AOS-W 6.4.4.23

Alcatel·Lucent
Enterprise

Release Notes

Contents

Revision History

The following table provides the revision history of this document.

Table 1: *Revision History*

Revision	Change Description
Revision 01	Initial release.

This AOS-W release notes includes the following topics:

For the list of terms, refer Glossary.

Important Points to Remember

This section describes the important points to remember before you upgrade the switch to this release of AOS-W.

AirGroup

Support for Wired Users

Starting from AOS-W 6.4.3.0, AirGroup does not support trusted wired users.

AP Settings Triggering a Radio Restart

If you modify the configuration of an AP, those changes take effect immediately; you do not need to reboot the switch or the AP for the changes to affect the current running configuration. Certain commands, however, automatically force the AP radio to restart.

Table 2: *Profile Settings in AOS-W 6.4.x*

Profile	Settings
802.11a/802.11g Radio Profile	■ Channel ■ Enable Channel Switch Announcement (CSA) ■ CSA Count ■ High throughput enable (radio) ■ Very high throughput enable (radio) ■ TurboQAM enable ■ Maximum distance (outdoor mesh setting) ■ Transmit EIRP ■ Advertise 802.11h Capabilities ■ Beacon Period/Beacon Regulate ■ Advertise 802.11d Capabilities
Virtual AP Profile	■ Virtual AP enable ■ Forward Mode ■ Remote-AP operation
SSID Profile	■ ESSID ■ Encryption ■ Enable Management Frame Protection ■ Require Management Frame Protection ■ Multiple Tx Replay Counters ■ Strict Spectralink Voice Protocol (SVP) ■ Wireless Multimedia (WMM) settings ● Wireless Multimedia (WMM) ● Wireless Multimedia U-APSD (WMM-UAPSD) Powersave ● WMM TSPEC Min Inactivity Interval ● Override DSCP mappings for WMM clients ● DSCP mapping for WMM voice AC ● DSCP mapping for WMM video AC ● DSCP mapping for WMM best-effort AC ● DSCP mapping for WMM background AC

Table 2: *Profile Settings in AOS-W 6.4.x*

Profile	Settings
High-throughput SSID Profile	■ High throughput enable (SSID) ■ 40 MHz channel usage ■ Very High throughput enable (SSID) ■ 80 MHz channel usage (VHT)
802.11r Profile	■ Advertise 802.11r Capability ■ 802.11r Mobility Domain ID ■ 802.11r R1 Key Duration ■ key-assignment (CLI only)
Hotspot 2.0 Profile	■ Advertise Hotspot 2.0 Capability ■ RADIUS Chargeable User Identity (RFC4372) ■ RADIUS Location Data (RFC5580)

Supported Browsers

The following browsers are officially supported for use with the Web User Interface (WebUI) in this release:

- 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 3: *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

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

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

AP-Platform

Support for Loop Protection

Starting from this release, the loop protect feature detects and avoids the formation of loops on the Ethernet ports of a Campus AP, Remote AP, or Mesh AP. The loop protect feature can be enabled on all APs that have multiple Ethernet ports and it supports tunnel, split-tunnel, and bridge modes.

The loop protection feature prevents the formation of loops when:

- An unmanaged switch is connected to one port of an AP and a loop forms in the unmanaged switch.
- The WAN port (port 0) and either of ports 1, 2, 3, or 4, if it exists, in an AP are connected to the same switch.
- Multiple ports in an AP are connected to an unmanaged switch.

The loop protection feature transmits a proprietary loop detection packet on one Ethernet port of an AP at the configured loop-protect interval (default value is 2 seconds). The loop protect feature transmits the loop detection packet without a VLAN tag irrespective of whether the Ethernet port of the AP is connected in access mode or trunk mode. That is, for trunk mode, loop protect is supported only in the native VLAN.

The Ethernet port of the AP that is shut down because of loop protection is marked with status **Loop-ERR**. A user can either recover the shutdown port from the managed device with manual intervention or enable automatic recovery mode and configure an automatic recovery interval. At the expiry of the automatic recovery interval, the **Loop-ERR** status of the Ethernet port is cleared and the Ethernet port is re-enabled automatically.

To prevent the downstream switch from dropping the loop detection packet, for example during broadcast storm state, if the AP takes longer time, or if the AP fails to detect a loop, a broadcast storm-control mechanism is provided as part of the loop protection feature. During broadcast-storm control, an AP counts the broadcast packets received on each of its Ethernet port and determines the packet rate in an interval. If the broadcast packet rate on one Ethernet port exceeds the configured threshold (default value is 2000 packets per second), the Ethernet port is shut down.

Configuring Loop Protection in the WebUI

The following procedure describes how to configure the loop protect feature:

1. Navigate to the **Configuration** > **WIRELESS** > **AP Configuration** page.
2. Select an AP group profile
3. In the selected AP group profile, navigate to **AP** > **Ethernet interface 1 port configuration** page.
4. Configure the loop protect parameters listed in the following table:

Table 4: *Loop Protect Parameters in AP Wired Port Profile*

Parameter	Description
Loop Protect Enable:	Enables loop protection on AP wired ports.
Loop Detection Interval:	Time, in seconds, to send loop detection packet. The supported range is 1 to 10 seconds and the default value is 2 seconds.
Storm Control Broadcast:	Enables storm control broadcast. If the number of broadcast packets per second on one port in the AP exceeds the configured threshold, the port is shutdown.
Storm Control Broadcast Threshold:	Storm control broadcast threshold in packets per second after which the port is shutdown. The default value is 2000 packets per second.
Auto Recovery Enable:	Enables automatic recovery of the port in the AP. After the automatic recovery, if the loop re-occurs, then the port is shutdown again.
Auto Recovery Interval:	Time, in seconds, to automatically recover the port in the AP. The supported range is 30 to 43200 seconds and the default value is 300 seconds.

Configuring Loop Protection in the CLI

The following procedure describes how to configure the loop protect feature:

```
(host) (config) #ap wired-port-profile <profile>
(host) (AP wired port profile "<profile>")#loop-protect-enable
(host) (AP wired port profile "<profile>")#loop-detection-interval <loop-detectioninterval>
(host) (AP wired port profile "<profile>")#auto-recovery-enable
(host) (AP wired port profile "<profile>")#auto-recovery-interval <auto-recoveryinterval>
(host) (AP wired port profile "<profile>")#storm-control-broadcast
(host) (AP wired port profile "<profile>")#storm-control-broadcast-threshold
```

The following CLI command displays the status of the loop protect parameters:

```
(host) #show ap wired-port-profile <profile>
AP wired port profile "<profile>"
-------------------------------
Loop Protect Enable                    Disabled
Loop Detection Interval                2
Storm Control Broadcast                Disabled
Storm Control Broadcast Threshold      2000
Auto Recovery Enable                   Disabled
Auto Recovery Interval                 300
```

The following CLI command manually recovers a port of an AP in loop error state:

```
(host) (config) #clear ap port ap-name <ap-name> <port>
```

Firewall Visibility

FW_AGG Sessions Message Enhancement

A new field, **client mac address**, is added to the FW_AGG sessions message table to establish a relationship between the station MAC address and the application details.

GRE

Allow Unknown Unicast Packets

Starting from AOS-W 6.4.4.23, the **bcmc-optimization allow-unknown-unicast** parameter is introduced in the **interface vlan** command. When the **bcmc-optimization allow-unknown-unicast** parameter is enabled, a switch floods unknown unicast packets.

The **bcmc-optimization allow-unknown-unicast** parameter is optional and can be enabled only if the **bcmc-optimization** parameter is enabled.

If both **bcmc-optimization** and **bcmc-optimization allow-unknown-unicast** parameters are disabled, the switch does not flood any broadcast, multicast, or unknown unicast packet.

If only the **bcmc-optimization** parameter is enabled, the switch drops all broadcast, multicast, and unknown unicast packets.

If both **bcmc-optimization** and **bcmc-optimization allow-unknown-unicast** parameters are enabled, the switch drops only broadcast and multicast packets and floods the unknown unicast packets.

The following CLI command allows unknown unicast packet:

```
(host) (config-subif) #bcmc-optimization allow-unknown-unicast
```

The following CLI command disallows unknown unicast packet:

```
(host) (config-subif) #no bcmc-optimization allow-unknown-unicast
```

Remote AP

Enhancements in USB Initialization of 4G/LTE Modem

AOS-W allows you to configure two AP Name (APN) during USB initialization of the 4G/LTE modem. While the first APN initiates the connection to obtain an IP address, the second APN sends and receives data. Use semicolon (;) as a delimiter to create two separate strings for the APN configurations in the following commands under the AP provisioning profile:

```
(host) (config) #ap provisioning-profile <profile-name>
(host) (Provisioning profile "<profile-name>") #usb-init <APN1-string>; <APN2-string>
```

Example

The following sample configuration includes the string values for two APN configurations:

```
(host) (config) #ap provisioning-profile default
(host) (Provisioning profile "default") #usb-init "AT+CGDCONT=1,\"IP\",\"APN1\";1,1,\"APN2\""
```

You must obtain the APN from your ISP and ensure that each APN entry follows the manufacturer's AT command reference.

Chapter 3
Regulatory Updates

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

Periodic regulatory changes require modifications to the regulatory channel list supported by an AP. To view a complete list of channels supported by an AP for a specific country domain, access the CLI and execute the **show ap allowed-channels country-code <country-code> ap-type <ap-model>** command.

For a complete list of countries certified with different AP models, refer to the respective DRT release notes at service.esd.alcatel-lucent.com.

The following DRT file version is part of this release:

- DRT-1.0_74885

This release includes a fix for **WPA and WPA2 Disassociation Vulnerability** documented in CVE-2019-15126. This vulnerability affects OAW-AP200 Series access points.

Also, the following issues are resolved in this release.

NOTE

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

Table 5: *Resolved Issues in AOS-W 6.4.4.23*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-118206 AOS-131986 AOS-195916	142106 160093	**Symptom:** A switch crashed due to low memory in the **Authentication** process. This issue is resolved by blocking certain facing scenarios that led to memory leak. **Scenario:** This issue was observed when a packet was sent to port 8082 of the switch. This issue was observed in switches running AOS-W 6.4.2.12 or later versions.	Base OS Security	All platforms	AOS-W 6.4.2.12
AOS-118439	142397	**Symptom:** IPv4 syslog messages were interpreted incorrectly because of an invalid timestamp format. The fix ensures that the correct syslog messages are interpreted. **Scenario:** The timestamp in the syslog message for IPv4 address included the year at the end, which was not according to the format defined in RFC-3164. This issue is not limited to any specific switch model or AOS-W release version.	Logging	All platforms	AOS-W 6.4.4.6
AOS-134412	163123	**Symptom:** The error log file in a switch repeatedly listed the **ERRS |ike| usec 0 ERRS |ike| timeout value is very small Sec 0** message. The fix ensures that the switch log file does not list the error message. **Scenario:** This issue occurred when a VPN connection was triggered with EAP-TLS. This issue was observed in switches running AOS-W 6.4.4.10 or later versions.	IPsec	All platforms	AOS-W 6.4.4.10

Table 5: *Resolved Issues in AOS-W 6.4.4.23*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-149309	182909	**Symptom:** An AP displayed incorrect ACL index value on the user datapath. The fix ensures that the correct value is displayed. **Scenario:** This issue was observed in APs connected to a stand-alone switch running AOS-W 6.4.0.0 or later versions.	AP Datapath	All platforms	AOS-W 6.5.1.9
AOS-155632	191489	**Symptom:** A switch crashed and rebooted unexpectedly. The log file listed the reason for this event as **Control Processor Kernel Panic**. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue occurred when IP options caused the **Datapath** process to crash. This issue was observed in switches running AOS-W 6.4.4.0 or later versions. **New Duplicates:** AOS-157337, AOS-157417, AOS-158610, AOS-158360, AOS-184786, AOS-186151, AOS-187156, AOS-187576, AOS-187752, AOS-187880, AOS-189198, AOS-189439, AOS-191458, AOS-191603, AOS-192748, AOS-193261, AOS-193272, AOS-193491, AOS-193997, AOS-194310, AOS-194588, AOS-194797, AOS-194817, AOS-196391, AOS-196952, AOS-197755, AOS-198457, AOS-198572, AOS-198833, AOS-198866, AOS-198868, AOS-198872, AOS-200100 **Old Duplicates:** 193793, 193945, 195645, 195329	Switch-Datapath	All platforms	AOS-W 6.5.4.0
AOS-192868	—	**Symptom:** The OV3600 graph for some clients displayed zero value. The fix ensures that the correct graph is displayed. **Scenario:** This issue occurred when the **CL_TX_DATA_BYTES_ TRANSMITTED** counter and the **CL_RX_DATA_BYTES** counter were decremented from **AMON_STATION_STATS_MESSAG**, and the wireless clients downloaded huge files from the wired side FTP Servers. This issue was observed in OAW-4030 switches running AOS-W 6.4.4.23 or later versions.	Air Management-IDS	OAW-4030 switches	AOS-W 6.5.4.13
AOS-193936 AOS-194470	—	**Symptom:** Some APs continuously displayed the error message **asap_ firewall_forward: br0, insufficient headroom, require 60, but 16,skb data length 60**. The fix ensures that the APs work as expected. **Scenario:** This issue was observed in APs running AOS-W 6.4.4.23.	AP Datapath	All platforms	AOS-W 6.5.4.7

Table 5: *Resolved Issues in AOS-W 6.4.4.23*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-194571	—	**Symptom:** Some wireless clients experienced **IEEE80211_IOCTL_ ARUBA_STA_STATS_64** call overflow like a 32-bit value that leads to counter reset. Updating the stats with correct 64 bit values resolved this issue. **Scenario:** This issue occurred when the correct 64 bit stats was not used for **IEEE80211_IOCTL_ARUBA_STA_STATS_64** call. This issue was observed in switches running AOS-W 6.4.4.23 or later versions.	AP-Wireless	All platforms	AOS-W 6.5.4.9
AOS-199119	—	**Symptom:** The IPv6 DNS address, 2001:4860:4860::8888 was not reachable from 33536 and higher source ports. The fix ensures that during MLD snooping packets are forwarded over port-channel also. **Scenario:** This issue occurred because UDP packets were treated as ICMPv6 packet and the packets were dropped. This issue was observed in switches running AOS-W 6.4.4.21 or later versions.	IPv6	All platforms	AOS-W 6.4.4.21
AOS-201951	—	**Symptom:** The **ISAKMPD** process went into busy state when the VIA or a Third Party VPN client tried to come up in a scale scenario. The fix ensures that IKE SA INIT packets are throttled at the starting to avoid the **ISAKMPD** process from going into a busy state continuously. **Scenario:** This issue occurred when the VIA or the Third Party VPN clients tried to establish a tunnel in a scale setup and experienced a delay in the authentication process. This issue was observed in switches running AOS-W 6.4.4.17 or later versions.	IPSec	All platforms	AOS-W 6.4.4.17
AOS-202195	—	**Symptom:** The **ISAKMPD** process crashed and rebooted unexpectedly. The fix ensures that the **ISAKMPD** process does not crash. **Scenario:** This issue occurred when VPN clients with a mix of **user-cert** and **eap-tls** authentication tried to establish a tunnel and got timed out due to a delay in the authentication process. This issue was observed in switches running AOS-W 6.4.4.17 or later versions.	IPSec	All platforms	AOS-W 6.4.4.17

This chapter describes the known issues and limitations identified in AOS-W 6.4.4.23.

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

Limitations in AOS-W 6.4.4.23

Following are the limitations observed in this release:

Base OS Security

AOS-W 6.4.4.23 currently does not support ASCOM device-type while performing device classification.

CLI

- AOS-126535: AOS-W 6.4.4.23 currently does not have any CLI command that provides the entire list of rogue APs. You can download a partial list of rogue APs from **Dashboard** > **Security** page in the WebUI.
- AOS-126389: The **show ap arm status** command output does not display **ARM history** and **ARM status** on 5 GHz radio. The channel changes are visible in the output of **ap debug radio stats** command.
- AOS-106974: The **Client Match Restriction timeout (sec)**, **Client Match Sticky client check SNR (dB)**, and **Client Match Sticky Min Signal** parameters under the **show rf arm-profile** command are inconsistent when compared to the corresponding configuration commands.
- AOS-110570: The **QOS-profile <profile name>** command is yet to be deprecated under AOS-W 6.4.x.x versions.

Switch-Platform

Alcatel-Lucent OWA-4005 switches do not allow you to specify a source address or interface (e.g. the loopback interface). This limitation does not allow the full functionality of unified management or monitoring of a device.

Station Management

The **Spoofed Deauth Blacklist** feature under **Configuration** > **Wireless** > **AP Configuration** page, or the **spoofed-deauth-blacklist** command does not allow blacklisting of clients.

UCC

A client device may run multiple UCC applications such as Lync, X-lite, Cisco soft phone etc., but the Alcatel-Lucent UCC solution supports only one UCC application per client device. It provides firewall, prioritization, and visibility services for the media sessions belonging to the UCC application that is registered first using the client device.

Known Issues in AOS-W 6.4.4.23

Following are the known issues observed in this release:

Table 6: *Known Issues in AOS-W 6.4.4.23*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-81973 AOS-88689	97030 105837	**Symptom:** Some bridge mode clients are unable to update **Roles**. **Scenario:** This issue occurs in a HA setup, when GSM channel object that should be deleted are in **REPLICATED** state. This causes the 802.11x authentication to be skipped when client re-connects. This issue is observed in switches running AOS-W 6.4.0.3 or later versions. **Workaround:** None.	Base OS Security	All platforms	AOS-W 6.4.0.3
AOS-86488 AOS-96071	102974 114831	**Symptom:** The **Authentication Manager** process crashes for bridge Captive Portal users. **Scenario:** This issue is observed when a reauthentication timer expires after the user table is emptied. This issue is observed in switches running AOS-W 6.4.0.3. **Workaround:** None.	XML API	All platforms	AOS-W 6.4.0.3
AOS-95455	114072	**Symptom:** Some switches display error message, **Auth GSM: DEV_ID_CACHE publish failed for mac**, as there are no free slots in the **dev_id_cache** GSM channel. **Scenario:** This issue is observed in switches running AOS-W 6.4.2.2 or later versions. **Workaround:** None.	Base OS Security	All platforms	AOS-W 6.4.2.2
AOS-96384 AOS-121104	115215 145811	**Symptom:** The **show ap spectrum channel-metrics ap-name** command output always displays the WiFi utility value as 0%. **Scenario:** This issue occurs when the AP operates on **Spectrum Monitor** mode. This issue is observed in APs running AOS-W 6.4.2.5 or later versions. **Workaround:** None.	Spectrum-Infrastructure	All platforms	AOS-W 6.4.2.5

Table 6: *Known Issues in AOS-W 6.4.4.23*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-96420 AOS-106521	115260 128209	**Symptom:** When an administrator tries to hard reboot a switch, it fails to reboot with the error message, **Not enough space on flash**. **Scenario:** This issue occurs due to a database file corruption. This issue is observed in switches running AOS-W 6.4.2.3 or later versions. **Workaround:** Contact Technical Support to remove the corrupted database file.	Switch-Platforms	All platforms	AOS-W 6.4.2.3
AOS-96856	115817	**Symptom:** A client witnesses unexpected runtime error in the **STM** process. The switch displays the **stm_sysctl_write_param, 10460, Error opening /proc/sys/dev/wifi0/active_voice_client : No such file or directory** error message. **Scenario:** This issue is observed in switches running AOS-W 6.4.2.6 or later versions. **Workaround:** None.	Station Management	All platforms	AOS-W 6.4.2.6
AOS-96993	115984	**Symptom:** The **WMS**, **STM**, and **Authentication** processes running on a switch crash unexpectedly. **Scenario:** This issue is observed in switches running AOS-W 6.4.1.0 or later versions. **Workaround:** None.	Switch-Platforms	All platforms	AOS-W 6.4.1.0
AOS-97746	116977	**Symptom:** Radius accounting stop is sent immediately after the accounting start. **Scenario:** This issue occurs when a bridge mode user roams from one AP to another AP. This issue is observed in switches running AOS-W 6.4.1.0. **Workaround:** None.	Base OS Security	All platforms	AOS-W 6.4.1.0
AOS-100066	120099	**Symptom:** The output of the **show airgroupservice** and **show airgroup vlan** command is not sorted. **Scenario:** This issue is observed in switches running AOS-W 6.4.2.6. **Workaround:** None.	AirGroup	All platforms	AOS-W 6.4.2.6

Table 6: *Known Issues in AOS-W 6.4.4.23*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-100169 AOS-139770 AOS-137716	120217 169889 167200	**Symptom:** The console logs and error logs of an AP display the **protocol 0000 is buggy, dev eth0 nh= (null) d=ca613052 t=ca613074** message. **Scenario:** This issue is observed in OAW-RAP155 and OAW-AP324 access points running AOS-W 6.4.4.0. **Workaround:** None.	AP-Platform	OAW-RAP155 and OAW-AP324 access points	AOS-W 6.4.4.0
AOS-102230	122797	**Symptom:** On configuring a Pre-Shared Key (PSK) for a High Availability (HA) group profile with a plus character, the switch converts the plus character to a blank space. **Scenario:** This issue occurs only when a PSK is configured using the WebUI. This issue is observed in switches running AOS-W 6.4.2.8 or later versions. **Workaround:** None.	WebUI	All platforms	AOS-W 6.4.2.8
AOS-102262 AOS-109632	122830 131827	**Symptom:** The **SAPD** process in an AP crashes and the AP reboots unexpectedly. **Scenario:** This issue occurs when the wireless driver unexpectedly generates a frame of size 0. This issue is observed in APs running AOS-W 6.4.4.0. **Workaround:** None.	AP-Platform	All platforms	AOS-W 6.4.4.0
AOS-102766	123400	**Symptom:** A client associates with an AP but does not communicate with it. **Scenario:** This issue is observed in OAW-AP215 access points running AOS-W 6.4.2.6. **Workaround:** None.	AP-Wireless	OAW-AP215 access points	AOS-W 6.4.2.6
AOS-102767	123401	**Symptom:** During AP reprovisioning, the logs indicate that an internal error related to AP regulatory, is encountered. **Scenario:** This issue occurs when the AP is reprovisioned from an older AP group (that may not exist on the switch) to a newer AP group. This issue is observed in switches running AOS-W 6.4.1.0 or later versions. **Workaround:** None.	AP Regulatory	All platforms	AOS-W 6.4.2.6

Table 6: *Known Issues in AOS-W 6.4.4.23*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-102818	123458	**Symptom:** A VoIP client receives an IP address from a wrong VLAN. **Scenario:** This issue occurs under the following scenarios: ■ When an AP fails to send LLDP-MED packets after receiving LLDP packets from the VoIP phone. ■ When a client that supports LLDP-MED is connected to the downlink Ethernet port of an AP. This issue is observed in APs running AOS-W 6.4.3.3. **Workaround:** None.	AP-Platform	All platforms	AOS-W 6.4.3.3
AOS-103500 AOS-125747	124275 151661	**Symptom:** All clients continue to obtain IP addresses from the same VLAN even though a RADIUS server VSA specifies a VLAN pool with multiple VLANs. **Scenario:** This issue occurs when a RADIUS server VSA overrides the virtual AP VLANs with a different VLAN pool that is configured with the even assignment type. This issue is observed in switches running AOS-W 6.4.2.6 or later versions. **Workaround:** Change the VLAN assignment type from **even** to **hash** using the following CLI command: `(host) (config) #vlan-name <name> assignment hash`	Station Management	All platforms	AOS-W 6.4.2.6
AOS-103875 AOS-103930	124767 124841	**Symptom:** Media traffic is not prioritized and call details are not visible for SIP calls on the UCC dashboard. **Scenario:** This issue occurs when large segmented SIP signaling messages are broken into multiple segments and delivered out of order. This issue is not limited to any specific switch model or AOS-W release version. **Workaround:** None.	UCC	All platforms	AOS-W 6.4.2.4
AOS-103946	124863	**Symptom:** Some switch nodes form a cluster group with VRRP IP and Wi-Fi clients cannot connect to an AP. **Scenario:** This issue occurs when the switch's VRRP IP is configured in the cluster group. This issue is observed in all platforms with cluster group-VRRP IP topology, running AOS-W 6.4.2.6 or later versions. **Workaround:** None.	AP-Platform	All AP Platforms	AOS-W 6.4.2.6

Table 6: *Known Issues in AOS-W 6.4.4.23*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-103960 AOS-108876 AOS-113674 AOS-116507 AOS-118740 AOS-141191	118740 124878 130917 136646 140035 171854	**Symptom:** When the **show running config** command is executed on the switch, the **Module AMAPI SNMP trap client is busy. Please try later** error message is displayed. **Scenario:** This issue occurs when bulk SNMP queries are executed on a switch. This issue is observed in switches running AOS-W 6.4.2.x, AOS-W 6.4.3.x, or AOS-W 6.4.4.x versions. **Workaround:** None.	SNMP	All platforms	AOS-W 6.4.3.5
AOS-104987	126176	**Symptom:** The LLDP requests from multiple clients triggers unnecessary wired authentication requests and the wired authentication requests fail. **Scenario:** This issue occurs when wired authentication is coupled with MAC authentication. This issue is observed in switches running AOS-W 6.4.2.4 or later versions. **Workaround:** None.	LLDP	All platforms	AOS-W 6.4.2.4
AOS-105090 AOS-109214	126328 131316	**Symptom:** Some clients receive the AMP alert, **Device Event: Event Type is Syslog and Syslog Severity >= Critical**. **Scenario:** This issue is observed in switches running AOS-W 6.4.2.12 or later versions. **Workaround:** None.	Logging	All platforms	AOS-W 6.4.2.12
AOS-106712	128457	**Symptom:** The **wlsxMeshNodeEntryChanged** trap generated by a switch does not have mesh link reset information. **Scenario:** This issue is observed in switches running AOS-W 6.4.3.1 or later versions. **Workaround:** None.	SNMP	All platforms	AOS-W 6.4.3.1
AOS-108888 AOS-147611	130931 180579	**Symptom:** The **Datapath** and **Authentication** processes running on a switch crash after the switch is upgraded. **Scenario:** This issue is observed in switches running AOS-W 6.4.4.16 or later versions. **Workaround:** None.	Switch-Datapath	All platforms	AOS-W 6.4.4.16

Table 6: *Known Issues in AOS-W 6.4.4.23*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-108917	130965	**Symptom:** The switch WebUI defaults the ACL queue priority value to **Low** even though it is set to **High**. However, the switch accepts the correct value when configured from the CLI. **Scenario:** This issue occurs only when the queue priority for an ACL is set to **High** from the WebUI. This issue is observed in switches running AOS-W 6.4.2.3 or later versions. **Workaround:** None.	WebUI	All platforms	AOS-W 6.4.2.3
AOS-108928	130981	**Symptom:** A switch crashes and reboots unexpectedly. The log file lists the reason for this as **datapath timeout**. **Scenario:** This issue occurs when the **copy** command has the **** characters at the end of the destination folder name. For example, AOS-W misinterprets the **** characters in the **copy flash: crash.tar ftp: 10.1.1.1.test-user \ArubaOS\\ crash.tar** command. This issue is observed in switches running AOS-W 6.4.4.0 or later versions. **Workaround:** None.	Switch-Platforms	All platforms	AOS-W 6.4.4.0
AOS-109282	131401	**Symptom:** The **RC_ERROR_PEER_DELETE_SA** error message is displayed even for successful IKE negotiations. **Scenario:** This issue is observed in switches running AOS-W 6.4.2.6 or later versions. **Workaround:** None.	Base OS Security	All platforms	AOS-W 6.4.2.6
AOS-109655	131857	**Symptom:** When the ToS value is set to **0** in the user role, the value does not take effect. **Scenario:** This issue is observed in switches running AOS-W 6.4.3.3 or later versions. **Workaround:** None.	Switch-Datapath	All platforms	AOS-W 6.4.3.3
AOS-110012 AOS-121852	132256 146837	**Symptom:** A JS error is displayed while trying to configure an **Override Rule** under **Configuration** > **Security** > **Access Control** > **Policies** tab in the WebUI. **Scenario:** This issue is observed in switches running AOS-W 6.4.4.8 or later versions. **Workaround:** None.	WebUI	All platforms	AOS-W 6.4.4.8

Table 6: *Known Issues in AOS-W 6.4.4.23*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-110394	132714	**Symptom:** When an administrator tries to add a static ARP entry, a switch displays the **Cannot add static ARP entry** error message. The log file lists the reason for this event as **Static ARP: too many entries (ipMapArpStaticEntryAdd)**. **Scenario:** This issue occurs because the static ARP counter continues to increment every time there is a change in the link status. This issue is observed in switches running AOS-W 6.4.3.4 or later versions. **Workaround:** None.	Switch-Platform	All platforms	AOS-W 6.4.3.4
AOS-110410	132734	**Symptom:** Some switches are unable to block torrent downloads on Bitcomet application using AppRF in ACLs. **Scenario:** This issue is observed in switches running AOS-W 6.4.3.0 or later versions. **Workaround:** None.	DPI	All platforms	AOS-W 6.4.3.6
AOS-112234 AOS-114137	134958 137206	**Symptom:** The **License Server IP** cannot be configured under **Network** > **Controller** > **Centralized License Management** > **Centralized Licenses** tab in the WebUI. **Scenario:** This issue is observed in switches running AOS-W 6.4.4.4 or later versions in a master-standby topology. **Workaround:** Use the CLI command to configure **License Server IP**.	WebUI	All platforms	AOS-W 6.4.4.4
AOS-112537 AOS-115030	135317 138269	**Symptom:** The returned SNMP value for OID **wlanAPBssidHTMode** does not specify the correct HT channel width for 80 Mhz, 80 + 80 Mhz, or 160 Mhz channels. **Scenario:** This issue is observed in switches running AOS-W 6.4.4.4 or later versions. **Workaround:** None.	SNMP	All platforms	AOS-W 6.4.4.4
AOS-112582 AOS-124422	135369 149880	**Symptom:** The **show gsm debug channel user** command displays incorrect role information on both UACs for bridge mode users. **Scenario:** This issue is observed in switches running AOS-W 6.4.2.6 or later versions. **Workaround:** None.	Base OS Security	All platforms	AOS-W 6.4.2.6

Table 6: *Known Issues in AOS-W 6.4.4.23*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-113240 AOS-124191	136147 149596	**Symptom:** Some APs are unable to discover IPv6 master using DHCPv6 option 60. **Scenario:** This issue is observed in APs running AOS-W 6.4.2.15 or later versions. **Workaround:** None.	AP-Platform	All platforms	AOS-W 6.4.2.15
AOS-113655 AOS-127753 AOS-128605	136623 154580 155690	**Symptom:** The status of Spectrum Monitor is active but displays error messages or does not display any content, when connected to the Spectrum UI. **Scenario:** This issue occurs due to a memory leak. This issue is observed in switches running AOS-W 6.3.x.x, AOS-W 6.4.x.x, or AOS-W 6.5.x.x versions. **Workaround:** None.	UI-Spectrum	All platforms	AOS-W 6.5.0.0
AOS-113955	136987	**Symptom:** A switch denies traffic after the AppRF ACL **appcategory peer-to-peer deny** classifies the DNS traffic as **thunder**. **Scenario:** This issue occurs when users try to connect to the 802.1x SSID **SecureTCC** with user-role set as **wlan-facstaff**. This issue is observed in switches running AOS-W 6.4.2.14 or later versions. **Workaround:** Remove **any any appcategory peer-to-peer deny** from the access-list.	Switch-Datapath	All platforms	AOS-W 6.4.2.14
AOS-114057	137108	**Symptom:** Some users are unable to log in to AOS-W VIA when they use special characters in the authentication password. **Scenario:** This issue is observed in switches running AOS-W 6.4.4.0 or later versions. **Workaround:** None.	RADIUS	All platforms	AOS-W 6.4.4.1
AOS-114654 AOS-168680	125154 137800	**Symptom:** An AP does not acquire a routable IPv6 address by monitoring the RA packets in the network. **Scenario:** This issue occurs when the **managed** flag is set in the RA packet. This issue is observed in APs running AOS-W 6.4.3.7 or later versions. **Workaround:** None.	AP-Wireless	All platforms	AOS-W 6.4.3.7
AOS-115062	138305	**Symptom:** A Remote AP fails to come up on a switch. **Scenario:** This issue occurs when the AP uses 4G uplink. This issue is observed in OAW-RAP3WN access points running AOS-W 6.4.3.7 or later versions. **Workaround:** None.	RAP-3G	OAW-RAP3WN access points	AOS-W 6.4.3.7

Table 6: *Known Issues in AOS-W 6.4.4.23*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-115173	138438	**Symptom:** The **Configuration** > **BRANCH** > **Smart Config** > **Networking** page in the WebUI does not provide an option to set the IP address of the user VLAN to **dhcp-client**. **Scenario:** This issue is observed in switches running AOS-W 6.4.4.6. **Workaround:** None.	WebUI	All platforms	AOS-W 6.4.4.6
AOS-115460 AOS-121750	138776 146701	**Symptom:** The **AP Poe Power Optimization** dropdown under **AP Configuration** > **AP** > **Provisioning** > **default** settings page cannot be configured. **Scenario:** This issue is observed in switches running AOS-W 6.4.4.5 or later versions. **Workaround:** None.	WebUI	All platforms	AOS-W 6.4.4.5
AOS-116437	139947	**Symptom:** Some wired clients that appear on the master through an untrusted tunnel and have AAA profile applied, record only the inbound traffic. **Scenario:** This issue occurs when the **packet-capture datapath mac <mac-address> all** command is executed and there are no packets that share the same source IP address with the clients. This issue is observed in switches running AOS-W 6.4.4.5 or later versions. **Workaround:** None.	Switch-Datapath	All platforms	AOS-W 6.4.4.5
AOS-116517	140049	**Symptom:** An AP takes longer than usual to boot. **Scenario:** This issue occurs when CPsec is enabled on a switch. This issue is observed in switches running AOS-W 6.4.3.3-FIPS. **Workaround:** None.	IPsec	All platforms	AOS-W 6.4.3.3-FIPS
AOS-117064	140721	**Symptom:** An AP reboots unexpectedly without providing any reboot information. **Scenario:** This issue is observed in OAW-AP103H access points running AOS-W 6.4.4.4 or later versions. **Workaround:** None.	AP-Platform	OAW-AP103H access points	AOS-W 6.4.4.4

Table 6: *Known Issues in AOS-W 6.4.4.23*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-117105	140779	**Symptom:** The SNMP enterprise-specific traps do not contain the enterprise trap OID. **Scenario:** This issue is observed in switches running AOS-W 6.4.4.5 or later versions. **Workaround:** None.	SNMP	All platforms	AOS-W 6.4.4.5
AOS-117129	140805	**Symptom:** The **Configuration** > **BRANCH** > **Smart config** > **Routing** > **DHCP** options page of the WebUI does not provide an option to configure multiple DHCP options for a DHCP pool. **Scenario:** This issue is observed in switches running AOS-W 6.4.3.6. **Workaround:** None.	WebUI	All platforms	AOS-W 6.4.3.6
AOS-117564	141310	**Symptom:** The **All WLAN Clients** tab on the acting master switch does not display any records for the clients that are connected. **Scenario:** This issue occurs because of the following reasons: ■ The LMS list is not relayed to apps if the role changes between master and standby switches. ■ There is no heartbeat activity on the master. This issue is observed in a Master-Standby topology and is not specific to any switch model or AOS-W release version. **Workaround:** None.	Master-Redundancy	All platforms	AOS-W 6.4.4.4
AOS-117783	141588	**Symptom:** The IPv6 router advertisements do not get optimized while forwarding to wireless clients. **Scenario:** This issue is observed in switches running AOS-W 6.4.4.3 or later versions. **Workaround:** None.	IPv6	All platforms	AOS-W 6.4.4.3
AOS-117871 AOS-111262 AOS-114809	131777 138008 141686	**Symptom:** A branch switch does not communicate with a master switch. **Scenario:** This issue occurs under the following scenarios: ■ The **NAT Outside** option is enabled in the **Configuration** > **BRANCH** > **Smart Config** > **Networking** page of the WebUI. ■ The IP address of the master switch is different from the public IP address. This issue is observed in branch switches running AOS-W 6.4.4.0 or later versions. **Workaround:** None.	Branch Switch	All platforms	AOS-W 6.4.4.0

Table 6: *Known Issues in AOS-W 6.4.4.23*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-117953	141791	**Symptom:** Video streaming for GLOP range of multicast addresses fails intermittently on different VLANs in a switch. **Scenario:** This issue is observed in switches running AOS-W 6.4.3.6 or later versions. **Workaround:** None.	WebUI	All platforms	AOS-W 6.4.3.6
AOS-117978 AOS-119196	141822 143282	**Symptom:** The process handling authentication requests crash due to a segmentation fault while sending RADIUS-accounting packets. **Scenario:** This issue occurs when you make the following changes to a AAA profile which is used by a client associated to the WLAN: ■ Modify the **RADIUS accounting server-group** assigned in the AAA profile to a different server-group. ■ Enable **multiple-server-accounting** which is originally disabled in the AAA profile. This issue is not limited to any specific switch model or AOS-W release version. **Workaround:** None.	RADIUS	All platforms	AOS-W 6.4.2.12
AOS-118437 AOS-128068	142395 154990	**Symptom:** The output of the **show boot history** command displays incorrect user information in the **Reboot Cause** message. However, the correct information is logged in the **Controller Reboot initiated** message before the reload. **Scenario:** This issue occurs because the switch incorrectly uses the current user information who logged in and executed the **show boot history** command for the **Reboot Cause** message. This issue is not limited to any specific switch model or AOS-W release version. **Workaround:** None.	Switch-Datapath	All platforms	AOS-W 6.4.3.7
AOS-118533	142514	**Symptom:** Some clients are unable to set IPv6 unique local address (ULA) as next-hop in static route. **Scenario:** This issue occurs when the kernel does not allow the addition of IPv6 ULA as nexthop in static route. This issue is observed in OWA-4005 switches running AOS-W 6.4.4.6 or later versions. **Workaround:** None.	IPv6	OWA-4005 switches	AOS-W 6.4.4.6

Table 6: *Known Issues in AOS-W 6.4.4.23*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-118623	142617	**Symptom:** An AP continues to reboot with the reason **Rebooting after provisioning**. **Scenario:** This issue occurs when an AP is provisioned with the **master clear** option and applied to the AP group. This results in the AP to reboot in a loop. This issue is observed in APs running AOS-W 6.4.4.6 or later versions. **Workaround:** None.	AP-Platform	All platforms	AOS-W 6.4.4.6
AOS-118682	142678	**Symptom:** Adding an NTP server to a switch causes the Remote APs to reconnect without notification and cannot recover many Instant AP VPNs. **Scenario:** This issue occurs when the NTP server tries to correct the time difference in the switch. This issue is not limited to any specific switch model or AOS-W release version. **Workaround:** Reboot the switch after configuring the NTP server.	IPsec	All platforms	AOS-W 6.4.2.13
AOS-118938	142975	**Symptom:** An AP stops forwarding traffic until it is rebooted. **Scenario:** This issue occurs in one of the following scenarios: ■ When virtual APs in tunnel mode and bridge mode are configured on the same AP. ■ When a tunnel mode virtual AP and a bridge mode wired AP are configured on the same AP. This issue is not limited to any specific AP model or AOS-W release version. **Workaround:** Configure different VLANs for the Virtual AP or Wired AP in tunnel mode and bridge mode.	AP Datapath	All platforms	AOS-W 6.4.4.6
AOS-119425	143566	**Symptom:** A switch displays the **Module authentication is busy. Please try later** error when the **show reference user-role <role-name>** command is executed. **Scenario:** This issue occurs when more than 212 entries exist for a given role in user derivation-rules or server-group derivation rules. This issue is observed in switches running AOS-W 6.4.2.16 in a master-local deployment. **Workaround:** None.	Configuration	All platforms	AOS-W 6.4.2.16

Table 6: *Known Issues in AOS-W 6.4.4.23*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-119819 AOS-125276	144039 150966	**Symptom:** The **Datapath** process in a switch crashes unexpectedly. **Scenario:** This issue occurs when a reputation-based deny ACL rule is configured and random URLs falling in the specific reputation range are sent to a switch. This issue is observed in switches running AOS-W 6.4.4.6. **Workaround:** None.	Switch-Datapath	All platforms	AOS-W 6.4.4.6
AOS-121097	145803	**Symptom:** A switch does not generate **wlsxNConnectionBackfromLocal** trap although the trap is enabled. **Scenario:** This issue occurs when a local switch is reloaded and the master switch does not generate the **wlsxNConnectionBackfromLocal** trap. This issue is observed in switches running AOS-W 6.4.4.6 or later versions. **Workaround:** None.	SNMP	All platforms	AOS-W 6.4.4.6
AOS-121851	146836	**Symptom:** While trying to apply the reordered policies for a new user role in the WebUI, the following error message is displayed: **Position 1 and 2 are reserved for Global and Role default session**. **Scenario:** This issue occurs when the **Apply** button is clicked after reordering the policies for a new role. This issue is not limited to any specific switch model or AOS-W release version. **Workaround:** None.	WebUI	All platforms	AOS-W 6.4.4.8
AOS-121917	146924	**Symptom:** The WIPS wizard does not load in a switch. **Scenario:** This issue is observed in switches running AOS-W 6.4.3.9-FIPS version. **Workaround:** None.	WebUI	All platforms	AOS-W 6.4.3.9-FIPS
AOS-122200	147300	**Symptom:** A switch fails to respond and reboots. **Scenario:** This issue is observed in switches running AOS-W 6.4.3.6 or later versions. **Workaround:** None.	Station Management	All platforms	AOS-W 6.4.3.6

Table 6: *Known Issues in AOS-W 6.4.4.23*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-122358 AOS-133091 AOS-140866 AOS-174935 AOS-175072 AOS-175903 AOS-176731	147483 161501 162368 163249 167972 171427 171581	**Symptom:** Multiple radio resets are observed on the **g** radio operating in AP and AM modes. **Scenario:** This issue occurs when scanning is enabled. This issue is observed in APs running AOS-W 6.4.4.0 or later versions. **Workaround:** None.	AP-Wireless	All platforms	AOS-W 6.5.0.0
AOS-122430 AOS-131021	147563 158837	**Symptom:** An AP shuts down unexpectedly and its power LED glows solid red. **Scenario:** This issue is observed in PoE enabled OAW-AP325 access points connected to switches running AOS-W 6.4.4.8 or later versions. **Workaround:** None.	BLE	OAW-AP325 access points	AOS-W 6.4.4.8
AOS-122794 AOS-131224 AOS-142597	147978 159105 173634	**Symptom:** An AP crashes and reboots unexpectedly. The log file lists the reason for this event as **Reboot caused by kernel panic: Rebooting the AP because of FW ASSERT**. **Scenario:** This issue occurs when the traffic from the AP is stopped and re-sent immediately. This issue is observed in APs running AOS-W 6.4.4.21. **Workaround:** None.	AP-Wireless	All platforms	AOS-W 6.4.4.21
AOS-123180 AOS-123885	148416 149211	**Symptom:** The **STM** process crashes due to memory corruption. **Scenario:** This issue occurs when there is an increase in the number of user roles. This results in the role bandwidth message not fitting into one PAPI message. This issue is observed in OAW-4550 switches running AOS-W 6.4.3.4 or later versions. **Workaround:** None.	AP-Platform	OAW-4550 switches	AOS-W 6.4.3.4
AOS-123307	148557	**Symptom:** Some clients observe a sudden increase in the number of DHCPv6 or Multicast messages from the APs. **Scenario:** This issue is observed in OAW-4650 switches running AOS-W 6.4.4.9 or later versions. **Workaround:** None.	AP-Platform	OAW-4650 switches	AOS-W 6.4.4.9

Table 6: *Known Issues in AOS-W 6.4.4.23*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-123661 AOS-128320 AOS-129313	148977 155343 156514	**Symptom:** A branch office switch randomly loses configuration updates from the master switch. **Scenario:** This issue occurs after a new license is sent from the master switch to the branch office switch. Thereafter, license-dependent configuration updates are not sent to the branch office switch. This issue is observed in branch office switches running AOS-W 6.4.4.8 or later versions. **Workaround:** None.	Licensing	All platforms	AOS-W 6.4.4.8
AOS-123701 AOS-139189	149019 169133	**Symptom:** The **USER_INFO AMON** message does not populate the IPv4 and IPv6 addresses even though the DHCP event is successful. **Scenario:** This issue is observed in switches running AOS-W 6.4.4.21. **Workaround:** None.	Base OS Security	All platforms	AOS-W 6.4.4.21
AOS-124189	149594	**Symptom:** The **AMON_USER_INFO_MESSAGE** message does not contain the user-agent information, whereas the SNMP user information has the user-agent information. **Scenario:** This issue is observed in a master-local topology when choosing AMON over SNMP in OV3600. This issue is observed in switches running AOS-W 6.4.3.9 or later versions. **Workaround:** Choose SNMP in OV3600.	Base OS Security	All platforms	AOS-W 6.4.3.9
AOS-124722	150245	**Symptom:** The **show user essid** command fails to execute. **Scenario:** This issue occurs when the ESSID contains one or more space characters. This issue is observed in switches running AOS-W 6.4.3.9. **Workaround:** None.	Base OS Security	All platforms	AOS-W 6.4.3.9
AOS-125100	150693	**Symptom:** The datapath route cache entry is not cleared when an L3 GRE tunnel is closed. **Scenario:** This issue occurs after a channel change is triggered on the APs due to radar detection. This issue is observed in switches running AOS-W 6.4.3.9. **Workaround:** None.	OSPF	All platforms	AOS-W 6.4.3.9

Table 6: *Known Issues in AOS-W 6.4.4.23*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-125432 AOS-128114 AOS-129538 AOS-132345 AOS-174959	151188 155048 156819 160570 162510	**Symptom:** An AP reboots unexpectedly. The log file lists the reason for this event as **FW ASSERT at _tx_send_setup_ppdu_params**. **Scenario:** This issue occurs in OAW-AP320 Series access points running AOS-W 6.4.4.9 or later versions. **Workaround:** None.	AP-Wireless	OAW-AP320 Series access points	AOS-W 6.4.4.9
AOS-125587	151416	**Symptom:** One of the FIPS KATs fails on booting up a switch. **Scenario:** This issue is observed in switches running AOS-W 6.4.4.21-FIPS or later versions. **Workaround:** None.	Base OS Security	All platforms	AOS-W 6.4.4.21-FIPS
AOS-125925	151995	**Symptom:** An AP crashes and reboots unexpectedly. The log file lists the reason for this event as **Reboot caused by kernel panic: Fatal exception**. **Scenario:** This issue occurs due to high CPU and memory utilization. This issue is observed in APs running AOS-W 6.4.4.8. **Workaround:** None.	Wi-Fi Driver	All platforms	AOS-W 6.4.4.8
AOS-126172 AOS-126208	152369 152427	**Symptom:** An AP stops responding and reboots. The log file lists the reason for this event as **soft lockup - CPU#0 stuck**. **Scenario:** This issue occurs due to a race condition between the virtual AP initialization and the LLDP PoE message. When the wireless driver of the AP tries to enable the virtual AP, it turns off the radio. This results in a soft lock. This issue is observed in OAW-AP200 Series, OAW-AP210 Series, OAW-AP220 Series, and OAW-AP270 Series access points running AOS-W 6.4.4.9 or later versions. **Workaround:** None.	AP-Platform	OAW-AP200 Series, OAW-AP210 Series, OAW-AP220 Series, and OAW-AP270 Series access points	AOS-W 6.4.4.9
AOS-126320 AOS-127713	152602 154513	**Symptom:** A master switch fails to delete the stale route entries of the branch office switch. When the entry is deleted manually, the switch displays the error, **ERROR: Cannot Delete Static Route**. **Scenario:** This issue occurs when the VLAN IP address of the branch office switch is changed and an updated CSV file (static IP address template) is uploaded on the master switch. This triggers the branch office switch to reboot, but fails to delete the stale route entries. This issue is observed in a master-branch office switch deployment with switches running AOS-W 6.4.4.8 or later versions. **Workaround:** None.	BOC	All platforms	AOS-W 6.4.4.8

Table 6: *Known Issues in AOS-W 6.4.4.23*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-126336 AOS-142989	152627 174134	**Symptom:** Multiple APs crash and reboot unexpectedly. The log file lists the reason for this event as **Kernel panic - not syncing: Rebooting the AP because of FW ASSERT**. **Scenario:** This issue occurs when the AP switches the spatial stream based on the client capabilities while transmitting or receiving data. This issue is observed in APs running AOS-W 6.4.4.16 or later versions. **Workaround:** None.	AP-Wireless	All platforms	AOS-W 6.4.4.16
AOS-126364	152672	**Symptom:** An AP generates multiple **asap_voip_log: netif_rx to stm failedwith ret : 1** messages. **Scenario:** This issue occurs when the AP generates unwanted log messages. This issue is observed in APs running AOS-W 6.4.4.10 or later versions. **Workaround:** None.	UCC	All platforms	AOS-W 6.4.4.10
AOS-126401 AOS-127493	152740 154234	**Symptom:** An increase in the memory consumption of the **authentication** process is observed when 802.11r clients are connected to the network. **Scenario:** The neighbor list entry associated with the roaming user is not released when the user entry times out or is deleted. This results in a memory leak of the **authentication** process in the switch. This issue is observed in OAW-4650 switches running AOS-W 6.4.3.10 or later versions. **Workaround:** None.	Base OS Security	OAW-4650 switches	AOS-W 6.4.3.10
AOS-126710 AOS-126711	153216 153217	**Symptom:** Multiple processes running on a switch terminate unexpectedly. **Scenario:** This issue occurs when an AAA server responds with more than one RADIUS-state attributes in the RADIUS packets. This issue is observed in switches running AOS-W 6.3.x.x, AOS-W 6.4.x.x, or AOS-W 6.5.x.x versions. **Workaround:** None.	Base OS Security	All platforms	AOS-W 6.4.3.6
AOS-126884	153463	**Symptom:** The AP channel utilization graph shows multiple breaks and is incomplete. **Scenario:** This issue is observed in switches running AOS-W 6.4.3.10 or later versions. **Workaround:** None.	AP-Wireless	All platforms	AOS-W 6.4.3.10

Table 6: *Known Issues in AOS-W 6.4.4.23*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-126926 AOS-128694	153520 155788	**Symptom:** The RF test for antenna connectivity with an AP always displays average SNR and success rate as either 0% or 9%. **Scenario:** This issue is observed in switches running AOS-W 6.4.4.9 or later versions. **Workaround:** None.	RF Troubleshooting	All platforms	AOS-W 6.4.4.9
AOS-127121 AOS-133318	153748 161770	**Symptom:** Mesh point does not connect with the correct mesh profile but uses recovery profile to connect instead. **Scenario:** This issue occurs when a mesh point roams to a portal on a different subnet. This issue is observed in switches running AOS-W 6.4.4.0 or later versions. **Workaround:** None.	Mesh	All platforms	AOS-W 6.4.3.7
AOS-127177	153824	**Symptom:** A switch fails to pass traffic when static IPsec routing with IP-to-IP IPsec tunnel is enabled. **Scenario:** This issue occurs when the route cache entry is installed with the wrong flag. This issue is observed in switches running AOS-W 6.4.4.10 or later versions. **Workaround:** None.	IPsec	All platforms	AOS-W 6.4.4.10
AOS-127353	154045	**Symptom:** Some APs keep sending the error message, **mini_httpd [806]: main: 1349: no more children available** to the switch syslog. This effects the control plane operations. **Scenario:** This issue occurs when a Wi-Fi client is disconnected from the AP while generating many HTTPS redirect requests. This issue is observed in APs running AOS-W 6.4.2.6 or later versions. **Workaround:** None.	AP-Platform	All platforms	AOS-W 6.4.2.6
AOS-127541 AOS-130229	154291 157755	**Symptom:** Although the user completes captive portal authentication and the appropriate role is set in the user table, the **web auth disabled** message is displayed when the user tries to login again. **Scenario:** This issue occurs when the user logs in again, and MAC authentication fails. This issue is observed in switches running AOS-W 6.3.1.23. **Workaround:** None.	Base OS Security	All platforms	AOS-W 6.3.1.23

Table 6: *Known Issues in AOS-W 6.4.4.23*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-127792 AOS-128115 AOS-134323	154628 155049 163007	**Symptom:** A switch incorrectly displays high memory utilization on the **Dashboard** > **Switches** > **Gauges** page of the WebUI. **Scenario:** This issue is observed in switches running AOS-W 6.4.3.7 or later versions. **Workaround:** None.	WebUI	All platforms	AOS-W 6.5.1.0
AOS-128201	155190	**Symptom:** A switch does not identify certain models of HPE DAC cables of 1 m, 3 m, or 7 m; for example, J9281B, J9285B, or J9536A. **Scenario:** This issue is observed in OAW-4x50 Series switches running AOS-W 6.4.3.9 or later versions. **Workaround:** None.	Switch-Platform	OAW-4x50 Series switches	AOS-W 6.4.3.9
AOS-128309	155332	**Symptom:** A mismatch in the number of APs in **Down** status is observed between the **Monitoring** > **Network Summary** page and the **Monitoring** > **All Access Points** page of the WebUI. **Scenario:** This issue occurs when an AP loses connectivity after it is changed from AP mode to AM mode. This issue is observed in switches running AOS-W 6.4.4.11 or later versions. **Workaround:** None.	WebUI	All platforms	AOS-W 6.4.4.11
AOS-128377	155419	**Symptom:** A switch crashes and reboots unexpectedly. The log file lists the reason for this issue as **Nanny rebooted machine - fpapps process failed**. **Scenario:** This issue is caused by a memory leak that occurs due to a certificate mismatch when APs try to establish a tunnel. This issue is observed in switches running AOS-W 6.4.3.6 or later versions. **Workaround:** None.	Switch-Platform	All platforms	AOS-W 6.4.3.6
AOS-128591	155672	**Symptom:** When the **snmpwalk** command is executed, the output does not reflect the configured Link Aggregation Identifier. **Scenario:** This issue is observed in switches running AOS-W 6.4.4.9 or later versions. **Workaround:** None.	SNMP	All platforms	AOS-W 6.4.4.9

Table 6: *Known Issues in AOS-W 6.4.4.23*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-128600	155685	**Symptom:** A master switch crashes and reboots unexpectedly. The log file lists the reason for this event as **Nanny rebooted machine - fpapps process died (Intent:cause:register 34:86:50:2) and crashed on fpapps module**. **Scenario:** This issue occurs when the **show datapath session dpi counters** command is executed. This issue is observed in switches running AOS-W 6.4.3.7 or later versions. **Workaround:** None.	Switch-Platform	All platforms	AOS-W 6.4.3.7
AOS-128792	155894	**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 6.4.4.16 in a master-local topology. **Workaround:** The suggested workarounds are: ■ Disable debug logs and syslog server. ■ Increase the advertisement interval. **New Duplicates:** AOS-127789, AOS-128621, AOS-129208, AOS-130788, AOS-133333, AOS-140532, AOS-141083, AOS-142791, AOS-148054 **Old Duplicates:** 154625, 155709, 156383, 158536, 161789, 170955, 171717, 173885, 181227	Switch-Platform	All platforms	AOS-W 6.4.4.16
AOS-129001	156124	**Symptom:** The VIA-VPN MOBIKE session establishment and termination generates negative values for user license usage. **Scenario:** This issue is observed in switches running AOS-W 6.4.4.10 or later versions. **Workaround:** None.	Base OS Security	All platforms	AOS-W 6.4.4.10
AOS-129609	156908	**Symptom:** An AP crashes and reboots unexpectedly. The log file lists the reason for this event as **Kernel panic - not syncing: softlockup: hung tasks**. **Scenario:** The issue occurs because the frames with sequence number 0 are inserted in the incorrect position. This issue is observed in APs running AOS-W 6.4.3.7 or later versions. **Workaround:** None.	AP-Wireless	All platforms	AOS-W 6.4.3.7

Table 6: *Known Issues in AOS-W 6.4.4.23*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-129902 AOS-140304	157301 170652	**Symptom:** Some APs reboot unexpectedly. The log file lists the reason for this event as **Rebooting the AP because of FW ASSERT**. **Scenario:** This issue occurs when a backup LMS is configured as a new LMS. This issue is observed in APs running AOS-W 6.4.4.16 or later versions. **Workaround:** None.	AP-Platform	All platforms	AOS-W 6.4.4.16
AOS-129929	157363	**Symptom:** An AP shuts down unexpectedly and its power LED glows solid red. **Scenario:** This issue is observed in POE enabled OAW-AP325 access points connected to a switch running AOS-W 6.4.4.8 or later versions. **Workaround:** None.	AP-Platform	OAW-AP325 access points	AOS-W 6.4.4.8
AOS-129930 AOS-150476	157364 184431	**Symptom:** Some APs display the error message, **Error opening /proc/sys/dev/wifi0/nchannel**, after booting up for the first time. **Scenario:** This issue occurs when the backup SSID tries to initialize the radio parameters when a new AP is booted up for the first time. This issue is observed in OAW-AP200 Series access points running AOS-W 6.4.4.9 or later versions. **Workaround:** None.	AP-Platform	OAW-AP200 Series access points	AOS-W 6.4.4.9
AOS-130226	157752	**Symptom:** Viber application traffic is not denied by AppRF as expected. **Scenario:** This issue occurs when a Viber call is initiated from one of the clients from an external network. This issue is observed in switches running AOS-W 6.4.4.10 or later versions. **Workaround:** None.	Switch-Datapath	All platforms	AOS-W 6.4.4.10
AOS-130444	158057	**Symptom:** The log file in a switch displays the **Unexpected fatal Configuration** error messages although there is no functionality impact. **Scenario:** This issue is observed in switches running AOS-W 6.4.3.7 or later versions. **Workaround:** None.	Configuration	All platforms	AOS-W 6.4.3.7

Table 6: *Known Issues in AOS-W 6.4.4.23*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-130790	158538	**Symptom:** A switch reboots continuously after upgrading from AOS-W 6.3.x.x version to AOS-W 6.4.x.x version. The log file lists the reason for this event as **Nanny rebooted machine - fpapps process died**. **Scenario:** This issue occurs due to an upgrade failure. This issue is observed in switches running AOS-W 6.4.4.12 or later versions. **Workaround:** None.	Switch-Platform	All platforms	AOS-W 6.4.4.12
AOS-130801	158550	**Symptom:** A user is unable to add RAP whitelist with special characters in the **full name** field under the **Configuration** > **AP Installation** > **Whitelist** WebUI page. **Scenario:** This issue is observed in switches running AOS-W 6.4.3.7 or later versions. **Workaround:** None.	WebUI	All platforms	AOS-W 6.4.3.7
AOS-130820	158576	**Symptom:** The word **Interference** is misspelled in the **Dashboard** mouse-over help for the **Channel Utilization** graph listed under the **Radios** table in the WebUI. **Scenario:** This issue is observed in switches running AOS-W 6.4.4.9 or later versions. **Workaround:** None.	WebUI	All platforms	AOS-W 6.4.4.9
AOS-130932 AOS-130933	158719 158720	**Symptom:** A switch crashes and reboots unexpectedly. The log file lists the reason for this event as **Reboot Cause: Datapath timeout (Intent:cause:register 56:86:50:2)**. **Scenario:** This issue occurs when two Ethernet ports of an AP are plugged into a switch which leads to a loop and datapath spike in the switch. This issue is observed in switches running AOS-W 6.4.3.6 or later versions. **Workaround:** None.	Switch-Platform	All platforms	AOS-W 6.4.3.6
AOS-131044 AOS-131815	158871 159851	**Symptom:** A switch reboots due to datapath crash. **Scenario:** This issue occurs due to a race condition. This issue is observed in OAW-4750 switches running AOS-W 6.4.4.0 or later versions. **Workaround:** None.	Switch-Datapath	OAW-4750 switches	AOS-W 6.4.4.0

Table 6: *Known Issues in AOS-W 6.4.4.23*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-131555 AOS-133514	159493 162023	**Symptom:** Multiple switches reboot unexpectedly. The log file lists the reason for this event as **datapath timeout**. **Scenario:** This issue occurs due to corrupt data entries in mobility multicast group table. This issue is observed in switches running AOS-W 6.4.4.12 or later versions. **Workaround:** None.	Switch-Datapath	All platforms	AOS-W 6.4.4.12
AOS-131586	159544	**Symptom:** Some switches display the error message, **Unexpected UCC runtime error at ucm_call_statistics_msg, 879, ucm-record lookup failed**. **Scenario:** This issue is observed in switches running AOS-W 6.4.4.12 or later versions. **Workaround:** None.	UCC	All platforms	AOS-W 6.4.4.12
AOS-131587	159547	**Symptom:** Some switches display the error message, **mDNS proxy runtime error at mdns_send_packet_pseudo_mcast 548 bad buff_len! 0**. **Scenario:** This issue occurs when an mdns packet is sent from another switch and the source cluster IP in the mDNS database cannot be found. This issue is observed in switches running AOS-W 6.4.4.12 or later versions. **Workaround:** None.	AirGroup	All platforms	AOS-W 6.4.4.12
AOS-131800 AOS-136100	159833 165229	**Symptom:** A user cannot enable or disable OSPF on a GRE tunnel interface. **Scenario:** This issue is observed in switches running AOS-W 6.4.3.4 or later versions. **Workaround:** None.	OSPF	All platforms	AOS-W 6.4.3.4
AOS-132155 AOS-142599	160323 173637	**Symptom:** Some APs crash and reboot unexpectedly. The log file lists the reason for this event as **Kernel panic - not syncing: Fatal exception**. **Scenario:** This issue is observed in OAW-AP320 Series access points running AOS-W 6.4.4.16 or later versions. **Workaround:** None.	AP-Wireless	OAW-AP320 Series access points	AOS-W 6.4.4.16

Table 6: *Known Issues in AOS-W 6.4.4.23*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-132315 AOS-130156 AOS-132374 AOS-146498	157662 160524 160615 178808	**Symptom:** The **Datapath** process crashes on a switch that acts as a standby switch. **Scenario:** This issue occurs due to corrupt data packets. This issue is observed in switches running AOS-W 6.4.4.0 or later versions. **Workaround:** None.	Switch-Datapath	All platforms	AOS-W 6.5.0.3
AOS-133436 AOS-147369	161922 180193	**Symptom:** Some AirGroup clients are unable to discover servers consistently. **Scenario:** This issue occurs as the switch keeps caching multiple entries of TXT records for wired AirGroup servers. This issue is observed on switches running AOS-W 6.4.4.0 or later versions. **Workaround:** None.	AirGroup	All platforms	AOS-W 6.5.1.4
AOS-133788 AOS-136900	162359 166229	**Symptom:** Some Instant AP clients that terminate on a switch are unable to pass traffic. Hence, clients are not assigned the required Instant AP user role. **Scenario:** This issue occurs when a custom AAA wired profile is applied on the port where the Instant AP is terminated. This issue is observed in OAW-4750 switches running AOS-W 6.4.4.11 or later versions. **Workaround**: Apply the default AAA wired profile on the port.	Remote AP	OAW-4750 switches	AOS-W 6.4.4.11
AOS-134947 AOS-137794 AOS-174465	159791 163802 167305	**Symptom:** An AP crashes and reboots unexpectedly. The log file lists the reason for this event as **Reboot Time and Cause: Reboot caused by kernel panic: Fatal exception in interrupt.** **Scenario:** This issue occurs when the IPsec tunnel is terminated while passing traffic. This issue is observed in OAW-AP215 access points running AOS-W 6.4.3.6 or later versions. **Workaround:** None.	VPN	OAW-AP215 access points	AOS-W 6.4.3.6
AOS-135483 AOS-145176	164476 177025	**Symptom:** The **show datapath session dpi** command output indicates that the non-FTP sessions are incorrectly classified as FTP sessions. **Scenario:** This issue occurs when DPI is enabled on switches running AOS-W 6.4.4.14 or later versions. **Workaround:** None.	Switch-Platform	All platforms	AOS-W 6.4.4.14

Table 6: *Known Issues in AOS-W 6.4.4.23*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-136453	165669	**Symptom:** A switch crashes and reboots unexpectedly. The log file lists the reason for this event as **Reboot Cause: Datapath timeout (Intent:cause:register 56:86:0:2c)**. **Scenario:** This issue is observed in switches running AOS-W 6.4.3.6 version. **Workaround:** None.	Switch-Platform	All platforms	AOS-W 6.4.3.6
AOS-136651	165908	**Symptom:** The kernel process in a switch crashes and the switch reboots unexpectedly. The log file lists the reason for this event as **control processor kernel panic**. **Scenario:** This issue is observed in switches running AOS-W 6.4.2.5 or later versions. **Workaround:** None. **New Duplicates:** AOS-140008, AOS-140614, AOS-142405, AOS-143136, AOS-143172, AOS-143582, AOS-143656, AOS-145264, AOS-145491, AOS-145643, AOS-146130, AOS-147592, AOS-147717, AOS-148015, AOS-149849, AOS-151349, AOS-152349, AOS-152535, AOS-152641, AOS-153358, AOS-156569, AOS-156881, AOS-158026, AOS-182050, AOS-183067, AOS-185346, AOS-185700 **Old Duplicates:** 170224, 171074, 173372, 174322, 174370, 174917, 175009, 177151, 177457, 177662, 178307, 180558, 180741, 181173, 183588, 185596, 186993, 187232, 187418, 188367, 192790, 193202, 194859	Switch-Platform	All platforms	AOS-W 6.4.2.5
AOS-137637 AOS-145111 AOS-150659	167111 176946 184674	**Symptom:** A few clients are unable to pass traffic although they receive the IP address from the correct VLAN. **Scenario:** This issue occurs when the netdestination configurations are updated. This issue is observed in switches running AOS-W 6.4.4.9 or later versions. **Workaround:** None.	Base OS Security	All platforms	AOS-W 6.4.4.9
AOS-138608	168363	**Symptom:** A few clients experience packet loss due to high datapath utilization in the CPU. **Scenario:** This issue is observed in OAW-4750 switches running AOS-W 6.4.3.6. **Workaround:** None.	Switch-Datapath	OAW-4750 switches	AOS-W 6.4.3.6

Table 6: *Known Issues in AOS-W 6.4.4.23*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-138799	168587	**Symptom:** An AP shows incorrect High Availability (HA) information and clients lose connectivity. **Scenario:** This issue occurs during HA failover when an AP does not receive a failover response from the standby switch. This issue is observed in APs running AOS-W 6.4.4.9 or later versions. **Workaround:** Reboot the AP.	AP-Platform	All platforms	AOS-W 6.4.4.9
AOS-138801 AOS-153250	168590 188228	**Symptom:** Some switches unexpectedly display many error messages, when an unsupported AP tries to connect to the switch. **Scenario:** This issue is observed in switches running AOS-W 6.4.4.21. **Workaround:** None.	AP-Platform	All platforms	AOS-W 6.4.4.21
AOS-138831	168634	**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 occurs after a switch is upgraded. This issue is observed in switches running AOS-W 6.4.4.15. **Workaround:** None.	Switch-Datapath	All platforms	AOS-W 6.4.4.15
AOS-138850 AOS-139737	168654 169843	**Symptom:** The **show datapath session table** command does not display the CPU ID. **Scenario:** This issue is observed in switches running AOS-W 6.4.4.21. **Workaround:** None.	Switch-Datapath	All platforms	AOS-W 6.4.4.21
AOS-138942 AOS-145229 AOS-146400	168795 177092 178670	**Symptom:** A WebCC URL cloud lookup in a switch fails. The log file lists the reason for the event as **<ERRS> |web_cc| web_cc_ callback: URL lookup failed**. **Scenario:** This issue occurs when WebCC is enabled on switches running AOS-W 6.4.4.16 or later versions. **Workaround:** None.	WebCC	All platforms	AOS-W 6.4.4.16
AOS-139079 AOS-139912 AOS-142606 AOS-143176 AOS-143647 AOS-152516	168984 170072 173647 174375 174998 187213	**Symptom:** A switch fails to update the syslog server. **Scenario:** This issue occurs because the syslog file becomes huge due to excess and incorrect logging from the switch. This issue is observed in switches running AOS-W 6.4.4.13 or later versions. **Workaround:** None.	Switch-Platform	All platforms	AOS-W 6.4.4.13

Table 6: *Known Issues in AOS-W 6.4.4.23*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-139604	169664	**Symptom:** A switch crashes and reboots unexpectedly. The log file lists the reason for this event as **Datapath timeout (Intent:cause:register 56:86:50)**. **Scenario:** This issue is observed in switches running AOS-W 6.4.2.16 or later versions. **Workaround:** None.	Switch-Platform	All platforms	AOS-W 6.4.2.16
AOS-139671	169749	**Symptom:** Some clients are unable to connect to 5 GHz radio on some APs. **Scenario:** This issue occurs because radio 0 does not transmit traffic. This issue is observed in OAW-AP325 access points running AOS-W 6.4.4.13 or later versions. **Workaround:** None.	AP-Wireless	OAW-AP325 access points	AOS-W 6.4.4.13
AOS-135373 AOS-158456	164342 195462	**Symptom:** A client does not associate with an AP. The log file lists the reason for this event as **Denied; AP Disable Timerange active**. **Scenario:** This issue is observed in switches running AOS-W 6.4.4.10 or later versions. **Workaround:** None.	Base OS Security	All platforms	AOS-W 6.4.4.10
AOS-140431	170813	**Symptom:** Some clients fail to associate with an 802.1X SSID after an AP fails over to the LMS from the backup LMS. **Scenario:** This issue occurs when 802.11r configuration is enabled on the backup LMS but not on the LMS. This issue is not limited to any specific switch model or AOS-W release version. **Workaround:** Ensure that the status of the 802.11r configuration is the same, either enabled or disabled, on both LMS and backup LMS.	AP-Platform	All platforms	AOS-W 6.4.4.16
AOS-141413 AOS-150894 AOS-157485	172149 184985 194055	**Symptom:** A switch crashes and reboots unexpectedly. The log file lists the reason for this event as **Reboot Cause: Kernel Panic (Intent:cause:register 12:86:f0:2)**. **Scenario:** This issue occurs when a DHCP pool is created. This issue is observed in OAW-4x50 Series switches running AOS-W 6.4.4.0 or later versions. **Workaround:** None	Switch-Platform	OAW-4x50 Series switches	AOS-W 6.4.4.15

Table 6: *Known Issues in AOS-W 6.4.4.23*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-144515	176105	**Symptom:** The configuration of an AP is lost and the AP reboots repeatedly. **Scenario:** This issue occurs due to a missing boot environment configuration. This issue is observed in OAW-AP205 access points running AOS-W 6.4.3.5. **Workaround:** None.	AP-Platform	OAW-AP205 access points	AOS-W 6.4.3.5
AOS-144669	176322	**Symptom:** An AP receives the IP address from an incorrect VLAN although the VLAN is changed through device-profile on the switch. **Scenario:** This issue occurs because the switch VLAN configuration does not change before the AP sends the DHCP information. This issue is observed in APs running AOS-W 6.4.4.6 or later versions. **Workaround:** None.	AP-Platform	All platforms	AOS-W 6.4.4.6
AOS-144968	176742	**Symptom:** The 5 GHz Tx power is lower than the maximum EIRP in an AP. **Scenario:** This issue occurs when a user configures the **min-tx-power** parameter in the **rf arm-profile** command and issues the **show ap bss-table** command to view the current EIRP value. This issue is observed in APs running AOS-W 6.4.4.0 or later versions. **Workaround:** None.	AP-Wireless	All platforms	AOS-W 6.4.4.0
AOS-145006 AOS-147868	176803 180975	**Symptom:** A switch dashboard does not display RF statistics or displays incomplete RF statistics of some APs. **Scenario:** This occurs when an AP truncates the client statistics. This issue is observed in switches running AOS-W 6.4.4.16 or later versions. **Workaround:** None.	Switch-Platform	All platforms	AOS-W 6.4.4.16
AOS-145018 AOS-173732	156127 176815	**Symptom:** The **STM** process running in a switch crashes unexpectedly. **Scenario:** This issue occurs when the switch is running low on memory. This issue is observed in OAW-6000 switches running AOS-W 6.4.4.9 or later versions. **Workaround:** None.	AirGroup	OAW-6000 switches	AOS-W 6.4.4.9

Table 6: *Known Issues in AOS-W 6.4.4.23*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-145463	177420	**Symptom:** The HTTP Strict Transport Security (HSTS) header is missing in HTTP response. **Scenario:** This issue is observed in switches running AOS-W 6.4.4.16 or later versions. **Workaround:** None.	Web Server	All platforms	AOS-W 6.4.4.16
AOS-146050 AOS-147029 AOS-185609	178182 179612	**Symptom:** A user experiences intermittent Skype call drops. **Scenario:** This issue occurs when an AP stops transmitting packets for a few seconds to track power save status. This issue is observed in APs running AOS-W 6.4.4.0 or later versions. **Workaround:** None.	AP-Wireless	All platforms	AOS-W 6.5.1.9
AOS-146248 AOS-146886 AOS-147357 AOS-147676 AOS-148060 AOS-150611 AOS-150664 AOS-153393	178462 179319 180173 180667 181235 184615 184679 188406	**Symptom:** The **show memory debug** command does not include the **memory available** column. **Scenario:** This issue is observed in switches running AOS-W 6.4.4.16 or later versions. **Workaround:** None.	Switch-Platform	All platforms	AOS-W 6.4.4.16
AOS-147344 AOS-147667 AOS-147792 AOS-153417	180146 180657 180855 188443	**Symptom:** Some clients fail RADIUS authentication when termination is enabled on a switch. **Scenario:** This issue occurs when Linux clients upgrade to Ubuntu 18.0.14 version. This issue is observed in switches running AOS-W 6.4.4.11 or later versions. **Workaround:** None.	802.1X	All platforms	AOS-W 6.4.4.11
AOS-148604	181972	**Symptom:** Some APs are unable to connect to the network on the 5 GHz radio. **Scenario:** This issue is observed in APs running AOS-W 6.4.4.8 or later versions. **Workaround:** None.	Mesh	All platforms	AOS-W 6.4.4.8
AOS-154853	190321	**Symptom:** An AP resolves the IP address of an Aeroscout Location Engine server in the reverse direction. **Scenario:** This issue is observed in APs running AOS-W 6.4.4.16 or later versions. **Workaround:** None.	Air Management - IDS	All platforms	AOS-W 6.4.4.16

Table 6: *Known Issues in AOS-W 6.4.4.23*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-154994 AOS-183903	190518	**Symptom:** When the client device sends an authentication frame after it is already authenticated, its association status is cleared but an incorrect error message is displayed. **Scenario:** This issue is observed in APs running AOS-W 6.4.4.20 or later versions. **Workaround:**	AP-Wireless	All platforms	AOS-W 6.4.4.20
AOS-156027 AOS-157576 AOS-158392 AOS-158580 AOS-182573 AOS-182796 AOS-183467 AOS-183992 AOS-184344 AOS-184510	192034 194197 195377 195607	**Symptom:** Some APs stop broadcasting on 2.4 GHz radios. **Scenario:** This issue is observed in OAW-AP105 access points connected to OAW-4650 switches running AOS-W 6.4.4.19 or later versions. **Workaround:** None.	AP-Wireless	OAW-AP105 access points	AOS-W 6.4.4.19
AOS-185920 AOS-185921	—	**Symptom:** A switch crashes and reboots unexpectedly. The log file lists the reason for this event as **Nanny Rebooted Machine – fpapps process died and crashed on pubsub, cfgm, syslogdwrap, aaa and nanny module**. **Scenario:** If the CPSec APs keep re-trying to terminate on the switch for which CPSec Whitelist DB entry is not present, or not-approved on the switch, then the memory leak in the ISAKMPD module leads to switch reboot subsequently. This issue is observed in switches running AOS-W 6.4.4.0 or later versions. **Workaround:** Correct the whitelist database entries (corresponding to re-trying CPSec APs) on the switch so that tunnel establishment does not fail for the CPSec APs and memory leak does not happen.	IPsec	All platforms	AOS-W 6.4.4.16

Table 6: *Known Issues in AOS-W 6.4.4.23*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-187036	—	**Symptom:** An AP is stuck in an upgrade loop and does not come up. **Scenario:** This issue is observed in APs running AOS-W 6.4.4.16 or later versions. **Workaround:** None.	AP-Platform	All platforms	AOS-W 6.4.4.16
AOS-187906	—	**Symptom:** The AP image miss-match logs are classified as debugging logs instead of error logs. **Scenario:** This issue is observed in APs running AOS-W 6.4.4.16 or later versions. **Workaround:** None.	AP-Platform	All platforms	AOS-W 6.4.4.16
AOS-198671	—	**Symptom:** An AP does not send authentication response frames to the client's authentication request. **Scenario:** This issue occurs due to radar detection causing deferred channel changes, when the CSA is enabled. This issue is observed in OAW-AP135 access points running AOS-W 6.4.4.21 or later versions. **Workaround:** The suggested workarounds are: ■ Reboot the AP. ■ Avoid using DFS channels. ■ Disable CSA.	AP-Wireless	OAW-AP135 access points	AOS-W 6.4.4.21

This chapter details software upgrade procedures. It is recommend 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

- AP LLDP profile is not supported on OAW-AP120 Series access points in AOS-W 6.4.x.
- Starting from AOS-W 6.3.1.0, the local file upgrade option in the OAW-4306 Series switch Web UIs have been disabled.
- AOS-W 6.4.x does not allow you to 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/alias
  - destination IP/alias
  - proto-port/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 below 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)#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
```

- AOS-W 6.4.x supports only the newer MIPS switches (OAW-4306 Series, OAW-4504XM, OAW-4604, OAW-4704, OAW-M3, OAW-40xx Series, and OAW-4x50 Series). Legacy PPC switches (OAW-4302, OAW-4308, OAW-4324, SC1/SC2) are not supported. Do not upgrade to AOS-W 6.4.x if your deployment contains a mix of MIPS and PPC switches in a master-local setup.
- 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 54.

GRE Tunnel-Type Requirements

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

- AOS-W 6.4.4.0 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.
- 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 you may require. For a detailed description of these new license modules, refer to the "Software Licenses" chapter in the *AOS-W 6.4.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 the 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.
- Do not proceed with an upgrade unless 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. 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 switch to a desired location. Deleted the following files 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 53 to copy the **crash.tar** file to an external server. 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 53 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 53 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 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 **Configuration**.
2. Click **Save Configuration**.
3. Navigate to the **Maintenance > File > Backup Flash** page.
4. Click **Create Backup** to backup 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

To restore the backup file to the flash memory, navigate to the:

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

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

   ```
   (host) #backup flash
   Please wait while we take the flash backup.......
   File flashbackup.tar.gz created successfully on flash.
   Please copy it out of the controller and delete it when done.
   ```

3. Execute either of the following command to transfer the flash backup file to an external server or storage device.

```
(host) copy flash: flashbackup.tar.gz ftp: <ftphost> <ftpusername> <ftpuserpassword> <remote directory>
(host) copy flash: flashbackup.tar.gz usb: partition <partition-number>
```

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

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

4. Execute the following command to untar and extract the **flashbackup.tar.gz** file to the flash memory.

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

Upgrading in a Multi-switch Network

In a multi-switch network, upgrade your switch based on the switch type (master or local). Back up your switch before upgrading, as described in, Backing Up Critical Data on page 53.

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 software 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. Ensure that the master and local switches are upgraded to the AOS-W version.

Upgrading AOS-W 6.4.4.x-FIPS

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 or CLI.

CAUTION

Ensure that there is enough free memory and flash space on your switch. For details, see Memory Requirements on page 52.

NOTE

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.

Upgrading From an Older Version of AOS-W

Before you begin, verify the version of AOS-W currently running on your switch. If you are running one of the following versions of AOS-W, you must download and upgrade to an interim version of AOS-W.

NOTE

When upgrading from an existing AOS-W 6.4.4.x release, set AMON packet size manually to a desired value. The packet size is increased to 32K by default for fresh installations of AOS-W 6.4.4.x.

- For switches running AOS-W 5.0.x versions earlier than AOS-W 5.0.3.1, download and install the latest version of AOS-W 5.0.4.x.
- For switches running AOS-W 6.0.0.0 or 6.0.0.1 versions, download and install the latest version of AOS-W 6.0.1.x.

Follow step 2 to step 11 of the procedure described in Upgrading AOS-W on page 55 to install the interim version of AOS-W, and then repeat steps 1 through 11 of the procedure to download and install AOS-W.

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

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 6.4.4.23 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.

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 > Switch > 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. Click the nonboot partition from the **Partition to Upgrade** radio button.
8. Click **Yes** in the **Reboot Switch After Upgrade** radio button to automatically reboot after upgrading. Click **No**, if you do not want the switch to reboot immediately.

Note that the upgrade will not take effect until you reboot the switch.

9. Click **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 53 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 52.

Upgrading From an Older Version of AOS-W

Before you begin, verify the version of AOS-W currently running on your switch. For more information, see Upgrading AOS-W on page 55.

Follow steps 2 through 7 of the procedure described in Upgrading AOS-W on page 55 to install the interim version of AOS-W, and then repeat steps 1 through 7 of the procedure to download and install AOS-W 6.4.4.23.

Upgrading From a Recent Version of AOS-W

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

- AOS-W 3.4.4.1 or later version of AOS-W
- AOS-W 5.0.3.1 or the latest version of AOS-W 5.0.x
- AOS-W 6.0.1.0 or later versions 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 6.4.4.23 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**.
   ```
   (host) #show image version
   ```
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-4010, OAW-4030, and OAW-4x50 Series switches.

6. Execute the **show image version** command to verify that the new image is loaded.
   ```
   (host)# show image version
   ```
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 53 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.

If you upgraded from AOS-W 3.3.x to AOS-W 5.0, the upgrade script encrypts the internal database. New entries created in AOS-W 6.4.4.23 are lost after the downgrade (this warning does not apply to upgrades from AOS-W 3.4.x to AOS-W 6.1).

If you downgrade to a pre-6.1 configuration that was not previously saved, some parts of your deployment may not work as they previously did. For example, when downgrading from AOS-W 6.4.4.23 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 software version, you must perform the following steps:

1. Back up your switch. For details, see Backing Up Critical Data on page 53.
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 partition that contains the pre-upgrade AOS-W version.

   When you specify a boot partition or copy an image file to a system partition, the switch checks to ensure that the image is compatible with the configuration file. An error message is displayed if the boot parameters are incompatible with the AOS-W version and configuration files.
5. After switching the boot partition, perform the following steps:
   - Restore pre-upgrade flash backup from the file stored on the 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.

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/TFTP server, copy the file to the switch by navigating to the **Maintenance > File > Copy Files** page.
   a. For **Source Selection**, select FTP server or TFTP server, and enter the IP address of the FTP server 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 server 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 lick **Continue**.
   The switch reboots after the countdown.
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 server 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 image is stored.

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

```
(host)# 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 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 the 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.

Appendix a
Acronyms and Abbreviations

The following table lists the acronyms and abbreviations used in Aruba documents.

Table 7: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
3G	Third Generation of Wireless Mobile Telecommunications Technology
4G	Fourth Generation of Wireless Mobile Telecommunications Technology
AAA	Authentication, Authorization, and Accounting
ABR	Area Border Router
AC	Access Category
ACC	Advanced Cellular Coexistence
ACE	Access Control Entry
ACI	Adjacent Channel interference
ACL	Access Control List
AD	Active Directory
ADO	Active X Data Objects
ADP	Aruba Discovery Protocol
AES	Advanced Encryption Standard
AIFSN	Arbitrary Inter-frame Space Number
ALE	Analytics and Location Engine

Table 7: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
ALG	Application Layer Gateway
AM	Air Monitor
AMON	Advanced Monitoring
AMP	AirWave Management Platform
A-MPDU	Aggregate MAC Protocol Data Unit
A-MSDU	Aggregate MAC Service Data Unit
ANQP	Access Network Query Protocol
ANSI	American National Standards Institute
AP	Access Point
API	Application Programming Interface
ARM	Adaptive Radio Management
ARP	Address Resolution Protocol
AVF	AntiVirus Firewall
BCMC	Broadcast-Multicast
BGP	Border Gateway protocol
BLE	Bluetooth Low Energy
BMC	Beacon Management Console
BPDU	Bridge Protocol Data Unit
BRAS	Broadband Remote Access Server

Table 7: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
BRE	Basic Regular Expression
BSS	Basic Service Set
BSSID	Basic Service Set Identifier
BYOD	Bring Your Own Device
CA	Certification Authority
CAC	Call Admission Control
CALEA	Communications Assistance for Law Enforcement Act
CAP	Campus AP
CCA	Clear Channel Assessment
CDP	Cisco Discovery Protocol
CDR	Call Detail Records
CEF	Common Event Format
CGI	Common Gateway Interface
CHAP	Challenge Handshake Authentication Protocol
CIDR	Classless Inter-Domain Routing
CLI	Command-Line Interface
CN	Common Name
CoA	Change of Authorization
CoS	Class of Service
CPE	Customer Premises Equipment

Table 7: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
CPsec	Control Plane Security
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
CRL	Certificate Revocation List
CSA	Channel Switch Announcement
CSMA/CA	Carrier Sense Multiple Access / Collision Avoidance
CSR	Certificate Signing Request
CSV	Comma Separated Values
CTS	Clear to Send
CW	Contention Window
DAS	Distributed Antenna System
dB	Decibel
dBm	Decibel Milliwatt
DCB	Data Center Bridging
DCE	Data Communication Equipment
DCF	Distributed Coordination Function
DDMO	Distributed Dynamic Multicast Optimization
DES	Data Encryption Standard
DFS	Dynamic Frequency Selection

Table 7: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
DFT	Discreet Fourier Transform
DHCP	Dynamic Host Configuration Protocol
DLNA	Digital Living Network Alliance
DMO	Dynamic Multicast optimization
DN	Distinguished Name
DNS	Domain Name System
DOCSIS	Data over Cable Service Interface Specification
DoS	Denial of Service
DPD	Dead Peer Detection
DPI	Deep Packet Inspection
DR	Designated Router
DRT	Downloadable Regulatory Table
DS	Differentiated Services
DSCP	Differentiated Services Code Point
DSSS	Direct Sequence Spread Spectrum
DST	Daylight Saving Time
DTE	Data Terminal Equipment
DTIM	Delivery Traffic Indication Message
DTLS	Datagram Transport Layer Security
DU	Data Unit

Table 7: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
EAP	Extensible Authentication Protocol
EAP-FAST	EAP-Flexible Authentication Secure Tunnel
EAP-GTC	EAP-Generic Token Card
EAP-MD5	EAP-Method Digest 5
EAP-MSCHAP EAP-MSCHAPv2	EAP-Microsoft Challenge Handshake Authentication Protocol
EAPoL	EAP over LAN
EAPoUDP	EAP over UDP
EAP-PEAP	EAP-Protected EAP
EAP-PWD	EAP-Password
EAP-TLS	EAP-Transport Layer Security
EAP-TTLS	EAP-Tunneled Transport Layer Security
ECC	Elliptical Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
EIGRP	Enhanced Interior Gateway Routing Protocol
EIRP	Effective Isotropic Radiated Power
EMM	Enterprise Mobility Management
ESI	External Services Interface
ESS	Extended Service Set

Table 7: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
ESSID	Extended Service Set Identifier
EULA	End User License Agreement
FCC	Federal Communications Commission
FFT	Fast Fourier Transform
FHSS	Frequency Hopping Spread Spectrum
FIB	Forwarding Information Base
FIPS	Federal Information Processing Standards
FQDN	Fully Qualified Domain Name
FQLN	Fully Qualified Location Name
FRER	Frame Receive Error Rate
FRR	Frame Retry Rate
FSPL	Free Space Path Loss
FTP	File Transfer Protocol
GBps	Gigabytes per second
Gbps	Gigabits per second
GHz	Gigahertz
GIS	Generic Interface Specification
GMT	Greenwich Mean Time
GPP	Guest Provisioning Page
GPS	Global Positioning System

Table 7: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
GRE	Generic Routing Encapsulation
GUI	Graphical User Interface
GVRP	GARP or Generic VLAN Registration Protocol
H2QP	Hotspot 2.0 Query Protocol
HA	High Availability
HMD	High Mobility Device
HSPA	High-Speed Packet Access
HT	High Throughput
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IAS	Internet Authentication Service
ICMP	Internet Control Message Protocol
IdP	Identity Provider
IDS	Intrusion Detection System
IE	Information Element
IEEE	Institute of Electrical and Electronics Engineers
IGMP	Internet Group Management Protocol
IGP	Interior Gateway Protocol
IGRP	Interior Gateway Routing Protocol

Table 7: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
IKE PSK	Internet Key Exchange Pre-shared Key
IoT	Internet of Things
IP	Internet Protocol
IPM	Intelligent Power Monitoring
IPS	Intrusion Prevention System
IPsec	IP Security
ISAKMP	Internet Security Association and Key Management Protocol
ISP	Internet Service Provider
JSON	JavaScript Object Notation
KBps	Kilobytes per second
Kbps	Kilobits per second
L2TP	Layer-2 Tunneling Protocol
LACP	Link Aggregation Control Protocol
LAG	Link Aggregation Group
LAN	Local Area Network
LCD	Liquid Crystal Display
LDAP	Lightweight Directory Access Protocol
LDPC	Low-Density Parity-Check
LEA	Law Enforcement Agency
LEAP	Lightweight Extensible Authentication Protocol

Table 7: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
LED	Light Emitting Diode
LEEF	Log Event Extended Format
LI	Lawful Interception
LLDP	Link Layer Discovery Protocol
LLDP-MED	LLDP–Media Endpoint Discovery
LMS	Local Management Switch
LNS	L2TP Network Server
LTE	Long Term Evolution
MAB	MAC Authentication Bypass
MAC	Media Access Control
MAM	Mobile Application Management
MBps	Megabytes per second
Mbps	Megabits per second
MCS	Modulation and Coding Scheme
MD5	Message Digest 5
MDM	Mobile Device Management
mDNS	Multicast Domain Name System
MFA	Multi-factor Authentication
MHz	Megahertz

Table 7: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
MIB	Management Information Base
MIMO	Multiple-Input Multiple-Output
MLD	Multicast Listener Discovery
MPDU	MAC Protocol Data Unit
MPLS	Multiprotocol Label Switching
MPPE	Microsoft Point-to-Point Encryption
MSCHAP	Microsoft Challenge Handshake Authentication Protocol
MSS	Maximum Segment Size
MSSID	Mesh Service Set Identifier
MSTP	Multiple Spanning Tree Protocol
MTU	Maximum Transmission Unit
MU-MIMO	Multi-User Multiple-Input Multiple-Output
MVRP	Multiple VLAN Registration Protocol
NAC	Network Access Control
NAD	Network Access Device
NAK	Negative Acknowledgment Code
NAP	Network Access Protection
NAS	Network Access Server Network-attached Storage
NAT	Network Address Translation

Table 7: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
NetBIOS	Network Basic Input/Output System
NIC	Network Interface Card
Nmap	Network Mapper
NMI	Non-Maskable Interrupt
NMS	Network Management Server
NOE	New Office Environment
NTP	Network Time Protocol
OAuth	Open Authentication
OCSP	Online Certificate Status Protocol
OFA	OpenFlow Agent
OFDM	Orthogonal Frequency Division Multiplexing
OID	Object Identifier
OKC	Opportunistic Key Caching
OS	Operating System
OSPF	Open Shortest Path First
OUI	Organizationally Unique Identifier
OVA	Open Virtual Appliance
OVF	Open Virtualization Format
PAC	Protected Access Credential

Table 7: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
PAP	Password Authentication Protocol
PAPI	Proprietary Access Protocol Interface
PCI	Peripheral Component Interconnect
PDU	Power Distribution Unit
PEAP	Protected Extensible Authentication Protocol
PEAP-GTC	Protected Extensible Authentication Protocol-Generic Token Card
PEF	Policy Enforcement Firewall
PFS	Perfect Forward Secrecy
PHB	Per-hop behavior
PIM	Protocol-Independent Multicast
PIN	Personal Identification Number
PKCS	Public Key Cryptography Standard
PKI	Public Key Infrastructure
PLMN	Public Land Mobile Network
PMK	Pairwise Master Key
PoE	Power over Ethernet
POST	Power On Self Test
PPP	Point-to-Point Protocol
PPPoE	PPP over Ethernet
PPTP	PPP Tunneling Protocol

Table 7: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
PRNG	Pseudo-Random Number Generator
PSK	Pre-Shared Key
PSU	Power Supply Unit
PVST	Per VLAN Spanning Tree
QoS	Quality of Service
RA	Router Advertisement
RADAR	Radio Detection and Ranging
RADIUS	Remote Authentication Dial-In User Service
RAM	Random Access Memory
RAP	Remote AP
RAPIDS	Rogue Access Point and Intrusion Detection System
RARP	Reverse ARP
REGEX	Regular Expression
REST	Representational State Transfer
RF	Radio Frequency
RFC	Request for Comments
RFID	Radio Frequency Identification
RIP	Routing Information Protocol
RRD	Round Robin Database

Table 7: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
RSA	Rivest, Shamir, Adleman
RSSI	Received Signal Strength Indicator
RSTP	Rapid Spanning Tree Protocol
RTCP	RTP Control Protocol
RTLS	Real-Time Location Systems
RTP	Real-Time Transport Protocol
RTS	Request to Send
RTSP	Real Time Streaming Protocol
RVI	Routed VLAN Interface
RW RoW	Rest of World
SA	Security Association
SAML	Security Assertion Markup Language
SAN	Subject Alternative Name
SCB	Station Control Block
SCEP	Simple Certificate Enrollment Protocol
SCP	Secure Copy Protocol
SCSI	Small Computer System Interface
SDN	Software Defined Networking
SDR	Software-Defined Radio

Table 7: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
SDU	Service Data Unit
SD-WAN	Software-Defined Wide Area Network
SFTP	Secure File Transfer Protocol
SHA	Secure Hash Algorithm
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SIRT	Security Incident Response Team
SKU	Stock Keeping Unit
SLAAC	Stateless Address Autoconfiguration
SMB	Small and Medium Business
SMB	Server Message Block
SMS	Short Message Service
SMTP	Simple Mail Transport Protocol
SNIR	Signal-to-Noise-Plus-Interference Ratio
SNMP	Simple Network Management Protocol
SNR	Signal-to-Noise Ratio
SNTP	Simple Network Time Protocol
SOAP	Simple Object Access Protocol
SoC	System on a Chip

Table 7: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
SoH	Statement of Health
SSH	Secure Shell
SSID	Service Set Identifier
SSL	Secure Sockets Layer
SSO	Single Sign-On
STBC	Space-Time Block Coding
STM	Station Management
STP	Spanning Tree Protocol
STRAP	Secure Thin RAP
SU-MIMO	Single-User Multiple-Input Multiple-Output
SVP	SpectraLink Voice Priority
TAC	Technical Assistance Center
TACACS	Terminal Access Controller Access Control System
TCP/IP	Transmission Control Protocol/ Internet Protocol
TFTP	Trivial File Transfer Protocol
TIM	Traffic Indication Map
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TLV	Type-length-value
ToS	Type of Service

Table 7: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
TPC	Transmit Power Control
TPM	Trusted Platform Module
TSF	Timing Synchronization Function
TSPEC	Traffic Specification
TTL	Time to Live
TTLS	Tunneled Transport Layer Security
TXOP	Transmission Opportunity
U-APSD	Unscheduled Automatic Power Save Delivery
UCC	Unified Communications and Collaboration
UDID	Unique Device Identifier
UDP	User Datagram Protocol
UI	User Interface
UMTS	Universal Mobile Telecommunication System
UPnP	Universal Plug and Play
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
USB	Universal Serial Bus
UTC	Coordinated Universal Time
VA	Virtual Appliance

Table 7: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
VBN	Virtual Branch Networking
VBR	Virtual Beacon Report
VHT	Very High Throughput
VIA	Virtual Intranet Access
VIP	Virtual IP Address
VLAN	Virtual Local Area Network
VM	Virtual Machine
VoIP	Voice over IP
VoWLAN	Voice over Wireless Local Area Network
VPN	Virtual Private Network
VRD	Validated Reference Design
VRF	Visual RF
VRRP	Virtual Router Redundancy Protocol
VSA	Vendor-Specific Attributes
VTP	VLAN Trunking Protocol
WAN	Wide Area Network
WebUI	Web browser User Interface
WEP	Wired Equivalent Privacy
WFA	Wi-Fi Alliance
WIDS	Wireless Intrusion Detection System

Table 7: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
WINS	Windows Internet Naming Service
WIPS	Wireless Intrusion Prevention System
WISPr	Wireless Internet Service Provider Roaming
WLAN	Wireless Local Area Network
WME	Wireless Multimedia Extensions
WMI	Windows Management Instrumentation
WMM	Wi-Fi Multimedia
WMS	WLAN Management System
WPA	Wi-Fi Protected Access
WSDL	Web Service Description Language
WWW	World Wide Web
WZC	Wireless Zero Configuration
XAuth	Extended Authentication
XML	Extensible Markup Language
XML-RPC	XML Remote Procedure Call
ZTP	Zero Touch Provisioning