AOS-W 6.4.4.8

Alcatel·Lucent
Enterprise

Release Notes

Contents

Revision History

The following table lists the revision history of this document.

Table 1: *Revision History*

Revision	Change Description
Revision 01	Initial release.

AOS-W 6.4.4.8 is a software patch release that includes new features and enhancements introduced in this release and fixes to issues identified in previous releases.

Use the following links to navigate to the corresponding topics:

- New Features on page 10 describes the features and enhancements introduced in this release.
- Regulatory Updates on page 12 lists the regulatory updates introduced in this release.
- Resolved Issues on page 13 describes the issues resolved in this release.
- Known Issues on page 26 describes the known and outstanding issues identified in this release.
- Upgrade Procedure on page 31 describes the procedures for upgrading a switch to this release.

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 10.x and 11 on Windows 7 and Windows 8
- Mozilla Firefox 23 or later on Windows Vista, Windows 7, Windows 8, and Mac OS
- Apple Safari 5.1.7 or later on Mac OS

Contacting Support

Table 3: *Contact Information*

Contact Center Online	
• Main Site	http://www.alcatel-lucent.com/enterprise
• Support Site	https://service.esd.alcatel-lucent.com
• Email	esd.support@alcatel-lucent.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 6.4.4.8.

Adaptive Radio Management

The following enhancement is introduced as part of Adaptive Radio Management.

Pending Client-Match Steers

The pending client-match entries (where the moves have not completed) are no longer displayed in the output of the **show ap arm client-match history** command which now displays only the last 32 completed moves. Starting from AOS-W 6.4.4.8, a new parameter, **pending**, is introduced in the **show ap arm client-match** command. This parameter is introduced to filter and view only the pending client-match entries.

The following sample displays the pending client-match entries:

```
(host) #show ap arm client-match pending

S: Source, T: Target, A: Actual
BTM-ACC: 11v BTM Accept, BTM-REJ#: 11v-BTM Reject with reason #, BTM-TO: 11v-BTM Timeout, BTM-FA: 11v-BTM False Accept
Unit of Roam Time: second
Unit of Signal: dBm

ARM Client match History
------------------------
Time of Change       Station            Reason  Status/Roam Time/Mode
--------------       -------            ------  --------------------
2016-05-24 15:53:26  xx:xx:xx:xx:xx:xx  Sticky  Pending/5403/Deauth
2016-05-24 13:08:01  yy:yy:yy:yy:yy:yy  Sticky  Pending/15328/Deauth

Signal(S/T/A)  Band(S/T/A)  Radio Bssid(S/T/A)                      AP Name(S/T/A)
-------------  -----------  ------------------                      --------------
-89/-59/-      5G/5G/-      11:11:11:11:11:11/22:22:22:22:22:22/-   AP1/AP2/-
-83/-64/-      5G/5G/-      22:22:22:22:22:22/33:33:33:33:33:33/-   AP2/AP3/-
```

AMON

The following enhancement is introduced as part of AMON.

AMON Packet Size

When upgrading from an existing AOS-W 6.4.4.x release, it is required to set the AMON packet size manually to a desired value. However, the packet size is increased to 32K by default for fresh installations of AOS-W 6.4.4.8.

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

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

The following default Downloadable Regulatory Table (DRT) file version is part of AOS-W 6.4.4.8:

- DRT-1.0_54672

This chapter describes the issues resolved in AOS-W 6.4.4.8.

Table 4: *Resolved Issues in 6.4.4.8*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
114189	**Symptom:** The firewall visibility cache entries were not cleared in a switch. This issue is resolved by setting the correct DNS entry type. **Scenario:** This issue occurred because IPv4 DNS records of incorrect type set were populated as IPv6 records. This issue was observed in switches running AOS-W 6.4.3.0.	Firewall Visibility	All platforms	AOS-W 6.4.3.0	AOS-W 6.4.4.8
124136 138762	**Symptom:** A client failed to connect to an SSID. The log file for the event listed the reason as **Capability requested by STA unsupported by AP**. This issue is resolved by adding a VLAN discovery message (if required) during a High Availability (HA) failover. **Scenario:** This issue occurred during a failover in a HA set up when no VLAN was assigned for the virtual AP profile that was configured in tunnel mode. This issue was observed in switches running AOS-W 6.4.2.5.	AP-Wireless	All platforms	AOS-W 6.4.2.5	AOS-W 6.4.4.8
125862	**Symptom:** A user was unable to edit a VLAN range in the port channel by using the WebUI. This issue is resolved by allowing changes to the VLAN range for port channels. **Scenario:** This issue was observed in both master and local switches running AOS-W 6.4.x in a master-standby-local topology.	WebUI	All platforms	AOS-W 6.4.2.5	AOS-W 6.4.4.8

Table 4: *Resolved Issues in 6.4.4.8*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
126713	**Symptom:** A switch continued to send authentication requests to an authentication server that was out of service and the clients never completed authentication. This issue is resolved by resetting the authentication server whenever a server in a group is back in service. cache entries of the authentication server group. **Scenario:** This issue occurred when an authentication server went out of service after authenticating a user and the same server was reused for authentication in the next instance. The authentication server stored in the user context was reused even if the server was out of service. This issue was observed in switches running AOS-W 6.4.2.5.	Base OS Security	All platforms	AOS-W 6.4.2.5	AOS-W 6.4.4.8
128057	**Symptom:** In centralized licensing, the number of remaining licenses mismatched with the number of remaining AP capacity on the licensing master switch. This issue is resolved by not accounting the number of standby access points when calculating the remaining AP capacity. **Scenario:** This issue occurred when centralized licensing was enabled and standby access points were also accounted for while calculating the remaining AP capacity. Additionally, there were controllers in HA mode with backup access points. This issue was observed in switches running AOS-W 6.4.x or later versions.	AP-Platform	All platforms	AOS-W 6.4.2.8	AOS-W 6.4.4.8
128441	**Symptom:** Packet loss was seen during peak data traffic. This issue is resolved by increasing the platform limit for sessions from 32768 to 65536. **Scenario:** This issue occurred when the session limit was reached in a switch. Session tables were full and a new session entry was not allotted. Hence, the switch dropped the packets. This issue was observed in OAW-40xx Series switches with a session limit of 32K (32768) running AOS-W 6.4.x.	Switch-Datapath	OAW-40xx Series switches	AOS-W 6.4.2.13	AOS-W 6.4.4.8

Table 4: *Resolved Issues in 6.4.4.8*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
128552	**Symptom:** All clients lost connectivity when multiple clients switched to hardware sleep mode. This issue is resolved by resuming normal operation when a client switches from inactive state to active state. **Scenario:** This issue occurred when multiple clients switched to hardware sleep mode without sending a deauthentication request for a duration equal to the ageout timer (default: 1000 seconds). This issue was observed in OAW-AP200 Series, OAW-AP210 Series, OAW-AP220 Series, or OAW-AP275 access points running AOS-W 6.4.2.8.	AP-Platform	OAW-AP200 Series, OAW-AP210 Series, OAW-AP220 Series, and OAW-AP275 access points	AOS-W 6.4.2.8	AOS-W 6.4.4.8
128916 132353 133884 138015	**Symptom:** A switch denied access to a user. The log file for the event listed the reason as **drop pkt as ip not assigned through dhcp**. This issue is resolved by enabling enforce-DHCP. **Scenario:** This issue occurred when DHCP enforcement failed. This issue was observed in switches running AOS-W 6.3.1.16.	Switch-Datapath	All platforms	AOS-W 6.3.1.16	AOS-W 6.4.4.8
131104 137024	**Symptom:** An incorrect AP interference statistic that was sent from a switch to an AP led to gaps in the channel utilization graph in OV3600. This issue is resolved by limiting the interference value of an AP in the range of 0-100. **Scenario:** This issue was observed in OAW-AP135 access points running AOS-W 6.3.1.5.	AP-Wireless	OAW-AP135 access points	AOS-W 6.3.1.5	AOS-W 6.4.4.8
130917 136646 140035	**Symptom:** When the **show running config** command was issued, the **Module AMAPI SNMP trap client is busy. Please try later** error message was displayed. The fix ensures that this error message is not displayed. **Scenario:** This issue occurred when bulk SNMP queries were executed in a switch. This issue was observed in switches running AOS-W 6.4.2.x, AOS-W 6.4.3.x, or AOS-W 6.4.4.x versions.	SNMP	All platforms	AOS-W 6.4.3.5	AOS-W 6.4.4.8

Table 4: *Resolved Issues in 6.4.4.8*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
131445 136572	**Symptom:** When roaming using 802.11r fast handoff, a client got an IP address from a VLAN mapped in the virtual AP profile although it was supposed to get an IP address from a VLAN derived from Vendor Specified Attribute (VSA). This issue is resolved by updating the **Station Management** (STM) process about the derived VLAN and avoiding key exchange when the **station management** process acknowledges the VLAN update. **Scenario:** This issue occurred for 802.1X authenticated clients when they roamed using 802.11r fast handoff. This issue was observed in switches running AOS-W 6.3.x or AOS-W 6.4.x.	Base OS Security	All platforms	AOS-W 6.4.3.4	AOS-W 6.4.4.8
131921 137958 138552 138581 138914 140744	**Symptom:** An AP rebooted unexpectedly. The log file for the event listed the reason as **memory corruption 0xAA**. The fix ensures that the AP does not reboot unexpectedly. **Scenario:** This issue was observed in OAW-AP325 access points running AOS-W 6.4.4.4.	AP-Platform	OAW-AP325 access points	AOS-W 6.4.4.4	AOS-W 6.4.4.8
132382	**Symptom:** Users could not add a username with an apostrophe character in the RAP whitelist database using the WebUI. The fix ensures that users can add a username with an apostrophe character. **Scenario:** This issue occurred when an add entry was enclosed in apostrophe character. This issue was observed in switches running AOS-W 6.4.2.x.	WebUI	All platforms	AOS-W 6.4.2.3	AOS-W 6.4.4.8
132814	**Symptom:** An AP rebooted unexpectedly. The log file for the event listed the reason as **reboot reason: Reboot caused by kernel panic**. The fix ensures that the AP does not reboot unexpectedly without generating a crash information file. **Scenario:** This issue was observed in OAW-AP210 Series, OAW-AP220 Series, OAW-AP228, or OAW-AP270 Series access points running AOS-W 6.4.2.6.	AP-Wireless	OAW-AP210 Series, OAW-AP220 Series, OAW-AP228, and OAW-AP270 Series access points	AOS-W 6.4.2.6	AOS-W 6.4.4.8

Table 4: *Resolved Issues in 6.4.4.8*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
133266	**Symptom:** A local switch rebooted unexpectedly. The log file for the event listed the reason as **Reboot Cause: Datapath timeout (Intent:cause:register 56:86:50:2)**. The fix ensures that a switch does not reboot unexpectedly. **Scenario:** This issue occurred because of memory corruption. This issue was observed in OAW-4650 switches running AOS-W 6.4.3.6.	Switch-Datapath	OAW-4650 switches	AOS-W 6.4.3.6	AOS-W 6.4.4.8
133366 139845	**Symptom:** The **station management** process frequently logged messages about tracing being on. The trace files were rotated and these logs could not be turned off through the logging level configuration. The fix ensures that logging level configuration is applied to these logs messages. **Scenario:** This issue was observed in access points that were logging station management trace-related log messages.	Station Management	All platforms	AOS-W 6.4.3.5	AOS-W 6.4.4.8
133442	**Symptom:** The inner pool Layer 2 Protocol Tunneling (L2PT) traffic of a RAP displayed clear-text traffic in a switch uplink with aged-out sessions. The fix ensures that a switch is marked as DOWN until the WLAN Management Suite (WMS) application acknowledges the inner IP change and updates its IP address to the inner IP of the RAP. **Scenario:** When RAPs rebootstrapped, the inner IP address of a RAP changed, but the WMS application was not updated immediately. The WMS application was only updated during the next AP periodic update session. However, the WMS application did not acknowledge the periodic update as the IP address in the WMS was incorrect and so the AP sent a probe register that updated the IP address at the WMS application. During this time, when the WMS application had the incorrect inner IP of the RAP, if it sent a message to the RAP, the message did not go through the IPsec tunnel and went in clear-text.	Air Management-IDS	All platforms	AOS-W 6.4.2.6	AOS-W 6.4.4.8
134479	**Symptom:** When a 340U USB modem was plugged into a RAP, the RAP rebooted continuously although the RAP was provisioned with the 340U USB modem parameters. This issue is resolved by changing the USB modem driver as recommended by the device manufacturer. **Scenario:** This issue occurred because of a missing Linux patch. This issue was observed in remote access points supporting 340U USB modems.	Remote Access Point	All platforms	AOS-W 6.4.4.6	AOS-W 6.4.4.8

Table 4: *Resolved Issues in 6.4.4.8*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
134646	**Symptom:** An **accounting-stop** message with wrong values was sent when posting XML user-add to a switch. The fix ensures that the **accounting-stop** message on XML user-add has correct values. **Scenario:** This issue was observed when user-add was posted to an authenticated Captive Portal user. The **accounting-stop** message contained all zeroes and the framed IP address was 0.0.0.0. This issue was observed in switches running AOS-W 6.4.2.12.	XML API	All platforms	AOS-W 6.4.2.12	AOS-W 6.4.4.8
134782 138446 138457 138513 138519 138536 138540 138542 138586	**Symptom:** An AP crashed unexpectedly. The log file for the event listed the reason as **__activate_page+0x68/0x108**. This issue is resolved by preventing access to a memory page that is not on the inactive list. **Scenario:** This issue was observed in OAW-AP325 access points running AOS-W 6.4.4.4.	AP-Platform	OAW-AP325 access points	AOS-W 6.4.4.4	AOS-W 6.4.4.8
134789	**Symptom:** When a user selected an AP listed in the **Monitoring > Network > All Access Points** page, information related to multiple APs was displayed although only one AP was selected. This issue is resolved by fetching and displaying information of only the queried AP. **Scenario:** This issue was observed in switches running AOS-W 6.4.3.4.	WebUI	All platforms	AOS-W 6.4.3.4	AOS-W 6.4.4.8
134884 135077	**Symptom:** A switch displayed an incorrect **Up time** value for some access points in the **Dashboard > Access Points** page of the WebUI. This issue is resolved by modifying the **Up time** in the time-range conversion logic. **Scenario:** This issue was observed in switches running AOS-W 6.4.2.14.	WebUI	All platforms	AOS-W 6.4.2.14	AOS-W 6.4.4.8

Table 4: *Resolved Issues in 6.4.4.8*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
135090	**Symptom:** A client received a malformed Reset (RST) from a switch. This issue is resolved by adding the missing byte to the RST. **Scenario:** This issue occurred when an Access Control Entry (ACE) in an Access Control List (ACL) was configured with **send-deny-response** and a switch responded to a client with an RST after dropping a matching packet. But the client received a malformed RST because of a missing byte in the RST response sent by the switch. This issue was observed in switches running AOS-W 6.4.2.3.	Switch-Datapath	All platforms	AOS-W 6.4.2.3	AOS-W 6.4.4.8
135097	**Symptom:** A switch rebooted unexpectedly. The log file for the event listed the reason as **Datapath timeout (Intent:cause:register 56:86:50:2)**. This issue is resolved by avoiding a race condition in aging sessions. **Scenario:** This issue occurred because of a race condition in aging session when a session had type 2 contract. This issue was observed in OAW-4650 switches running AOS-W 6.4.3.6.	Switch-Datapath	OAW-4650 switches	AOS-W 6.4.3.6	AOS-W 6.4.4.8
135569 135570	**Symptom:** An AP crashed unexpectedly. The log file for the event listed the reason as **Kernel panic - not syncing: Fatal exception in interrupt**. The fix ensures that an AP functions as expected. **Scenario:** This issue occurred when spectrum monitoring was enabled in an AP. When the AP radio changed from spectrum mode to normal mode on the home channel, it experienced a phenomenon called as stuck beacon. Stuck beacon is a driver-level error indicating that the chipset failed to complete a Tx function. This issue was observed in OAW-AP130 Series access points running AOS-W 6.4.3.6 or later versions.	AP-Wireless	OAW-AP130 Series access points	AOS-W 6.4.4.4	AOS-W 6.4.4.8
135742	**Symptom:** The **authentication** process crashed in a local switch. The fix ensures that the **authentication** process does not crash. **Scenario:** This issue occured when new entries were added in an IPv6 net destination (or alias) followed by a full synchronization between the master and local switches. This issue was observed in switches AOS-W 6.4.2.x, AOS-W 6.4.3.x, or AOS-W 6.4.4.x in a master-local topology.	Base OS Security	All platforms	AOS-W 6.4.2.14	AOS-W 6.4.4.8

Table 4: *Resolved Issues in 6.4.4.8*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
135862	**Symptom:** After configuring the Maximum Transmission Unit (MTU) in **ap system-profile**, the **show ap bss-table** command displayed an incorrect MTU value. This issue is resolved by resending the MTU update message to a switch within 60 seconds. **Scenario:** This issue occurred when the MTU update message was lost. This issue was observed in access points running AOS-W 6.3.x.	AP-Datapath	All platforms	AOS-W 6.3.1.9	AOS-W 6.4.4.8
136444	**Symptom:** The Network Time Protocol (NTP) authentication keys failed to synchronize between a master switch and a standby switch. The fix ensures that the NTP authentication keys are synchronized on the standby switch. **Scenario:** This issue occurred when NTP authentication was enabled but the NTP authentication keys failed to synchronize from a master switch to a standby switch. This issue was observed in switches running AOS-W 6.4.3.5 in a master-standby topology.	Configuration	All platforms	AOS-W 6.4.3.5	AOS-W 6.4.4.8
136672 139929 142307	**Symptom:** An AP failed to come up when it connected with a 4-wire Ethernet cable to a switch. This issue is resolved by ignoring the advised ability bit. **Scenario:** This issue occurred because the **sapd** process missed the advised ability bit. This issue was observed in OAW-AP105 access points running AOS-W 6.4.4.3.	AP-Platforms	OAW-AP105 access points	AOS-W 6.4.4.3	AOS-W 6.4.4.8
136724	**Symptom:** The **wlanAPRadioTransmitPower** trap displayed an incorrect value for Equivalent Isotropically Radiated Power (EIRP) in an AP. The fix ensures that the trap displays the correct EIRP value. **Scenario:** This issue occurred when the **wlanAPRadioTransmitPower** trap was incorrectly calculated for EIRP in an AP. This issue was observed in switches running AOS-W 6.4.3.x or AOS-W 6.4.4.x.	Station Management	All platforms	AOS-W 6.4.4.6	AOS-W 6.4.4.8

Table 4: *Resolved Issues in 6.4.4.8*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
136851	**Symptom:** An AP crashed and rebooted unexpectedly. The log file for the event listed the reason as **kernel panic: Fatal exception**. The fix ensures that an AP does not access wrong memory or reboot. **Scenario:** This issue occurred because of wrong memory access. This issue was observed in OAW-AP210 Series, OAW-AP220 Series, OAW-AP277, or OAW-AP320 Series access points running AOS-W 6.4.3.5.	AP-Platform	OAW-AP210 Series, OAW-AP220 Series, OAW-AP277, and OAW-AP320 Series access points	AOS-W 6.4.3.5	AOS-W 6.4.4.8
137549	**Symptom:** The **no export-route** parameter under the **aaa authentication vpn** command did not work as expected. This issue is resolved by correcting the profile checking. **Scenario:** This issue occurred because the inner IP of IAP VPN was distributed over Open Shortest Path First (OSPF) after the **no export-route** parameter was configured under the **aaa authentication vpn** command. This issue was observed in switches running AOS-W 6.4.2.x, AOS-W 6.4.3.x or AOS-W 6.4.4.x.	OSPF	All platforms	AOS-W 6.4.2.13	AOS-W 6.4.4.8
138014	**Symptom:** An AP crashed and rebooted frequently. The log file for the event listed the reason as **Reboot caused by kernel panic: Fatal exception in interrupt** or **Reboot due to out of Memory**. The fix ensures that an AP does not reboot unexpectedly. **Scenario:** This issue occurred because of a memory leak caused by jumbo frames. This issue was observed in OAW-AP200 Series access points running AOS-W 6.4.4.5.	AP-Platform	OAW-AP200 Series access points	AOS-W 6.4.4.5	AOS-W 6.4.4.8
138196 138482 138560 139345 140196 141406	**Symptom:** The **authentication** process stopped responding and crashed in a switch. The fix ensures that the **authentication** process does not crash in a switch. **Scenario:** This issue occurred because of a memory corruption. This issue was observed in local switches running AOS-W 6.4.3.6 in a master-local topology.	Base OS Security	All platforms	AOS-W 6.4.3.6	AOS-W 6.4.4.8
138356	**Symptom:** AppRF failed to block certain social networking sites. the fix ensures that AppRF block such sites. **Scenario:** This issue occurred because the Deep Packet Inspection (DPI) engine classified the social networking sites but the **WebCC** process did not. This issue was observed in switches running AOS-W 6.4.3.7.	Switch-Datapath	All platforms	AOS-W 6.4.3.7	AOS-W 6.4.4.8

Table 4: *Resolved Issues in 6.4.4.8*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
138433	**Symptom:** An AP rebooted unexpectedly. The log file for the event listed the reason as **FW ASSERT [02] 0x00980730**. The fix ensures that an AP does not reboot unexpectedly. **Scenario:** This issue was observed in OAW-AP325 access points running AOS-W 6.4.4.4.	AP-Wireless	OAW-AP325 access points	AOS-W 6.4.4.4	AOS-W 6.4.4.8
138508	**Symptom:** An AP rebooted unexpectedly. The log file for the event listed the reason as **Rebooting the AP because of FW ASSERT [02] : 0x009C43F8**. This issue is resolved by adding protection that prevents the passing of an invalid index. **Scenario:** This issue was observed in OAW-AP325 access points running AOS-W 6.4.4.4.	AP-Platform	OAW-AP325 access points	AOS-W 6.4.4.4	AOS-W 6.4.4.8
138686	**Symptom:** A client failed to pass traffic intermittently. The log file for the event listed the reason as **drop pkt as ip not assigned through dhcp**. This issue is resolved by manually clearing the route cache entry. **Scenario:** This issue occurred when a user entry existed in the station table and the route cache entry for the station IP address had the **OH** flag. This issue was observed in switches running AOS-W 6.4.3.5.	Switch-Datapath	All platforms	AOS-W 6.4.3.5	AOS-W 6.4.4.8
138785	**Symptom:** On configuring the **Host Controller Name** and **Master Controller IP Address/DNS name** fields in the AP provisioning profile, the WebUI did not display the field values. The fix ensures that the correct field values are displayed. **Scenario:** This issue was not observed on executing the **show ap provisioning ap-name** command in the CLI. This issue was observed in switches running AOS-W 6.4.3.7.	WebUI	All platforms	AOS-W 6.4.3.7	AOS-W 6.4.4.8
139007	**Symptom:** The **WebCC** process stopped responding and crashed in a switch. The fix ensures that the value of the web_cc_category is always below 82. **Scenario:** This issue occurred when the **show gsm debug channel web_cc_info** command was executed and the webroot returned a value of the web_cc_category, returned that was greater than the maximum value (82). This issue was observed in switches running AOS-W 6.4.2.x, AOS-W 6.4.3.x, or AOS-W 6.4.4.x.	WebCC	All platforms	AOS-W 6.4.3.5	AOS-W 6.4.4.8

Table 4: *Resolved Issues in 6.4.4.8*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
139026	**Symptom:** When multiple clients (VM or physical) initiated Internet Control Message Protoco (ICMP) pings to the same destination IP address almost simultaneously, the ICMP pings from only one client succeeded while those from the other clients failed. This issue is resolved by fixing the ICMP sequence of the Source Network Address Translation (SRC-NAT) in the datapath. **Scenario:** This issue occurred when SRC-NAT—that is, the **ip nat inside** option—was configured in the client VLANs and multiple clients started the ICMP pings to the same destination IP address simultaneously. This issue was not limited to any specific switch model or AOS-W version.	Switch-Datapath	All platforms	AOS-W 6.4.3.7	AOS-W 6.4.4.8
139268 139351	**Symptom:** The **datapath** process in a switch crashed and the switch rebooted unexpectedly. The log file for the event listed the reason as **Datapath timeout**. This issue is resolved by dropping the packets that come over the mobility tunnel from Home Agent (HA) to Foreign Agent (FA) if they cause a bridge miss. **Scenario:** This issue occurred when packets coming over the mobility tunnel from HA to FA caused a bridge miss. This issue was observed in switches running AOS-W 6.4.3.6.	Switch-Datapath	All platforms	AOS-W 6.4.3.6	AOS-W 6.4.4.8
139341	**Symptom:** A branch office switch ignored the branch configuration group **interface VLAN 4094** sub mode configuration including **ip nat outside**. This issue is resolved by moving the VLAN 4094 configuration before **interface vlan 4094** sub mode configuration when a master switch generates the configuration to be pushed to the branch office switch. **Scenario:** This issue occurred because VLAN 4094 was added after all **interface vlan 4094 ...** configuration was received when the configuration was pushed to the branch office switch from a master switch after the branch office switch was reloaded. This issue was observed in branch office switches running AOS-W 6.4.4.5.	Branch Office Switch	All platforms	AOS-W 6.4.4.5	AOS-W 6.4.4.8

Table 4: *Resolved Issues in 6.4.4.8*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
139653	**Symptom:** An AP rebooted unexpectedly. The log file for the event listed the reason as **unknown**. This issue is resolved by disregarding the result of the pre-standard 802.3AT classification method based on the input voltage level measurement. Additionally, the power requested by the AP over LLDP is adjusted from 19.0 W to 20.2 W in normal mode and from 17.1 W to 17.2 W in reduced power mode. This allows an AP to operate during adverse conditions. **Scenario:** This issue occurred because the pre-standard 802.3AT classification created a false positive and an AP operated in full power mode when connected to a switch that was only 802.3AF compliant. Thus, the AP exceeded the limits of the 802.3AF power budget of 12.9 W and consequently rebooted or was current limited by the switch and the log file for the event listed the reason as **unknown**. This issue was observed in OAW-AP220 Series access points connected to PoE switch fetching power.	AP-Platform	OAW-AP220 Series access points	AOS-W 6.4.4.4	AOS-W 6.4.4.8
140121	**Symptom:** A user was unable to create an SNMPv3 community/user string with 6 characters. The fix ensures that an SNMPv3 community/user string can be created with a minimum of 6 characters. **Scenario:** This issue was observed in switches running AOS-W 6.4.3.x or later versions.	SNMP	All platforms	AOS-W 6.4.3.7-FIPS	AOS-W 6.4.4.8
140386	**Symptom:** A switch did not allow the addition of multiple trap host with the same SNMPv3 user. The fix ensures that a switch allows the addition of multiple trap host with the same SNMPvV3 user. **Scenario:** This issue was observed in switches running AOS-W 6.4.3.7.	SNMP	All platforms	AOS-W 6.4.3.7	AOS-W 6.4.4.8

Table 4: *Resolved Issues in 6.4.4.8*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
140447 140889 141215 141481 141911	**Symptom:** The **Guest Provisioning Page** (GPP) in the WebUI did not load as expected. The fix ensures that the GPP loads correctly. **Scenario:** This issue occurred when a GPP account was created and used to log in. This issue was observed in switches running AOS-W 6.4.4.6.	WebUI	All platforms	AOS-W 6.4.4.6	AOS-W 6.4.4.8
140507	**Symptom:** When a client switched from power-save mode to normal mode, it was unable to obtain an IP address although the client entry existed in the user-table of the switch. This issue is resolved by moving the client to the ready state when MAC authentication is completed from the cache. **Scenario:** This issue occurred when the **mac-auth** and **enforce-user-vlan** parameters were enabled and an existing client re-associated. This issue was observed in switches running AOS-W 6.4.4.3.	Base OS Security	All platforms	AOS-W 6.4.4.3	AOS-W 6.4.4.8
140923	**Symptom:** A switch randomly displayed some access points as DOWN and the **Station Management** (STM) process in some access points was busy. This issue is resolved by checking if the length of the packet field representing the information ID is within the value configured for the **ANQP Query Element Length** parameter. **Scenario:** This issue occurred because the packet field representing the information ID length was not checked against the value configured for the **ANQP Query Element Length** parameter. This issue was observed in switches running AOS-W 6.4.2.14.	Station Management	All platforms	AOS-W 6.4.2.14	AOS-W 6.4.4.8

This chapter describes the known and outstanding issues identified in AOS-W 6.4.4.8.

Support for OAW-AP320 Series Access Points

The following features are not supported in OAW-AP320 Series access points:

- Enterprise Mesh
- Turbo QAM
- Modem Support
- Radio Frequency Test (RFT)

If there is any specific bug that is not documented in this chapter, contact Alcatel-Lucent Technical Support with your case number.

Table 5: *Known Issues in 6.4.4.8*

Bug ID	Description	Component	Platform	Reported Version
117155 119427 119959 123347 123772 123880 124583 136369	**Symptom:** The number of clients displayed in the CLI when the **show-user-table** command is executed does not match with the number of clients displayed in the **Monitoring > CONTROLLER > Clients** page of the WebUI. **Scenario:** This issue is observed in switches running AOS-W 6.4.4.0. **Workaround:** None.	WebUI	All platforms	AOS-W 6.4.4.0
122043 127497	**Symptom:** The AppRF dashboard displays **Unknown** or blank roles in the WebUI. **Scenario:** This issue is observed in switches running AOS-W 6.4.2.8. **Workaround:** None.	Base OS Security	All platforms	AOS-W 6.4.2.8
123458	**Symptom:** An AP fails to send Link Layer Discovery Protocol-Media Endpoint Discovery (LLDP-MED) Type-Length-Value (TLV) information after receiving an LLDP packet from a Cisco VoIP phone. **Scenario:** This issue occurs when devices that support LLDP-MED are connected to the downlink Ethernet port of an AP. This issue is observed in access points running AOS-W 6.4.3.3. or later versions. **Workaround:** None.	AP-Platform	All platforms	AOS-W 6.4.3.3
124275	**Symptom:** All clients obtain IP addresses from the same VLAN even though a RADIUS server Vendor-Specific Attribute (VSA) specifies a VLAN pool with multiple VLANs. **Scenario:** This issue occurs when a RADIUS server VSA overrides the VAP VLAN 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. **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

Table 5: *Known Issues in 6.4.4.8*

Bug ID	Description	Component	Platform	Reported Version
124767 124841	**Symptom:** When a Session Initiation Protocol (SIP) call is made using the ClearSea application, a Call Detail Record (CDR) is not generated. The call detail is not visible on the Unified Communication and Collaboration (UCC) dashboard. The media traffic is not prioritized. **Scenario:** The issue is observed only when the SIP signaling message is large and is delivered in multiple Transmission Control Protocol (TCP) segments. These TCP segments are received out of order. This issue is observed in switches running AOS-W 6.4.2.4. **Workaround:** None.	Unified Communication and Collaboration	All platforms	AOS-W 6.4.2.4
126793 128230 131927 132149 132304 134889 137322 140746	**Symptom:** An OAW-AP324 access point crashes unexpectedly. The log file for the event lists the reason as **kernel panic: PC is at nss_core_handle_napi**. **Scenario:** This issue is observed in OAW-AP324 access points running AOS-W 6.4.4.1. **Workaround:** None.	AP-Wireless	OAW-AP324 access points	AOS-W 6.4.4.1
127848	**Symptom:** A Remote Access Point (RAP) fails to re-establish its Point-to-Point Protocol over Ethernet (PPPoE) connection to the backup Local Management Switch (LMS) IP address when the primary LMS IP address is not available. **Scenario:** This issue is observed in OAW-AP205 or OAW-AP274 access points running AOS-W 6.4.4.0. **Workaround:** None.	Remote Access Point	OAW-AP205 and OAW-AP274 access points	AOS-W 6.4.4.0
128457	**Symptom:** The **wlsxMeshNodeEntryChanged** trap generated by a switchdoes not have mesh link reset information. **Scenario:** This issue is observed in switches running AOS-W 6.4.3.1. **Workaround:** None.	SNMP	All platforms	AOS-W 6.4.3.1
129096	**Symptom:** The Lightweight Directory Access Protocol (LDAP) connection in a switch keeps resetting due to a search failure. As a result, the switch fails to authenticate or query the users using the LDAP server. **Scenario:** This issue is observed when a search request from a switch to an LDAP server is redirected to another LDAP server that does not support anonymous queries. This issue is not limited to any specific switch model or AOS-W version. **Workaround:** Ensure that the referred LDAP server supports anonymous queries.	LDAP	All platforms	AOS-W 6.4.2.12

Table 5: *Known Issues in 6.4.4.8*

Bug ID	Description	Component	Platform	Reported Version
130981	**Symptom:** A switch reboots unexpectedly. The log file for the event lists the reason as **datapath timeout**. **Scenario:** This issue occurs when the **copy** command has the **** (backslash) character at the end of the destination folder name. For example: **copy flash: crash.tar ftp: 10.1.1.1. test-user \ArubaOS\\ crash.tar** ArubaOS misinterprets the **** (backslash) character causing a memory fault. This issue is observed in switches running AOS-W 6.4.4.0. **Workaround:** None.	Switch-Platform	All platforms	AOS-W 6.4.4.0
131857	**Symptom:** The Type of Service (TOS) value of 0 does not take effect when it is set in the user-role. **Scenario:** This issue is observed in switches running AOS-W 6.4.3.3. **Workaround:** None.	Switch-Datapath	All platforms	AOS-W 6.4.3.3
132714	**Symptom:** When a user tries to add a static Address Resolution Protocol (ARP) entry, a switch displays the error message **Cannot add static ARP entry**. The log file for the event lists the reason 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. **Workaround:** None.	Switch-Platform	All platforms	AOS-W 6.4.3.4
134417	**Symptom:** Clients fail to get an IP address from an external DHCP server. **Scenario:** This issue occurs because the switch drops the DHCP return message from the DHCP server. This issue is observed in OAW-4306 Series and OAW-M3 switches running AOS-W 6.4.2.14. **Workaround:** None.	Switch-Datapath	OAW-4306 Series and OAW-M3 switches	AOS-W 6.4.2.14
135029 137672	**Symptom:** The **Monitoring > NETWORK > All Access Points** page in the WebUI displays an incorrect user count. **Scenario:** A mismatch in the user count is observed when seen in the **Monitoring** and **Dashboard** pages of the WebUI. This issue is not observed in the CLI. This issue is observed in controllers running AOS-W 6.4.2.12, AOS-W 6.4.3.x, or AOS-W 6.4.4.x. **Workaround:** None.	WebUI	All platforms	AOS-W 6.4.2.12

Table 5: *Known Issues in 6.4.4.8*

Bug ID	Description	Component	Platform	Reported Version
135132	**Symptom:** An AP crashes unexpectedly. The log file for the event lists the reason as **ar5416IsInterruptPending+0x24/0x98 [ath_hal]**. **Scenario:** This issue occurs when spectrum monitoring is enabled in the AP. This issue is observed in 100 Series access points running AOS-W 6.4.3.6. **Workaround:** None.	AP-Wireless	100 Series access points	AOS-W 6.4.3.6
136501	**Symptom:** A switch crashes unexpectedly. The log file for the event lists the reason as **Datapath timeout (Intent:cause:register 56:86:50:2)**. **Scenario:** This issue occurs because of a memory corruption. This issue is observed in switches running AOS-W 6.4.3.4. **Workaround:** None.	Base OS Security	All platforms	AOS-W 6.4.3.4
138438	**Symptom:** A user cannot enable DHCP client on a VLAN using the WebUI. **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
139174	**Symptom:** On sending an SNMP message for a client, the 64-bit Rx/Tx rate fields are not populated by an AP. **Scenario:** This issue is observed when clients are associated to OAW-AP320 Series access points running AOS-W 6.4.4.x. **Workaround:** None.	Station Management	OAW-AP320 Series access points	AOS-W 6.4.4.3
143101	**Symptom:** A client cannot connect to an AP. The log file for the event lists the reason as **capability requested by STA unsupported by AP**. **Scenario:** This issue occurs during HA failover and fallback when no VLAN is assigned for the virtual AP profile that is configured in tunnel mode. This issue is observed when clients are associated to OAW-AP320 Series access points running AOS-W 6.4.2.5. **Workaround:** None.	AP-Platform	OAW-AP320 Series access points	AOS-W 6.4.2.5

This chapter details 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

- 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 WebUIs 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) and OAW-4504 switches 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 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 35.)

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 6.4.4.0 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

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 6.4.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. 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 34 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 34 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 34 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 34.

For proper operation, all switches in the network must be upgraded with the same version of AOS-W software. For redundant (VRRP) environments, 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 6.4.4.8

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

Instructions on Installing FIPS Software

Follow these steps to install the FIPS software 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 6.4.4.8

The following sections provide the procedures for upgrading the switch to AOS-W 6.4.4.8 by using the WebUI or 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 33.

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 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 before upgrading to AOS-W 6.4.4.8.

NOTE

When upgrading from an existing AOS-W 6.4.4.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 6.4.4.8.

- 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 to AOS-W 6.4.4.8 on page 36 to install the interim version of AOS-W, and then repeat steps 1 through 11 of the procedure to download and install AOS-W 6.4.4.8

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 6.4.4.8 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.

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 34 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. The OAW-RAP5/OAW-RAP5WN reboots to complete the provisioning image upgrade.

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 33.

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 to AOS-W 6.4.4.8 on page 36.

Follow steps 2 through 7 of the procedure described in Upgrading to AOS-W 6.4.4.8 on page 36 to install the interim version of AOS-W, and then repeat steps 1 through 7 of the procedure to download and install AOS-W 6.4.4.8

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 6.4.4.8 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**.
```
(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 Seriesswitches.

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 34 for information on creating a backup.

Downgrading

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

CAUTION

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 6.4.4.8 are lost after the downgrade (this warning does not apply to upgrades from AOS-W 3.4.x to AOS-W 6.1).

CAUTION

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 6.4.4.8 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.

CAUTION

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 34.
2. Verify that the control plane security is disabled.
3. Set the switch to boot with the previously saved pre-AOS-W 6.4.4.8 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 6.4.4.8 flash backup from the file stored on the switch. Do not restore the AOS-W 6.4.4.8 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 6.4.4.8, the changes do not appear in RF Plan in the downgraded AOS-W version.
   - If you installed any certificates while running AOS-W 6.4.4.8, 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 6.4.4.2. Partition 0, the default boot partition, contains the AOS-W 6.4.4.8 image.

   ```
   #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 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.