AOS-W 6.5.4.8

Alcatel·Lucent
Enterprise

Release Notes

Revision History

The following table provides the revision history of this document.

Table 1: *Revision History*

Revision	Change Description
Revision 01	Initial release.

The AOS-W 6.5.4.8 release notes includes the following topics:

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

Supported Browsers

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

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

Contacting Support

Table 2: *Contact Information*

Contact Center Online	
Main Site	https://www.al-enterprise.com
Support Site	https://support.esd.alcatel-lucent.com
Email	ebg_global_supportcenter@al-enterprise.com
Service & Support Contact Center Telephone	

Contact Center Online	
North America	1-800-995-2696
Latin America	1-877-919-9526
EMEA	+800 00200100 (Toll Free) or +1(650)385-2193
Asia Pacific	+65 6240 8484
Worldwide	1-818-878-4507

This chapter describes the new features and/or enhancements introduced in AOS-W 6.5.4.8. For more information about these features, refer to the *AOS-W 6.5.4.x User Guide*.

Disable Default Password Recovery User

Starting from AOS-W 6.5.4.8, the **password-recovery-disable** and **password-recovery-user <username>** commands are introduced.

Use the **password-recovery-disable** command to disable the default password recovery user. Use the **no password-recovery-disable** command to enable the default password recovery user.

```
(host) (config) #password-recovery-disable
(host) (config) #no password-recovery-disable
```

Use the **password-recovery-user <username>** command to create an alternate recovery user. The alternate recovery user includes a username and password. The alternate recovery user username can be 16 characters long and the alternate recovery user password can be 32 characters long. Use the **no password-recovery-user** command to disable the alternate recovery user.

```
(host) (config) #password-recovery-user <username>
(host) (config) #no password-recovery-user
```

Use the **show mgmt-user** command to show the configured password recovery user and the status of the **password-recover-disable** command.

```
(host) #show mgmt-user

Default password recovery user: Enabled

Management User Table
---------------------
USER    PASSWD  ROLE   STATUS
----    ------  ----   ------
admin   *****   root   ACTIVE
test    *****   root   ACTIVE
```

New OUI

Starting from AOS-W 6.5.4.8, a new OUI, B0:B8:67 for Hewlett Packard Enterprise is introduced.

Switch-Datapath

Validuser Firewall Rule

Starting from AOS-W 6.5.4.8, the **any any any deny** default rule check for validuser ACL is removed. This allows you to configure the **any any any deny** rule for validuser and enable local-valid-user in the firewall to allow users only from local subnets to join the network.

GRE

Allow Unknown Unicast

Starting from AOS-W 6.5.4.8, 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 forwards unknown unicast packets.

Use the following command to allow unknown unicast:

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

Use the following command to disallow unknown unicast:

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

Base OS Security

Ageout Bridge Users

Starting from AOS-W 6.5.4.8, the **ageout-bridge-user** parameter is introduced in the **aaa-profile** command. When the **ageout-bridge-user** parameter is enabled, bridge mode clients are aged out instead of immediately deleting deauthenticated bridge mode clients. Bridge mode clients are deauthenticated when the **authentication** process receives a station-down message when bridge mode clients disconnect from an AP or roam to another AP.

Use the following command to enable ageout of bridge users:

```
(host) (AAA Profile "default") #ageout-bridge-user
```

Use the following command to disable ageout of bridge users:

```
(host) (AAA Profile "default") #no ageout-bridge-user
```

ACL for Branch Gateway Uplinks

Starting from AOS-W 6.5.4.8, an ACL for the WAN interface on branch is introduced. This ACL allows only the desired traffic and blocks other traffic. When an interface is classified as WAN interface, this ACL is automatically applied. The desired traffic is similar to:

ip access-list protect-wan

Any any svc-dchp permit

User any svc-dns permit

User any svc-natt permit

User alias aruba-central svc-aruba-central permit

User any svc-icmp permit

netdestination aruba-central

Name *.arubanetworks.com

Name d2vxf1j0rhr3p0.cloudfront.net

Name aruba.brightcloud.com

Remote AP

Support for U370L Modem

AOS-W 6.5.4.8 supports U370L LTE modems on remote APs.

Chapter 3
Regulatory Updates

This chapter describes the regulatory updates in AOS-W 6.5.4.8.

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

The following default Downloadable Regulatory Table (DRT) version is part of AOS-W 6.5.4.8:

- DRT-1.0_65685

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

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

This chapter describes the issues resolved in AOS-W 6.5.4.8.

Table 3: *Resolved Issues in AOS-W 6.5.4.8*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
114524	**Symptom:** An AP displayed 270% channel utilization. The fix ensures that the APs do not display excessive channel utilization. **Scenario:** This issue was observed in APs running AOS-W 6.4.3.0.	AP-Wireless	All platforms	AOS-W 6.4.3.0	AOS-W 6.5.4.8
154096	**Symptom:** The channel of a virtual AP was inconsistent after a radar event was detected. This issue is resolved allowing the access switch to change the channel when a virtual AP is created and a radar event is detected on the channel. **Scenario:** This issue occurred when a virtual AP was created, a radar event was detected on the channel, and the AP selected a new channel without informing the access switch. This issue was observed in OAW-AP300 Series access points running AOS-W 6.5.2.0.	AP Regulatory	OAW-AP300 Series access points	AOS-W 6.5.2.0	AOS-W 6.5.4.8
163458 172251	**Symptom:** An AP listed the **sapd| An internal system error has occurred at file sapd_wlanconfig.c function sapd_wlanconfig_destroy line 82 error Error destroying VAP 0:2 created:1: No such device** error message in the console log. The fix ensures that an AP does not list the error message **Scenario:** This issue occurred when an AP was provisioned from campus AP to outdoor AP mesh portal. This issue was observed in access points running AOS-W 6.5.3.1.	AP-Platform	All platforms	AOS-W 6.5.3.1	AOS-W 6.5.4.8
165180 179864	**Symptom:** The **Authentication** process in a switch crashed unexpectedly. This issue is resolved by returning an error message when a switch uses mschapv2 for authentication with an LDAP server. **Scenario:** This issue occurred when a switch used mschapv2 for authentication with an LDAP server. This issue was observed in switches running AOS-W 6.5.4.4.	LDAP	All platforms	AOS-W 6.5.4.4	AOS-W 6.5.4.8

Table 3: *Resolved Issues in AOS-W 6.5.4.8*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
165535 178753	**Symptom:** A client was not able to complete connection with an AP. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue was observed in access points running AOS-W 6.5.4.5 with WPA TKIP security.	AP-Wireless	All platforms	AOS-W 6.5.4.5	AOS-W 6.5.4.8
168279 172750	**Symptom:** The configured bandwidth contracts were not applied for some clients. The fix ensures that the configured bandwidth contracts are applied to clients. **Scenario:** This issue occurred when user role derivation was delayed after MAC authentication. This issue was observed in switches running AOS-W 6.5.3.0.	Base OS Security	All platforms	AOS-W 6.5.3.0	AOS-W 6.5.4.8
168985	**Symptom:** A remote AP booted with D or dirty flag. This issue is resolved by linking IPv6 remote entries into the hash table. **Scenario:** This issue occurred when IPv6 remote entries were not linked into the hash table. This issue was observed in switches running AOS-W 6.5.4.0.	Switch-Datapath	All platforms	AOS-W 6.5.4.0	AOS-W 6.5.4.8
170249 172066 175830 175931 176688 179004 181990 182574 182752	**Symptom:** A client was unable to connect to an AP that reported 100% CPU utilization. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue was observed in OAW-AP100 Series access points running AOS-W 6.5.1.9 or later versions.	AP-Wireless	OAW-AP100 Series access points	AOS-W 6.5.1.9	AOS-W 6.5.4.8
171230	**Symptom:** A client experienced intermittent packet loss. This issue is resolved by limiting the number of retries attempted when a client is unresponsive. **Scenario:** This issue occurred when a client did not send a deauthentication or disassociation request to an AP and became unresponsive. The AP attempted to communicate with the unresponsive clients and created an RTS and BAR storm in the network. Hence, other clients in the network experienced intermittent packet loss. This issue was observed in OAW-AP205, OAW-AP215, and OAW-AP225 access points running AOS-W 6.4.4.16 or later versions.	AP-Wireless	OAW-AP205, OAW-AP215, and OAW-AP225 access points	AOS-W 6.4.4.16	AOS-W 6.5.4.8

Table 3: *Resolved Issues in AOS-W 6.5.4.8*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
171521 175748	**Symptom:** The Captive Portal page for a Linux client displayed **Authentication failed** after a user entered the login credentials. The fix ensures that the Captive Portal page works as expected **Scenario:** This issue occurred when a switch did not hijack DNS response. This issue was observed in switches running AOS-W 6.5.4.3.	Switch-Datapath	All platforms	AOS-W 6.5.4.3	AOS-W 6.5.4.8
172019 172464 175355	**Symptom:** A switch displayed high CPU utilization. This issue is resolved by allowing clients to choose non-ECDH-based ciphers. High mode includes only ECDHE and DHE ciphers, medium mode includes only DHE and RSA ciphers, and low mode includes only RSA ciphers. **Scenario:** This issue occurred when the Web Server accepted ECDH-based ciphers proposed by a client. However, ECDH-based ciphers were not hardware accelerated on the switches and hence its CPU utilization was high. This issue was observed in switches running AOS-W 6.5.1.4.	Web Server	All platforms	AOS-W 6.5.1.4	AOS-W 6.5.4.8
172109	**Symptom:** The AP driver log listed the **vap-0 AP PS: AID=4342056 select next response** message. This issue is resolved by removing the debug log messages in the AP driver. **Scenario:** This issue was observed in access points running AOS-W 6.5.4.0.	AP-Wireless	All platforms	AOS-W 6.5.4.0	AOS-W 6.5.4.8
172320	**Symptom:** A VRRP flap was observed between master and local switches. The fix ensures that there is no unnecessary VRRP flapping. In adverse conditions, the VRRP failover takes an extra second. **Scenario:** This issue occurred when VRRP was enabled in switches running AOS-W 6.4.4.16 or later versions in a master-local topology.	VRRP	All platforms	AOS-W 6.4.4.16	AOS-W 6.5.4.8
172680	**Symptom:** The Mib files and IDS logs had references to an unnecessary URL. This issue is resolved by removing references to the URL. **Scenario:** This issue was observed in Mib files and IDS logs of switches running AOS-W 6.5.4.0.	SNMP	All platforms	AOS-W 6.5.4.0	AOS-W 6.5.4.8
172801 175444 176229	**Symptom:** An AP crashed and rebooted unexpectedly. The log file listed the reason for the event as **Kernel panic: Fatal exception**. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue was observed in OAW-AP225 access points running AOS-W 6.4.4.16 or later versions.	AP-Wireless	OAW-AP225 access points	AOS-W 6.4.4.16	AOS-W 6.5.4.8

Table 3: *Resolved Issues in AOS-W 6.5.4.8*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
173328	**Symptom:** A user was not able to configure **block-redirect-url** on a standby switch. This issue is resolved by saving the command to the configuration file. **Scenario:** This issue occurred when the command was not saved to the configuration file. This issue was observed in a standby switch running AOS-W 6.5.4.2 in a master-standby topology.	DPI	All platforms	AOS-W 6.5.4.2	AOS-W 6.5.4.8
173441	**Symptom:** An AP crashed and rebooted unexpectedly. The log file listed the reason for the event as **Reboot caused by kernel panic**. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue was observed in access points running AOS-W 6.4.4.16 or later versions.	AP-Wireless	All platforms	AOS-W 6.4.4.16	AOS-W 6.5.4.8
173788 174490 178159	**Symptom:** Clients switched between APs or sometimes to the other band on the same AP. The fix ensures that the clients age out normally when roaming. **Scenario:** This issue occurred when a client sent packets that indicated that it is about to roam but attempted to re-associate with the same AP. This issue was observed in access points running AOS-W 6.5.3.3 or later versions.	AP-Wireless	All platforms	AOS-W 6.5.3.3	AOS-W 6.5.4.8
173807 175068	**Symptom:** An AP crashed and rebooted unexpectedly. The log file listed the reason for the event as **Reboot caused by out of memory**. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue was observed in access points running AOS-W 6.4.4.14 or later versions.	AP-Wireless	All platforms	AOS-W 6.4.4.14	AOS-W 6.5.4.8
173868	**Symptom:** A user with the same static IP address failed to send or receive traffic when connected to an SSID. This issue is resolved by resetting the user information associated with the IP address and inheriting it from the client with the new MAC-address. **Scenario:** This issue occurred when the **prohibit-ip-spoofing** parameter was disabled in the firewall settings. This issue was observed in switches running AOS-W 6.5.3.3 or later versions.	Base OS Security	All platforms	AOS-W 6.5.3.3	AOS-W 6.5.4.8

Table 3: *Resolved Issues in AOS-W 6.5.4.8*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
173993	**Symptom:** An AP falsely classified neighboring APs on the wired network as rogue APs. The fix ensures that the wired clients do not incorrectly introduce invalid wired MAC addresses into the Ethernet MAC list. **Scenario:** This issue occurred when a client moved from an external wireless network to a wired corporate network. This issue was observed in access points running AOS-W 6.4.4.10 or later versions.	Air Management - IDS	All platforms	AOS-W 6.4.4.10	AOS-W 6.5.4.8
174320 173924 174100 175992 176293 177665 178689 179464	**Symptom:** An AP did not support fast recovery. This issue is resolved by adding support for fast recovery on OAW-AP303H, OAW-AP305, OAW-AP315, OAW-AP325, and OAW-AP335 access points. **Scenario:** This issue was observed in OAW-AP303H, OAW-AP305, OAW-AP315, OAW-AP325, and OAW-AP335 access points running AOS-W 6.4.3.4.	AP-Wireless	OAW-AP303H, OAW-AP305, OAW-AP315, OAW-AP325, and OAW-AP335 access points	AOS-W 6.5.3.4	AOS-W 6.5.4.8
174337	**Symptom:** IDS tarpit containment was inconsistent in APs. This issue is resolved by sending tarpit frames on the same channel as the intercepted frame. **Scenario:** This issue occurred when APs were configured in AM mode and the tarpit frames are sent on the wrong channel. This issue was not limited to any specific access point model or AOS-W release version.	Air Management - IDS	All platforms	AOS-W 6.5.4.4	AOS-W 6.5.4.8
174799	**Symptom:** A switch displayed the **Module Authentication is busy. Please try later** message when the **show firewall dns-names** command was executed. **Scenario:** This issue occurred when multiple DNS names were configured in a switch and one of the DNS names had too many IP addresses associated with it. This issue was observed in switches running AOS-W 6.5.4.3.	Base OS Security	All platforms	AOS-W 6.5.4.3	AOS-W 6.5.4.8
174865	**Symptom:** A client proceeded to 802.1X authentication although it failed MAC authentication. This issue is resolved by not allowing 802.1X authentication if a client fails MAC authentication. **Scenario:** This issue occurred when MAC authentication with L2 authentication fail-through was disabled. This issue was observed in switches running AOS-W 6.5.3.3 or later versions	Base OS Security	All platforms	AOS-W 6.5.3.3	AOS-W 6.5.4.8

Table 3: *Resolved Issues in AOS-W 6.5.4.8*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
175061	**Symptom:** The time of a switch was displayed incorrectly. This issue is resolved by allowing the switch to reach the NTP server thrice during boot. After failed three attempts, the show command displays a warning message to reconfigure the NTP server. **Scenario:** This issue occurred when the **NTPD** process in a switch used a local interface during boot time. The local interface did not have a route to the NTP server and hence the time of the switch was not synchronized. This issue was observed in a switches running AOS-W 6.5.1.9 or later versions.	Switch-Platform	All platforms	AOS-W 6.5.1.9	AOS-W 6.5.4.8
175583	**Symptom:** An AP rebooted unexpectedly. The log file did not indicate the reason for the event. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue was observed in OAW-AP200 Series access points running AOS-W 6.5.4.3 or later versions.	AP-Wireless	OAW-AP200 Series access points	AOS-W 6.5.4.3	AOS-W 6.5.4.8
175669	**Symptom:** The **show ap active** command did not show any flag for an AP that was operating in restricted mode because of POE-AF. This issue is resolved by showing the m flag in the **show ap active** command for an AP that operates in restricted mode. **Scenario:** This issue was observed in access points running AOS-W 6.5.1.9.	AP-Platform	All platforms	AOS-W 6.5.1.9	AOS-W 6.5.4.8
175937 177417 180023	**Symptom:** A switch rebooted unexpectedly. The log file listed reason for the event as **kernel panic**. The fix ensures that the switch works as expected. **Scenario:** This issue was observed in switches running AOS-W 6.5.4.4.	Switch-Platform	All platforms	AOS-W 6.5.4.4	AOS-W 6.5.4.8
175945	**Symptom:** A stand-alone switch, acting as a DHCP server for multiple VLAN pools, tagged DHCP-offer packets with the wrong VLAN. The fix ensures that the DHCP-offer packets are tagged with the correct VLAN. **Scenario:** This issue was observed in stand-alone switch running AOS-W 6.5.3.3 or later version in master-standby topology.	VLAN	All platforms	AOS-W 6.5.3.3	AOS-W 6.5.4.8

Table 3: *Resolved Issues in AOS-W 6.5.4.8*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
176404	**Symptom:** An AP did not send GARP when initialization was in progress. The fix ensures that the AP sends GARP when an interface is up. **Scenario:** This issue occurred when an IP address was assigned to an interface. So, when a new AP was statically allocated with an IP address of an old AP, the devices on the network were not notified and the ARP table was not updated. As a result, devices had to wait till the ARP entry expired or the new AP sent a message. This issue was observed in APs running AOS-W 6.5.1.9 or later versions.	AP Datapath	All platforms	AOS-W 6.5.1.9	AOS-W 6.5.4.8
176430	**Symptom:** An AP sent ARP request to a gateway with an incorrect IP address. The fix ensures that the AP sends ARP request with the correct IP address. **Scenario:** The issue occurred during any of the following scenarios: ■ When the AP disconnected from the switch. ■ When the DHCP server was unreachable. ■ When the gateway was unreachable. This issue was observed in APs running AOS-W 6.4.4.16 or later versions.	AP Datapath	All platforms	AOS-W 6.4.4.16	AOS-W 6.5.4.8
176607	**Symptom:** A client that was connected to an AP failed to obtain an IP address. The fix ensures that the client obtains an IP address. **Scenario:** This issue occurred due to a memory leak in the APs with onboard or USB-based BLE radios. This issue was observed in OAW-AP203H, OAW-AP203R Series OAW-AP205H, OAW-AP210 Series, OAW-AP220 Series, OAW-AP300 Series, OAW-AP310 Series, OAW-AP320 Series, OAW-AP330 Series, and OAW-AP360 Series access points running AOS-W 6.5.1.9 or later versions.	BLE	OAW-AP203H, OAW-AP203R SeriesOAW-AP205H, OAW-AP210 Series, OAW-AP220 Series, OAW-AP300 Series, OAW-AP310 Series, OAW-AP320 Series, OAW-AP330 Series, and OAW-AP360 Series access points	AOS-W 6.5.1.9	AOS-W 6.5.4.8

Table 3: *Resolved Issues in AOS-W 6.5.4.8*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
176902	**Symptom:** A switch dropped ARP response from a silent client. The fix ensures that the switch does not drop ARP response from silent clients. **Scenario:** This issue occurred when the protect ARP spoofing was enabled and a switch deleted the datapath user entries of the silent client. This issue was observed in switches running AOS-W 6.4.4.16.	Switch-Database	All platforms	AOS-W 6.4.4.16	AOS-W 6.5.4.8
176957	**Symptom:** The user-name attribute in a radius response message was not populated in the user-table during Captive Portal authentication. The fix ensures that the switch updates the user-name attribute in a radius response in the user-table. **Scenario:** This issue was observed in switches running AOS-W 6.5.4.4.	Radius	All platforms	AOS-W 6.5.4.4	AOS-W 6.5.4.8
177045	**Symptom:** An AP rebooted unexpectedly. The log file listed the reason for the event as **external watchdog reset**. The fix ensures that the AP works as expected. **Scenario:** This issue occurred when radio in the AP tried to reset PHY and the driver was stuck. This issue was observed in OAW-AP203H and OAW-AP207 access points running AOS-W 6.5.4.4.	AP-Platform	OAW-AP203H and OAW-AP207 access points	AOS-W 6.5.4.4	AOS-W 6.5.4.8
177142	**Symptom:** The periodic PHY calibration was not disabled when the radio operated in monitor or spectrum mode. This issue is resolved by enabling periodic PHY calibration only when the radio of an AP operates in AP mode. **Scenario:** This issue was observed in access points operating in monitor or spectrum mode and running AOS-W 6.5.4.7.	AP-Wireless	All platforms	AOS-W 6.5.4.7	AOS-W 6.5.4.8
177299 180021	**Symptom:** A remote AP did not connect when an OCSP server was not reachable. This issue is resolved by allowing the remote AP to connect when the OCSP server is not reachable and the **ocsp_default** environment variable is set to accept. **Scenario:** This issue occurred when the **ocsp_default** environment variable was set to accept and the OCSP server was not reachable. This issue was observed in remote APs running ArubaOS 6.5.3.5.	IPsec	All platforms	AOS-W 6.5.3.5	AOS-W 6.5.4.8

Table 3: *Resolved Issues in AOS-W 6.5.4.8*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
177571	**Symptom:** An IPv6 link local address was incorrectly generated for a VLAN interface that was configured only with IPv4 address. The fix ensures that the link local address is generated only if IPv6 is enabled on the VLAN interface. **Scenario:** This issue occurred when the operational state of the VLAN interface that was configured only with an IPv4 address was up. This issue was observed in switches running AOS-W 6.4.4.0 or later versions.	IPv6	All platforms	AOS-W 6.4.4.0	AOS-W 6.5.4.8
177575	**Symptom:** The output of the **show interface gigabitethernet <slot/module/port> counters** command displayed incorrect count of unicast and multicast packets. The fix ensures that the following show commands work appropriately: ■ The output of the **show interface gigabitethernet <slot/module/port> counters** command displays the correct count of unicast packets on 40 Gbps ports. ■ The **show interface gigabitethernet <slot/module/port> counters** command and any other command do not display the count of unicast packets on the 1 Gbps and 10 Gbps ports. **Scenario:** This issue was observed in 7280 switches running AOS-W 6.4.4.7.	Switch-Platform	7280 switches	AOS-W 6.4.4.7	AOS-W 6.5.4.8
177653	**Symptom:** The console log of an AP listed multiple user-miss and resource temporarily unavailable messages. The log on AMP listed multiple sessions for the same remote AP split-tunnel client. The fix ensures that the AP console log does not unnecessarily list user-miss and resource temporarily messages. **Scenario:** This issue was observed in access points running AOS-W 6.5.4.3.	Remote AP	All platforms	AOS-W 6.5.4.3	AOS-W 6.5.4.8
177788	**Symptom:** A client experienced slow network experience or network connectivity issue although the number of sessions in the AP did not reach the maximum value. The fix ensures that clients get a better network experience. **Scenario:** This issue was observed in OAW-AP315 access points running AOS-W 6.5.3.4.	AP Datapath	OAW-AP315 access points	AOS-W 6.5.3.4	AOS-W 6.5.4.8
178016	**Symptom:** An AP detected false radar signals and changed its radio channel frequently. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue occurred when the false radar typeid was 36. This issue was observed in OAW-AP105 access points running AOS-W 6.5.3.4.	AP-Wireless	OAW-AP105 access points	AOS-W 6.5.3.4	AOS-W 6.5.4.8

Table 3: *Resolved Issues in AOS-W 6.5.4.8*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
178032	**Symptom:** A client dropped the connection to an AP. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue occurred when active-scan was enabled in an AP. However, after 1.5 seconds, a client did not transmit or receive any packet on non-home channel, did not send beacons, or disconnected from the AP and roamed to another AP. The AP did not report neighbors in active scanning channels (channel 1 through 9 and 5 GHz non-DFS channels). This issue was observed in access points running AOS-W 6.5.4.5.	AP-Wireless	All platforms	AOS-W 6.5.4.5	AOS-W 6.5.4.8
178124	**Symptom:** Redirects failed for large cookies on Edge browser. This issue is resolved by increasing the maximum HTTP header in Apache to 128k **Scenario:** This issue occurred because the maximum HTTP header size in Apache was set to 8k. This lead to requests which had large or higher number of cookies to turn to bad requests. This issue was observed in switches running AOS-W 6.5.1.9.	Web Server	All platforms	AOS-W 6.5.1.9	AOS-W 6.5.4.8
178182 179612	**Symptom:** An AP stopped transmitting packets unexpectedly and deauthenticated clients. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue occurred because of an out-of-memory access. This issue was observed in OAW-AP225 access points running AOS-W 6.5.1.9.	AP-Wireless	All platforms	AOS-W 6.5.1.9	AOS-W 6.5.4.8
178357	**Symptom:** An AP crashed and rebooted unexpectedly. The log files listed the reason for the event as **FW ASSERT at rc_get_nss_from_chainmask()**. Enhancements to the wireless driver resolved the issue. **Scenario:** This issue was observed in OAW-AP300 Series access points running AOS-W 6.5.4.0 or later versions.	AP-Wireless	OAW-AP300 Series access points	AOS-W 6.5.4.0	AOS-W 6.5.4.8

Table 3: *Resolved Issues in AOS-W 6.5.4.8*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
178758	**Symptom:** A split-tunnel user was stuck with large idle time on a switch. This issue is resolved by adding station ageout when a client is not responsive after associating with an AP but does not complete the 4-way handshake in bridge, split-tunnel, or D-tunnel modes. **Scenario:** This issue occurred because of stale entries in the client-table of the driver. This issue was observed in access points running AOS-W 6.5.3.6.	AP-Wireless	All platforms	AOS-W 6.5.3.6	AOS-W 6.5.4.8
178998	**Symptom:** An AP changed its channel unexpectedly. The fix ensures that the AP works as expected. **Scenario:** This issue occurred when the client-aware feature was enabled and ARM wrongly triggered a channel change. This issue was observed in access points running AOS-W 6.5.1.9.	ARM	All platforms	AOS-W 6.5.1.9	AOS-W 6.5.4.8
178999	**Symptom:** A switch lost the inner IP address of a switch from its internal user-table and was not able to recover it. This lead to loss of connectivity. This issue is resolved by allowing the switch to sent the auth-ip-down message only for remote APs and not for switches. **Scenario:** This issue occurred when a switch received the IPsec delete notification from a switch before receiving a IPsec rekey message. The switch wrongly sent the auth-ip-down message to the **Authentication** process and freed the user-entry related to the inner IP address of the switch. This issue was observed in switches running AOS-W 6.5.3.6.	IPsec	All platforms	AOS-W 6.5.3.6	AOS-W 6.5.4.8

This chapter describes the known and outstanding issues identified in AOS-W 6.5.4.8.

Table 4: *Known Issues in AOS-W 6.5.4.8*

Bug ID	Description	Component	Platform	Reported Version
154625 155709 155894 156383 158536 161789	**Symptom:** The VRRP state changes although heartbeats are not missed. **Scenario:** This issue occurs when a standby switch inadvertently transitions to master state because the master switch delays the processing of VRRP advertisements. This issue is observed in switches running AOS-W 6.5.0.3 in a local-master topology. **Workaround:** Disable debug logs and syslog server. Increase the advertisement interval.	Switch-Platform	All platforms	AOS-W 6.5.0.3
157199	**Symptom:** An AP crashes unexpectedly. The log file lists the reason for the event as **kernel BUG at kernel/timer.c:869!**. **Scenario:** This issue is observed in OAW-AP225 access points running AOS-W 6.5.2.0. **Workaround:** None.	AP-Wireless	OAW-AP225 access points	AOS-W 6.5.2.0
158149 176715	**Symptom:** The BLE scanning in an AP is slow and fewer BLE devices is reported. **Scenario:** This issue is observed in OAW-AP207 access points running AOS-W 6.5.2.0 or later versions. **Workaround:** None.	BLE	AP-207 access points	AOS-W 6.5.2.0
161655	**Symptom:** Some of the high-frequency radio statistics such as tx_time, rx_time, and rx_clear are not collected correctly per beacon period on some APs. **Scenario:** This issue is observed in access points running AOS-W 6.5.2.0. **Workaround:** None.	AP-Platform	All platforms	AOS-W 6.5.2.0
163295 179432 181438	**Symptom:** An AP beacons without CAC. **Scenario:** This issue occurs when an AP boots with DFS channels. This issue is observed in OAW-AP300 Series access points running AOS-W 6.5.4.3. **Workaround:** None.	AP Regulatory	OAW-AP300 Series access points	AOS-W 6.5.4.3

Table 4: *Known Issues in AOS-W 6.5.4.8*

Bug ID	Description	Component	Platform	Reported Version
165804	**Symptom:** HTTP security header is not detected on ports 8080 or 8088 in a switch. **Scenario:** This issue is observed in switches running AOS-W 6.5.3.3. **Workaround:** None.	Switch-Platform	All platforms	AOS-W 6.5.3.3
166426 167050 170409	**Symptom:** A master and standby switch reboot unexpectedly. The log file lists the reason for the event as **Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:60)**. **Scenario:** This issue is observed in switches running AOS-W 6.5.1.9 in a master-standby topology. **Workaround:** None.	Switch-Datapath	All platforms	AOS-W 6.5.1.9
167028	**Symptom:** The SNMP walk reports AP port speed as greater than 1 Gbps on a 1 Gbps Ethernet Port. **Scenario:** This issue occurs when the **STM** process incorrectly calculates the Ethernet port speed. This issue is observed in access points running AOS-W 6.5.1.5 or later versions. **Workaround:** None.	Air Management - IDS	All platforms	AOS-W 6.5.1.5
168789	**Symptom:** An AP with a 802.1X supplicant configuration fails to boot. **Scenario:** This issue occurs when an ACL denies a DNS response from DNS server. This issue is observed in access points running AOS-W 6.5.4.0 or later versions. **Workaround:** None.	AP-Platform	All platforms	AOS-W 6.5.4.0
169622	**Symptom:** A syslog server reports the **aruba_change_channel 512 channel 6 mode 3 not found** error for some APs. **Scenario:** This issue is observed in OAW-AP314 and OAW-AP315 access points running AOS-W 6.5.1.5. **Workaround:** None.	AP-Wireless	OAW-AP314 or OAW-AP315 access points	AOS-W 6.5.1.5
170037 170055	**Symptom:** An AP does not discover a master switch through ADP. **Scenario:** This issue occurs when a static IP address is configured in an AP and the ACL denies ADP packets. This issue is observed in access points running AOS-W 6.5.4.2. **Workaround:** None.	AP-Platform	All platforms	AOS-W 6.5.4.2

Table 4: *Known Issues in AOS-W 6.5.4.8*

Bug ID	Description	Component	Platform	Reported Version
171103	**Symptom:** A switch crashes and reboots unexpectedly. The log file lists the reason for the event as **Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2)**. **Scenario:** This issue is observed in switches running AOS-W 6.5.1.9. **Workaround:** None.	Switch-Datapath	All platforms	AOS-W 6.5.1.9
171726	**Symptom:** A switch crashes and reboots unexpectedly. The log lists the reason for the event as **Datapath timeout (SOS Assert) (Intent: cause:register 54:86:50:2)**. **Scenario:** This issue is observed in OAW-4650switches running AOS-W 6.5.3.3. **Workaround:** None.	Switch-Datapath	OAW-4650switches	AOS-W 6.5.3.3
171840 177067 179206	**Symptom:** A downloaded role becomes invalid in a switch. **Scenario:** This issue occurs when an access-list name is configured using uppercase characters. This issue is observed in switches running ArubaOS 6.5.4.4. **Workaround:** None.	Role/VLAN Derivation	All platforms	AOS-W 6.5.4.4
172506	**Symptom:** A switch discards the first TCP SYN packet when a client connects to a FTP server. **Scenario:** This issue occurs in a switch when DPI is enabled. This issue is observed in switches running AOS-W 6.4.4.14. **Workaround:** None.	Switch-Datapath	All platforms	AOS-W 6.4.4.14
172987	**Symptom:** A switch crashes and reboots unexpectedly. The log file lists the reason for the event as **Kernel panic: Fatal exception**. **Scenario:** This issue is observed in OAW-4550switches running AOS-W 6.5.3.3. **Workaround:** None.	Switch-Datapath	OAW-4550switches	AOS-W 6.5.3.3
173359	**Symptom:** A switch crashes and reboots unexpectedly. The log file lists the reason for the event as **Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2)**. **Scenario:** This issue is observed in OAW-4750 switches running AOS-W 6.5.3.3. **Workaround:** None.	Switch-Datapath	OAW-4750switches	AOS-W 6.5.3.3

Table 4: *Known Issues in AOS-W 6.5.4.8*

Bug ID	Description	Component	Platform	Reported Version
173465	**Symptom:** A switch crashes and reboots unexpectedly. The log file lists the reason for the event as **Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2)**. **Scenario:** This issue is observed in OAW-4650 switches running AOS-W 6.5.4.3. **Workaround:** None.	Switch-Datapath	OAW-4650switches	AOS-W 6.5.4.3
173906	**Symptom:** The NTP authentication keys are not automatically deleted on a standby switch after they are deleted on the master switch. **Scenario:** This issue is observed in switches running AOS-W 6.5.3.3 or later versions. **Workaround:** None.	Switch-Platform	All platforms	AOS-W 6.5.3.3
174150	**Symptom:** A switch crashes and reboots unexpectedly. The log file lists the reason for the event as **Datapath crash**. **Scenario:** This issue is observed in 7280switches running AOS-W 6.5.4.2 or later versions. **Workaround:** None.	Switch-Datapath	7280switches	AOS-W 6.5.4.2
174473	**Symptom:** A switch crashes and reboots unexpectedly. The log file lists the reason for the event as **Datapath crash**. **Scenario:** This issue is observed in 7280switches running AOS-W 6.5.4.0. **Workaround:** None.	Switch-Datapath	7280switches	AOS-W 6.5.4.0
174670 178706	**Symptom:** An LACP port channel receives multiple warning messages, **LACP: Disabling Collection and Distribution on port 0/0/0 LAG 0.** **Scenario:** This issue occurs when the port channel is in trusted mode and the trusted VLAN list for the port channel does not have the default VLAN in its list. This issue is observed in switches running AOS-W 6.5.3.5. **Workaround:** None.	Port-Channel	All platforms	AOS-W 6.5.3.5
174743	**Symptom:** A switch crashes and reboots unexpectedly. The log file lists the reason for the event as **Datapath crash**. **Scenario:** This issue is observed in 7280switches running AOS-W 6.5.4.0 or later versions. **Workaround:** None.	Switch-Datapath	7280switches	AOS-W 6.5.4.0

Table 4: *Known Issues in AOS-W 6.5.4.8*

Bug ID	Description	Component	Platform	Reported Version
174823 175163	**Symptom:** The **Authentication** process in a switch crashes unexpectedly. **Scenario:** This issue occurs when the **aaa test-server verbose** command is executed. This issue is observed in switches running AOS-W 6.5.3.3 or later versions. **Workaround:** None.	Base OS Security	All platforms	AOS-W 6.5.3.3
175493	**Symptom:** A switch crashes and reboots unexpectedly. The log file lists the reason for the event as **Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2)**. **Scenario:** This issue is observed in a OAW-4750switches running AOS-W 6.5.3.3 or later versions. **Workaround:** None.	Switch-Datapath	OAW-4750switches	AOS-W 6.5.3.3
175852	**Symptom:** A switch displays the **Save failed: Module Authentication is busy. Please try later** error when the user attempts to save the configuration. **Scenario:** This issue is observed in switches running AOS-W 6.5.3.3 or later versions. **Workaround:** None.	Base OS Security	All platforms	AOS-W 6.5.3.3
176062	**Symptom:** A switch does not retain the configured member 0/0/2 on its the static port channel interface. **Scenario:** This issue is occurs when a switch is rebooted. This issue is observed in switches running AOS-W 6.5.4.4. **Workaround:** None.	Port-Channel	All platforms	AOS-W 6.5.4.4
176344	**Symptom:** A switch does not retain the cached ACR license. **Scenario:** This issue is observed in switches running AOS-W 6.5.3.3-FIPS. **Workaround:** None.	Licensing	All platforms	AOS-W 6.5.3.3-FIPS
176774 177016	**Symptom:** An AP crashes and reboots unexpectedly. The log file lists the reason for the event as **Kernel panic - not syncing: Fatal exception in interrupt**. **Scenario:** This issue is observed in OAW-AP225 access points running AOS-W 6.5.1.4. **Workaround:** None.	AP-Wireless	OAW-AP225 access points	AOS-W 6.5.1.4

Table 4: *Known Issues in AOS-W 6.5.4.8*

Bug ID	Description	Component	Platform	Reported Version
177017	**Symptom:** An AP crashes and reboots unexpectedly. The log file lists the reason for the event as **Kernel panic - not syncing: Fatal exception in interrupt**. **Scenario:** This issue is observed in OAW-AP225 access points running AOS-W 6.5.1.4. **Workaround:** None.	AP-Wireless	OAW-AP225 access points	AOS-W 6.5.1.4
177205	**Symptom:** The STM process in a switch crashes and the switch reboots unexpectedly. The log file lists the reason for the event as **unexpected stm (Station management) runtime error at data_path_handler, 1324, data_path_handler: recv - Network is down** **Scenario:** This issue is observed in OAW-4650 switches running AOS-W 6.5.3.4. **Workaround:** None.	Station Management	OAW-4650 switches	AOS-W 6.5.3.4
177652 182718	**Symptom:** The uptime displayed in the CLI is different from the value in the **Dashboard > Access Points** page in the WebUI. **Scenario:** This issue was observed in switches running AOS-W 6.5.4.2. **Workaround:** None.	WebUI	All platforms	AOS-W 6.5.4.2
178114 180746	**Symptom:** A remote AP fails to come up. **Scenario:** This issue occurs when the MTU is not adjusted automatically. This issue is observed in OAW-AP305 access points running AOS-W 6.5.1.8. **Workaround:** None.	AP Datapath	OAW-AP305 access points	AOS-W 6.5.1.8
179150 178445 178593 179787 179847 182020	**Symptom:** The memory in the wireless driver of an AP is corrupted. **Scenario:** This issue is observed in access points running AOS-W 6.5.4.5. **Workaround:** None.	AP-Wireless	All platforms	AOS-W 6.5.4.5
179360	**Symptom:** A switch displays the **Module L2TP is busy. Please try later** error message and does not provide L2TP IP address. **Scenario:** This issue is observed in switches running AOS-W 6.5.2.0. **Workaround:** None.	IPsec	All platforms	AOS-W 6.5.2.0

Table 4: *Known Issues in AOS-W 6.5.4.8*

Bug ID	Description	Component	Platform	Reported Version
179408	**Symptom:** A switch log displays the **|localdb| |wl-sync| Skipping db_sync** messages. **Scenario:** This issue is observed in OAW-4650 switches running AOS-W 6.5.3.4. **Workaround:** None.	802.1X	All platforms	AOS-W 6.5.3.4
179939	**Symptom:** A user is not able to configure the **radius-interim-accounting** parameter in the **aaa profile** command. **Scenario:** This issue occurs when the **dhcp-option-12** parameter in the **aaa derivation-rules** command and the **enforce-dhcp** parameter in **aaa profile** command are enabled. This issue is observed in switches running AOS-W 6.5.3.7 or later versions. **Workaround:** None.	Base OS Security	All platforms	AOS-W 6.5.3.7
179970	**Symptom:** The flags column in the output of the **show ap bss-table** displays wrong characters for AP enet wired clients. **Scenario:** This issue is observed in switches running AOS-W 6.5.4.7. **Workaround:** None.	Station Management	All platforms	AOS-W 6.5.4.7
180118	**Symptom:** An AP broadcasts an SSID that is configured with opensystem encryption as WEP SSID. **Scenario:** This issue is observed in access points running AOS-W 6.5.3.3. **Workaround:** None.	AP-Platform	All platforms	AOS-W 6.5.3.3

Chapter 6
Upgrade Procedure

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

Read all the information in this chapter before upgrading your switch.

Topics in this chapter include:

Upgrade Caveats

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

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

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

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

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

- When upgrading the software in a multiswitch network (one that uses two or more Alcatel-Lucent switches), special care must be taken to upgrade all the switches in the network and to upgrade them in the proper sequence. (See Upgrading in a Multiswitch Network on page 34.)

Failure to Upgrade to AOS-W 6.5.0.0-FIPS

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

This condition is caused by a change in the FIPS requirement for the strength of the hashing algorithm that is used to protect the configuration file from outside tampering. Starting from AOS-W 6.5.0.0-FIPS, all versions of AOS-W are changed to use the stronger hashing algorithm to meet FIPS requirements. This change is known to create a challenge when upgrading or downgrading a switch between AOS-W 6.4.0.0-FIPS version and AOS-W 6.5.0.0-FIPS version. In some instances the new stronger hash value may be missing or incorrect. This may cause the switch to not boot normally.

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

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

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

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

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

GRE Tunnel-Type Requirements

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

- AOS-W 6.5.4.8 continues to support L2 GRE tunnel type zero, but it is recommended to use a non-zero tunnel type.
- If both L2 and L3 tunnels are configured between endpoint devices, you must use a non-zero tunnel type for L2 GRE tunnels.

Important Points to Remember and Best Practices

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

- Schedule the upgrade during a maintenance window and notify your community of the planned upgrade. This prevents users from being surprised by a brief wireless network outage during the upgrade.
- Avoid making any other changes to your network, such as configuration changes, hardware upgrades, or changes to the rest of the network during the upgrade. This simplifies troubleshooting.
- Know your network and verify the state of your network by answering the following questions:
  - How many APs are assigned to each switch? Verify this information by navigating to the **Monitoring > NETWORK > All Access Points** section of the WebUI, or by executing the **show ap active** and **show ap database** CLI commands.
  - How are those APs discovering the switch (DNS, DHCP Option, Broadcast)?
  - What version of AOS-W is currently on the switch?
  - Are all switches in a master-local cluster running the same version of software?
  - Which services are used on the switches (employee wireless, guest access, remote AP, wireless voice)?
- Resolve any existing issues (consistent or intermittent) before you upgrade.
- If possible, use FTP to load software images to the switch. FTP is faster than TFTP and offers more resilience over slow links. If you must use TFTP, ensure the TFTP server can send over 30 MB of data.
- Always upgrade the non-boot partition first. If problems occur during the upgrade, you can restore the flash, and switch back to the boot partition. Upgrading the non-boot partition gives you a smoother downgrade path should it be required.
- Before you upgrade to this version of AOS-W, assess your software license requirements and load any new or expanded licenses you may require. For a detailed description of these new license modules, refer to the "Software Licenses" chapter in the *AOS-W 6.5.x User Guide*.

Memory Requirements

All Alcatel-Lucent switches store critical configuration data on an onboard compact flash memory module. Ensure that there is always free flash space on the switch. Loading multiple large files such as JPEG images for RF Plan can consume flash space quickly. To maintain the reliability of your WLAN network, the following compact memory best practices are recommended:

- Confirm that there is at least 60 MB of free memory available for an upgrade using the WebUI, or execute the **show memory** command to confirm that there is at least 40 MB of free memory available for an upgrade using the CLI. Do not proceed unless this much free memory is available. To recover memory, reboot the switch. After the switch comes up, upgrade immediately.
- Confirm that there is at least 75 MB of flash space available for an upgrade using the WebUI, or execute the **show storage** command to confirm that there is at least 60 MB of flash space available for an upgrade using the CLI.

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

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

- **Crash Data:** Execute the **tar crash** command to compress crash files to a file named **crash.tar**. Use the procedures described in Backing up Critical Data on page 32 to copy the **crash.tar** file to an external server, and then execute the **tar clean crash** command to delete the file from the switch.
- **Flash Backups:** Use the procedures described in Backing up Critical Data on page 32 to back up the flash directory to a file named **flash.tar.gz**, and then execute the **tar clean flash** command to delete the file from the switch.
- **Log files:** Execute the **tar logs** command to compress log files to a file named **logs.tar**. Use the procedures described in Backing up Critical Data on page 32 to copy the **logs.tar** file to an external server, and then execute the **tar clean logs** command to delete the file from the switch.

Backing up Critical Data

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

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

- X.509 certificates
- Switch Logs

Backing up and Restoring Compact Flash in the WebUI

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

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

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

Backing up and Restoring Compact Flash in the CLI

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

1. Make sure you are in the **enable** mode in the switch CLI, and execute the following command:
   ```
   (host) # write memory
   ```
2. Execute the **backup** command to back up the contents of the compact flash file system to the **flashbackup.tar.gz** file.
   ```
   (host) # backup flash
   Please wait while we tar relevant files from flash...
   Please wait while we compress the tar file...
   Checking for free space on flash...
   Copying file to flash...
   File flashbackup.tar.gz created successfully on flash.
   ```
3. Execute the **copy** command to transfer the backup flash file to an external server or storage device.
   ```
   (host) copy flash: flashbackup.tar.gz ftp: <ftphost> <ftpusername> <ftpuserpassword> <remote directory>
   (host) copy flash: flashbackup.tar.gz usb: partition <partition-number>
   ```

   You can later transfer the backup flash file from the external server or storage device to the compact flash file system by executing the **copy** command.
   ```
   (host) # copy tftp: <tftphost> <filename> flash: flashbackup.tar.gz
   (host) # copy usb: partition <partition-number> <filename> flash: flashbackup.tar.gz
   ```
4. Execute the **restore** command to untar and extract the **flashbackup.tar.gz** file to the compact flash file system.
   ```
   (host) # restore flash
   ```

Upgrading in a Multiswitch Network

In a multiswitch network (a network with two or more Alcatel-Lucent switches), special care must be taken to upgrade all switches based on the switch type (master or local). Be sure to back up all switches being upgraded, as described in Backing up Critical Data on page 32.

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

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

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

Installing the FIPS Version of AOS-W 6.5.4.8

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

Instructions on Installing FIPS Software

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

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

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

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

Upgrading to AOS-W 6.5.4.8

The following sections provide the procedures for upgrading the switch to AOS-W 6.5.4.8 by using the WebUI and the CLI.

Install Using the WebUI

CAUTION

Confirm that there is at least 60 MB of free memory and at least 75 MB of flash space available for an upgrade using the WebUI. For details, see Memory Requirements on page 32.

NOTE

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

Upgrading From a Recent Version of AOS-W

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

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

NOTE

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

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

1. Download AOS-W 6.5.4.8 from the customer support site.
2. Upload the new software image(s) to a PC or workstation on your network.
3. Validate the SHA hash for a software image:
   a. Download the **Alcatel.sha256** file from the download directory.
   b. To verify the image, load the image onto a Linux system and execute the **sha256sum <filename>** command or use a suitable tool for your operating system that can generate a **SHA256** hash of a file.
   c. Verify that the output produced by this command matches the hash value found on the support site.

NOTE

The AOS-W image file is digitally signed, and is verified using RSA2048 certificates preloaded on the switch at the factory. Therefore, even if you do not manually verify the SHA hash of a software image, the switch will not load a corrupted image.

4. Log in to the AOS-W WebUI from the PC or workstation.
5. Navigate to the **Maintenance > Controller > Image Management** page.
   a. Select the **Local File** option.
   b. Click **Browse** to navigate to the saved image file on your PC or workstation.

6. Select the downloaded image file.
7. Choose the nonboot partition from the **Partition to Upgrade** radio button.
8. Choose **Yes** in the **Reboot Controller After Upgrade** radio button to automatically reboot after upgrading. Choose **No**, if you do not want the switch to reboot immediately.

Upgrade will not take effect until you reboot the switch.

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

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

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

When your upgrade is complete, perform the following steps to verify that the switch is functioning as expected.

1. Log in to the WebUI to verify all your switches are up after the reboot.
2. Navigate to the **Monitoring > NETWORK > Network Summary** page to determine if your APs are up and ready to accept clients. In addition, verify that the number of access points and clients are what you would expect.
3. Verify that the number of access points and clients are what you would expect.
4. Test a different type of client for each access method that you use and in different locations when possible.
5. Complete a backup of all critical configuration data and files on the compact flash file system to an external server or mass storage facility. See Backing up Critical Data on page 32 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 32.

Upgrading From a Recent Version of AOS-W

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

- AOS-W 3.4.4.1 or later

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

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

1. Download AOS-W 6.5.4.8 from the customer support site.
2. Open an SSH session on your master (and local) switches.
3. Execute the **ping** command to verify the network connection from the target switch to the SCP/FTP/TFTP server.
   ```
   (host)# ping <ftphost>
   ```
   or
   ```
   (host)# ping <tftphost>
   ```
   or
   ```
   (host)# ping <scphost>
   ```
4. Execute the **show image version** command to check if the AOS-W images are loaded on the switch's flash partitions. The partition number appears in the **Partition** row; **0:0** is partition 0, and **0:1** is partition 1. The active boot partition is marked as **Default boot**.
5. Execute the **copy** command to load the new image onto the nonboot partition.
   ```
   (host)# copy ftp: <ftphost> <ftpusername> <image filename> system: partition <0|1>
   ```
   or
   ```
   (host)# copy tftp: <tftphost> <image filename> system: partition <0|1>
   ```
   or
   ```
   (host)# copy scp: <scphost> <scpusername> <image filename> system: partition <0|1>
   ```
   or
   ```
   (host)# copy usb: partition <partition-number> <image filename> system: partition <0|1>
   ```

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

6. Execute the **show image version** command to verify that the new image is loaded.
7. Reboot the switch.
   ```
   (host)# reload
   ```
8. Execute the **show version** command to verify that the upgrade is complete.
   ```
   (host)# show version
   ```

When your upgrade is complete, perform the following steps to verify that the switch is functioning as expected.

1. Log in to the CLI to verify that all your switches are up after the reboot.
2. Execute the **show ap active** command to determine if your APs are up and ready to accept clients.
3. Execute the **show ap database** command to verify that the number of access points and clients are what you expected.

4. Test a different type of client for each access method that you use and in different locations when possible.
5. Complete a backup of all critical configuration data and files on the compact flash file system to an external server or mass storage facility. See Backing up Critical Data on page 32 for information on creating a backup.

Downgrading

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

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

If you do not downgrade to a previously saved pre-6.1 configuration, some parts of your deployment may not work as they previously did. For example, when downgrading from AOS-W 6.5.4.8 to 5.0.3.2, changes made to WIPS in AOS-W 6.x prevent the new predefined IDS profile assigned to an AP group from being recognized by the older version of AOS-W. This unrecognized profile can prevent associated APs from coming up, and can trigger a profile error. These new IDS profiles begin with *ids-transitional* while older IDS profiles do not include *transitional*. If you have encountered this issue, execute the **show profile-errors** and **show ap-group** commands to view the IDS profile associated with the AP group.

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

Before You Begin

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

1. Back up your switch. For details, see Backing up Critical Data on page 32.
2. Verify that the control plane security is disabled.
3. Set the switch to boot with the previously saved pre-AOS-W 6.5.4.8 configuration file.
4. Set the switch to boot from the system partition that contains the previously running AOS-W image.

   When you specify a boot partition (or copy an image file to a system partition), the software checks to ensure that the image is compatible with the configuration file used on the next switch reload. An error message is displayed if system boot parameters are set for incompatible image and configuration files.
5. After downgrading the software on the switch, perform the following steps:
   - Restore pre-AOS-W 6.5.4.8 flash backup from the file stored on the switch. Do not restore the AOS-W 6.5.4.8 flash backup file.
   - You do not need to reimport the WMS database or RF Plan data. However, if you have added changes to RF Plan in AOS-W 6.5.4.8, the changes do not appear in RF Plan in the downgraded AOS-W version.
   - If you installed any certificates while running AOS-W 6.5.4.8, you need to reinstall the certificates in the downgraded AOS-W version.

Downgrading Using the WebUI

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

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

Downgrading Using the CLI

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

1. If the saved preupgrade configuration file is on an external FTP/TFTP server, use the following command to copy it to the switch:
   ```
   (host) # copy ftp: <ftphost> <ftpusername> <image filename> system: partition 1
   ```
   or
   ```
   (host) # copy tftp: <tftphost> <image filename> system: partition 1
   ```
2. Set the switch to boot with your preupgrade configuration file.
   ```
   (host) # boot config-file   <backup configuration filename>
   ```
3. Execute the **show image version** command to view the partition on which your previous software image is stored. You cannot load a new image into the active system partition (the default boot).

In the following example, partition 1, the backup system partition, contains the backup release AOS-W 6.1.3.2. Partition 0, the default boot partition, contains the AOS-W 6.5.4.8 image.

4. Set the backup system partition as the new boot partition.
   ```
   (host) # boot system partition 1
   ```
5. Reboot the switch.
   ```
   (host) # reload
   ```
6. When the boot process is complete, verify that the switch is using the correct software.
   ```
   (host) # show image version
   ```

Before You Call Technical Support

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

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