- Before you upgrade to this version of AOS-W, assess your software license requirements and load any new or expanded licenses you may 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. To maintain the reliability of your WLAN network, the following compact memory best practices are recommended:

- Confirm that there is at least 60 MB of free memory 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. Do not proceed unless this much free memory is available. To recover memory, reboot the switch. After the switch comes up, upgrade immediately.
- Confirm that there is at least 75 MB of flash space available for an upgrade using the 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.

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

If the output of the **show storage** command indicates that there is insufficient flash memory space, you must free up some used memory. Any switch logs, crash data, or flash backups should be copied to a location off the switch, then deleted from the switch to free up flash space. You can delete the following files from the switch to free up some memory before upgrading:

- **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 37 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 37 to back up the flash directory to a file named **flash.tar.gz**, and then 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 37 to copy the **logs.tar** file to an external server, and then execute the **tar clean logs** command to delete the file from the switch.

Backing up Critical Data

It is important to frequently back up all critical configuration data and files on the compact flash file system to an external server or mass storage device. At the very least, you should include the following files in these frequent backups:

- Configuration data
- WMS database
- Local user database
- Licensing database
- Floor plan JPEGs
- Custom captive portal pages

- X.509 certificates
- Switch Logs

Backing up and Restoring Compact Flash in the WebUI

The WebUI provides the easiest way to back up and restore the entire compact flash file system. The following steps describe how to back up and restore the compact flash file system using the WebUI on the switch:

1. Click the **Configuration** tab.
2. Click **Save Configuration** at the top of the page.
3. Navigate to the **Maintenance > File > Backup Flash** page.
4. Click **Create Backup** to back up the contents of the compact flash file system to the **flashbackup.tar.gz** file.
5. Click **Copy Backup** to copy the file to an external server.

   You can later copy the backup file from the external server to the compact flash file system using the file utility in the **Maintenance > File > Copy Files** page.
6. To restore the backup file to the Compact Flash file system, navigate to the **Maintenance > File > Restore Flash** page and click **Restore**.

Backing up and Restoring Compact Flash in the CLI

The following steps describe the backup and restore procedure for the entire compact flash file system using the switch's command line:

1. Make sure you are in the **enable** mode in the switch CLI, and execute the following command:
   ```
   (host) # write memory
   ```
2. Execute the **backup** command to back up the contents of the compact flash file system 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 the **copy** command to transfer the backup flash 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 later transfer the backup flash file from the external server or storage device to the compact flash file system by executing the **copy** command.
   ```
   (host) # copy tftp: <tftphost> <filename> flash: flashbackup.tar.gz
   (host) # copy usb: partition <partition-number> <filename> flash: flashbackup.tar.gz
   ```
4. Execute the **restore** command to untar and extract the **flashbackup.tar.gz** file to the compact flash file system.
   ```
   (host) # restore flash
   ```

Upgrading in a Multiswitch Network

In a multiswitch network (a network with two or more Alcatel-Lucent switches), special care must be taken to upgrade all switches based on the switch type (master or local). Be sure to back up all switches being upgraded, as described in Backing up Critical Data on page 37.

For proper operation, all switches in the network must be upgraded with the same version of AOS-W software. For redundant environments such as VRRP, the switches should be of the same model.

To upgrade an existing multiswitch system to this version of AOS-W:

1. Load the software image onto all switches (including redundant master switches).
2. If all the switches cannot be upgraded with the same software image and rebooted simultaneously, use the following guidelines:
   a. Upgrade the software image on all the switches. Reboot the master switch. After the master switch completes rebooting, you can reboot the local switches simultaneously.
   b. Verify that the master and all local switches are upgraded properly.

Installing the FIPS Version of AOS-W 6.5.4.13

Download the FIPS version of the software from https://support.esd.alcatel-lucent.com.

Instructions on Installing FIPS Software

Before you install a FIPS version of the software on a switch that is currently running a non-FIPS version of the software, follow the procedure below. If you are currently running a FIPS version of the software on the switch, you do not have to perform a **write erase** to reset the configuration as mentioned in step 2.

Follow the steps below to install the FIPS software on a switch that is currently running a non-FIPS version of the software:

1. Install the FIPS version of the software on the switch.
2. Execute the **write erase** command to reset the configuration to the factory default; otherwise, you cannot log in to the switch using the CLI or WebUI.
3. Reboot the switch by executing the **reload** command.

This is the only supported method of moving from non-FIPS software to FIPS software.

Upgrading to AOS-W 6.5.4.13

The following sections provide the procedures for upgrading the switch to AOS-W 6.5.4.13 by using the WebUI and the CLI.

Install Using the WebUI

CAUTION

Confirm that there is at least 60 MB of free memory and at least 75 MB of flash space available for an upgrade using the WebUI. For details, see Memory Requirements on page 37.

NOTE

When you navigate to the **Configuration** tab of the switch's WebUI, the switch may display the **Error getting information: command is not supported on this platform** message. This error occurs when you upgrade the switch from the WebUI and navigate to the **Configuration** tab as soon as the switch completes rebooting. This error is expected and disappears after clearing the Web browser cache.

Upgrading From a Recent Version of AOS-W

The following steps describe the procedure to upgrade from one of these recent AOS-W versions:

- 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

NOTE

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.

Install the AOS-W software image from a PC or workstation using the WebUI on the switch. You can also install the software image from a TFTP or FTP server using the same WebUI page.

1. Download AOS-W 6.5.4.13 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. To verify the image, load the image onto a Linux system and execute the **sha256sum <filename>** command or 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 support site.

NOTE

The AOS-W image file is digitally signed, and is verified using RSA2048 certificates preloaded on the switch at the factory. Therefore, even if you do not manually verify the SHA hash of a software image, the switch will not load a corrupted 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 nonboot partition from the **Partition to Upgrade** radio button.
8. Choose **Yes** in the **Reboot Controller After Upgrade** radio button to automatically reboot after upgrading. Choose **No**, if you do not want the switch to reboot immediately.

Upgrade will not take effect until you reboot the switch.

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

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

    If you chose to automatically reboot the switch in step 8, the reboot process starts automatically within a few seconds (unless you cancel it).
12. When the reboot process is complete, log in to the WebUI and navigate to the **Monitoring > NETWORK > All WLAN Controllers** page to verify the upgrade.

When your upgrade is complete, perform the following steps 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. In addition, verify that the number of access points and clients are what you would expect.
3. Verify that the number of access points and clients are what you would expect.
4. Test a different type of client for each access method that you use and in different locations when possible.
5. Complete a backup of all critical configuration data and files on the compact flash file system to an external server or mass storage facility. See Backing up Critical Data on page 37 for information on creating a backup. If the flash (Provisioning/Backup) image version string shows the letters *rn*, for example, 3.3.2.11-rn-3.0, note those AP names and IP addresses.

Install Using the CLI

Confirm that there is at least 40 MB of free memory and at least 60 MB of flash space available for an upgrade using the CLI. For details, see Memory Requirements on page 37.

Upgrading From a Recent Version of AOS-W

The following steps describe the procedure to upgrade from one of these recent AOS-W versions:

- 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

To install the AOS-W software image from a PC or workstation using the CLI on the switch:

1. Download AOS-W 6.5.4.13 from the customer support site.
2. Open an SSH session on your master (and local) switches.
3. Execute the **ping** command to verify the network connection from the target switch to the SCP/FTP/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 are loaded on the switch's 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**.
5. Execute the **copy** command to load the new image onto the nonboot 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 Series switches.

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
   ```

When your upgrade is complete, perform the following steps 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 access points and clients are what you expected.

4. Test a different type of client for each access method that you use and in different locations when possible.
5. Complete a backup of all critical configuration data and files on the compact flash file system to an external server or mass storage facility. See Backing up Critical Data on page 37 for information on creating a backup.

Downgrading

If necessary, you can return to your previous version of AOS-W.

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 6.5.4.13 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, whenever possible, use the previous version of software known to be used on the system. Loading a release not previously confirmed to operate in your environment could result in an improper configuration.

Before You Begin

Before you reboot the switch with the preupgrade software version, you must perform the following steps:

1. Back up your switch. For details, see Backing up Critical Data on page 37.
2. Verify that the control plane security is disabled.
3. Set the switch to boot with the previously saved pre-AOS-W 6.5.4.13 configuration file.
4. Set the switch to boot from the system partition that contains the previously running AOS-W image.

   When you specify a boot partition (or copy an image file to a system partition), the software checks to ensure that the image is compatible with the configuration file used on the next switch reload. An error message is displayed if system boot parameters are set for incompatible image and configuration files.
5. After downgrading the software on the switch, perform the following steps:
   - Restore pre-AOS-W 6.5.4.13 flash backup from the file stored on the switch. Do not restore the AOS-W 6.5.4.13 flash backup file.
   - You do not need to reimport the WMS database or RF Plan data. However, if you have added changes to RF Plan in AOS-W 6.5.4.13, the changes do not appear in RF Plan in the downgraded AOS-W version.
   - If you installed any certificates while running AOS-W 6.5.4.13, you need to reinstall the certificates in the downgraded AOS-W version.

Downgrading Using the WebUI

The following section describes how to use the WebUI to downgrade the software on the switch.

1. If the saved preupgrade configuration file is on an external FTP/TFTP server, copy the file to the switch by navigating to the **Maintenance > File > Copy Files** page.
   a. For **Source Selection**, select FTP/TFTP server, and enter the IP address of the FTP/TFTP server and the name of the preupgrade 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 preupgrade configuration file by navigating to the **Maintenance > Controller > Boot Parameters** page.
   a. Select the saved preupgrade configuration file from the **Configuration File** drop-down list.
   b. Click **Apply**.
3. Determine the partition on which your previous software image is stored by navigating to the **Maintenance > Controller > Image Management** page. If there is no previous software image stored on your system partition, load it into the backup system partition (you cannot load a new image into the active system partition) by performing the following steps:
   a. Enter the FTP/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 preupgrade image file as the boot partition.
   b. Click **Apply**.
5. Navigate to the **Maintenance > Controller > Reboot Controller** page. Click **Continue**. The switch reboots after the countdown period.
6. When the boot process is complete, verify that the switch is using the correct software by navigating to the **Maintenance > Controller > Image Management** page.

Downgrading Using the CLI

The following section describes how to use the CLI to downgrade the software on the switch.

1. If the saved preupgrade 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 preupgrade configuration file.
   ```
   (host) # boot config-file   <backup configuration filename>
   ```
3. Execute the **show image version** command to view the partition on which your previous software image is stored. You cannot load a new image into the active system partition (the default boot).

In the following example, partition 1, the backup system partition, contains the backup release AOS-W 6.1.3.2. Partition 0, the default boot partition, contains the AOS-W 6.5.4.13 image.

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

Before You Call Technical Support

Before you place a call to Technical Support, follow these steps:

1. Provide a detailed network topology (including all the devices in the network between the user and the Alcatel-Lucent switch with IP addresses and Interface numbers if possible).
2. Provide the wireless device's make and model number, OS version (including any service packs or patches), wireless Network Interface Card (NIC) make and model number, wireless NIC's driver date and version, and the wireless NIC's configuration.
3. Provide the switch logs and output of the **show tech-support** command via the WebUI Maintenance tab or via the CLI (**tar logs tech-support**).
4. Provide the syslog file of the switch at the time of the problem. Alcatel-Lucent strongly recommends that you consider adding a syslog server if you do not already have one to capture logs from the switch.
5. Let the support person know if this is a new or existing installation. This helps the support team to determine the troubleshooting approach, depending on whether you have an outage in a network that worked in the past, a network configuration that has never worked, or a brand new installation.
6. Let the support person know if there are any recent changes in your network (external to the Alcatel-Lucent switch) or any recent changes to your switch and/or AP configuration. If there was a configuration change, list the exact configuration steps and commands used.
7. Provide the date and time (if possible) of when the problem first occurred. If the problem is reproducible, list the exact steps taken to re-create the problem.
8. Provide any wired or wireless sniffer traces taken during the time of the problem.
9. Provide the switch site access information, if possible.