AOS-W 6.4.4.6

Alcatel·Lucent
Enterprise

Release Notes

Copyright Information

Legal Notice

The use of Alcatel-Lucent switching platforms and software, by all individuals or corporations, to terminate Cisco or Nortel VPN client devices constitutes complete acceptance of liability by that individual or corporation for this action and indemnifies, in full, Alcatel- Lucent from any and all legal actions that might be taken against it with respect to infringement of copyright on behalf of Cisco Systems or Nortel Networks.

Revision History

The following table lists the revision history of this document.

Table 1: *Revision History*

Revision	Change Description
Revision 01	Initial release.

Chapter 1
Release Overview

AOS-W 6.4.4.6 is a software patch release that includes new features and enhancements introduced in this release and fixes to issues identified in previous releases.

NOTE

See the Upgrade Procedure on page 32 for instructions on how to upgrade your switch to this release.

Use the following links navigate to the corresponding topics:

- New Features on page 10 describes the features and enhancements introduced in this release.
- Regulatory Updates on page 13 lists the regulatory updates introduced in this release.
- Resolved Issues on page 14 describes the issues resolved in this release
- Known Issues on page 25 describes the known and outstanding issues identified in this release.
- Upgrade Procedure on page 32 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

Chapter 2
New Features

This chapter describes the new features and/or enhancements introduced in AOS-W 6.4.4.6.

AP-Platform

802.11k Support for OAW-AP320 Series Access Points

Starting from AOS-W 6.4.4.6, the OAW-AP320 Series access points support 802.11k.

Unified Communication and Collaboration

Associate Idle VoIP Client

Starting from AOS-W 6.4.4.6, idle Voice over Internet Protocol (VoIP) clients can associate with access points when the Call Handoff Reservation (CHR) limit or Peak Capacity Threshold (PCT) is reached. This setting appears in the switch CLI and WebUI.

In the CLI

A new **allow-idle-voip-client** parameter is introduced in the **wlan voip-cac-profile** command. By default, the **allow-idle-voip-client** parameter is disabled.

wlan voip-cac-profile

The following new parameter is introduced in the **wlan voip-cac-profile** command:

Table 4: *Associate Idle VoIP Client*

Parameter	Description	Default
allow-idle-voip-client	Enable/Disable idle VoIP clients to associate after CHR limit or PCT is reached.	Disabled

In the WebUI

A new **Allow Idle VOIP Client** parameter is introduced in **VoIP Call Admission Control Profile**. To configure the **Allow Idle VOIP Client** parameter:

1. Navigate to **Configuration > Wireless > AP Configuration**.
2. Select a profile under **AP Group**.

3. Select **QoS > VoIP Call Admission Control** under **Profiles**
4. Select **Advanced** under Profile Details.
5. Select **Allow Idle VOIP Client** parameter.
6. Click **Apply**.

Customize AP Console Logging Level

Starting from AOS-W 6.4.4.6, the logging level of the AP console can be customized. You can configure this parameter only from the switch CLI.

In the CLI

A new **console-log-lvl** parameter is introduced in the **ap system-profile** command. By default, the **console-log-lvl** parameter is set to emergencies.

ap system-profile

The following new parameter is introduced in the **ap system-profile** command:

Table 5: *AP Console Logging Level*

Parameter	Description	Default
console-log-lvl	Customize the logging level of the driver log prints displayed in the AP console. The logging level includes: Alerts–Log messages that require immediate action Critical–Log messages related to critical conditions Debugging–Log debug messages Emergencies–Log messages related to unusable system Errors–Log messages related to error conditions Informational–Log informational messages Notifications–Log messages related to normal but significant conditions Warnings–Log messages related to warning conditions	Emergencies

Unified Communication and Collaboration

Associate Idle VoIP Client

Starting from AOS-W 6.4.4.6, idle Voice over Internet Protocol (VoIP) clients can associate with access points when the Call Handoff Reservation (CHR) limit or Peak Capacity Threshold (PCT) is reached. This setting appears in the switch CLI and WebUI.

In the CLI

A new **allow-idle-voip-client** parameter is introduced in the **wlan voip-cac-profile** command. By default, the **allow-idle-voip-client** parameter is disabled.

wlan voip-cac-profile

The following new parameter is introduced in the **wlan voip-cac-profile** command:

Table 6: *Associate Idle VoIP Client*

Parameter	Description	Default
allow-idle-voip-client	Enable/Disable idle VoIP clients to associate after CHR limit or PCT is reached.	Disabled

In the WebUI

A new **Allow Idle VOIP Client** parameter is introduced in **VoIP Call Admission Control Profile**. To configure the **Allow Idle VOIP Client** parameter:

1. Navigate to **Configuration > Wireless > AP Configuration**.
2. Select a profile under **AP Group**.
3. Select **QoS > VoIP Call Admission Control** under **Profiles**
4. Select **Advanced** under Profile Details.
5. Select **Allow Idle VOIP Client** parameter.
6. Click **Apply**.

Chapter 3
Regulatory Updates

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 6.4.4.6:

- DRT-1.0_54367

Chapter 4
Resolved Issues

This chapter describes the issues resolved in AOS-W 6.4.4.6.

Table 7: *Resolved Issues in 6.4.4.6*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
117815	**Symptom:** A user could not change the maximum retries setting of an Access Point (AP). The fix allows a user to change the maximum retries setting. **Scenario:** This issue was observed in an OAW-AP324 or OAW-AP325 AP running AOS-W 6.4.4.0.	AP-Wireless	OAW-AP324 or OAW-AP325 access points	AOS-W 6.4.4.0	AOS-W 6.4.4.6
121020 124020	**Symptom:** An Access Point (AP) crashed unexpectedly. The log file for the event listed the reason as **Reboot caused by kernel panic: Fatal exception**. This issue is resolved by limiting the number of in-transit broadcasts to 128 and the maximum length of the queues to 32 bits. **Scenario:** This issue occurred because the memory was exhausted from several queues with several broadcasts. This issue was observed in OAW-AP210 Series, OAW-AP224, OAW-AP225, OAW-AP228, OAW-AP275, or OAW-AP277 AP running AOS-W 6.4.2.3.	AP-Wireless	OAW-AP210 Series, OAW-AP224, OAW-AP225, OAW-AP228, OAW-AP275, or OAW-AP277 access points	AOS-W 6.4.2.3	AOS-W 6.4.4.6
122695 128425 134457	**Symptom**: A Remote Access Point (RAP) failed to come online and displayed the **check_aruba_vid: STRAP License not available** error message. This issue is resolved by sending the RAP feature limit and bitmap updates to the applications. **Scenario**: This issue occurred after upgrading a switch to AOS-W 6.4.4.1 and converting a Campus Access Point (CAP) to a RAP.	Licensing	All platforms	AOS-W 6.4.4.1	AOS-W 6.4.4.6
124173	**Symptom**: An unexpected speed mismatch error was observed on the 10G port-channel of OAW-M3 switches. This issue is resolved by calculating the correct speed of the port channel. **Scenario**: This issue occurred because a wrong speed was calculated for the port channel. This issue was observed in OAW-M3 switches running AOS-W 6.3.1.x, AOS-W 6.4.3.x, AOS-W or 6.4.4.x.	Interface	OAW-M3 switches	AOS-W 6.4.2.4	AOS-W 6.4.4.6

Table 7: *Resolved Issues in 6.4.4.6*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
125183 137806	**Symptom**: The **Station Management Module** (STM) process crashed in a switch. The fix ensures that the STM process does not crash while processing an Access Point (AP) whose system profile has not been created yet. **Scenario**: This issue occurred when the STM process was processing an AP whose system profile had not yet been created. 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.	Station Management	All platforms	AOS-W 6.4.4.4	AOS-W 6.4.4.6
126418	**Symptom**: When the **show ap database flags D** command was executed on a master switch, the output incorrectly displayed the **D** flag (dirty or no configuration) for an Access Point (AP) that had good configuration. This issue is resolved by ensuring that the **D** flag is retrieved only from local switches where an AP is terminated. On the master switch, the **D** flag is not displayed unless the AP is terminated on the master switch. **Scenario**: This issue occurred when an AP was connected to a local switch and not the master switch. This issue was observed in switches running AOS-W 6.4.x in a master-local topology.	AP-Platform	All platforms	AOS-W 6.4.2.10	AOS-W 6.4.4.6
128466	**Symptom**: A switch displayed the **Invalid TLS version** error message in authentication trace buffer after uploading a new certificate for Extensible Authentication Protocol-Protected Extensible Authentication Protocol (EAP-PEAP) authentication. This resulted in user authentication failure. This issue is resolved by adding zeros to the private key so that it is 256 bytes in length. **Scenario**: This issue occurred while decrypting the pre-master secret key when a client attempted Transport Layer Security (TLS) for 802.1X authentication. 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.	Base OS Security	All platforms	AOS-W 6.4.2.12	AOS-W 6.4.4.6

Table 7: *Resolved Issues in 6.4.4.6*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
129055 137138	**Symptom**: A switch stopped responding and rebooted unexpectedly. While collecting the crash logs, the switch crashed again and over-wrote the crash logs of the previous crash. This issue is resolved by removing the access to the device name for a given interrupt number in the crash path. **Scenario**: This issue occurred while collecting the crash logs in a OAW-4650 switch. This issue was observed in OAW-4650 switches running AOS-W 6.3.1.x, AOS-W 6.4.2.x, AOS-W 6.4.3.x, or AOS-W 6.4.4.x.	Switch-Platform	OAW-4650 switches	AOS-W 6.4.4.1	AOS-W 6.4.4.6
129464	**Symptom**: Clients took long time to connect after a High Availability (HA) failover. The log file for the event listed the reason as **Station Up Message to Controller Timed Out**. This issue is resolved by cleaning the deferred deauthentication list. **Scenario**: This issue occurred when the acknowledgment for the **STA UP** message arrived after the message list was moved to the deferred deauthentication list and the **STA UP** message was not processed normally. 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.	AP-Wireless	All platforms	AOS-W 6.4.3.2	AOS-W 6.4.4.6
129535 134047	**Symptom**: An Access Point (AP) did not receive Link Layer Discovery Protocol (LLDP) packets from the Local Area Network (LAN) port of a switch. Improvements in the wireless driver of the AP resolves this issue. **Scenario**: This issue occurred because of wrong positioning of the Ethernet header. This issue was observed in an AP running AOS-W 6.4.3.x or AOS-W 6.4.4.x.	AP-Platform	All platforms	AOS-W 6.4.3.3	AOS-W 6.4.4.6

Table 7: *Resolved Issues in 6.4.4.6*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
129698 132761	**Symptom**: A client experienced a one-way VoIP communication. The fix ensures that the Session Initiation Protocol Application Level Gateway (SIP ALG) uses the right datapath opcode to send the SIP 486 message so that the route cache entry for the client remains intact. **Scenario**: This issue was seen under the following circumstances: ● Call Admission Control (CAC) was enabled. ● The switch blocked the SIP-based call due to CAC. ● On clearing the CAC limitation, when a subsequent SIP-based call was made to or from the client, the switch dropped all RTP and RTCP packets to this client. This issue was seen because the route cache entry for the client was modified when SIP ALG sent a SIP 486 message to the client for blocking the call. This allowed the switch to detect an IP spoofing because the route cache entry for the client indicated the wrong MAC address. This issue was observed in switches running AOS-W 6.4.x.	Unified Communication and Collaboration	All platforms	AOS-W 6.4.2.5	AOS-W 6.4.4.6
129877 138133	**Symptom**: The **tx_flush reset** process did not recover a frozen FW tx pcu in an Access Point (AP). This resulted in a burst of tx_flush resets. This issue is resolved by applying cold reset after a FW tx pcu freezes. **Scenario**: This issue was observed in an OAW-AP325 AP running AOS-W 6.4.4.2.	AP-Wireless	OAW-AP325 access points	AOS-W 6.4.4.2	AOS-W 6.4.4.6
130611	**Symptom**: A user failed to set the **no spanning-tree** command for a port-channel. The fix ensures that a user can set the command for a port-channel. **Scenario**: This issue was observed when a port-channel was changed to trunk mode in switches running AOS-W 6.4.4.x.	Port-Channel	All platforms	AOS-W 6.4.4.0	AOS-W 6.4.4.6

Table 7: *Resolved Issues in 6.4.4.6*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
131118 133267	**Symptom**: A switch rebooted unexpectedly. The log file for the event listed the reason as **datapath timeout**. This issue is resolved by letting the FP reassemble the IP fragments. **Scenario**: This issue occurred when the **datapath** module received fragmented DHCP packets. This issue occurred in switches having single SP. This issue was observed in OAW-4306 Series, OAW-4x04 Series, or OAW-M3 switches running AOS-W 6.4.x.	Switch-Datapath	OAW-4306 Series, OAW-4x04 Series, or OAW-M3 controllers	AOS-W 6.4.2.5	AOS-W 6.4.4.6
131815 131874 132843 133107 136379	**Symptom**: The **Monitoring** page in the WebUI displayed incorrect count of active clients when searching with filters like Extended Service Set Identifier (ESSID). Additionally, the output of the **show ipv4 user-table rows <starting-row-number> <number-of-rows>** command displayed more records than the pagination count. This issue is resolved by applying filters before selecting the rows on the filtered list. **Scenario**: This issue occurred because the rows were selected before the filters were applied on the user entries. This issue was observed in switches running AOS-W 6.4.2.14 or later versions of AOS-W.	WebUI	All platforms	AOS-W 6.4.2.14	AOS-W 6.4.4.6
132231 132593 135251 136274 137409 137857 138030 138213 138651	**Symptom**: Users observed high memory utilization in the **Station Management Module** (STM) when a switch was upgraded to AOS-W 6.4.3.x. The fix ensures that monitoring- and statistics-related information is properly cleaned up when a station leaves the network. **Scenario**: This issue occurred because a change to one of the station identifiers in the system led to some monitoring and statistics information not being cleaned up when a station left the network. The 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 6.4.3.6	AOS-W 6.4.4.6
133562 133565 133566 133569 134162	**Symptom**: An Access Point (AP) crashed and rebooted unexpectedly. This issue is resolved by not copying the Virtual Memory Area (VMA) of the parent process. **Scenario**: This issue occurred when a child process was released. This issue was observed in an OAW-AP124 AP running AOS-W 6.4.4.3.	AP-Platform	OAW-AP124 access points	AOS-W 6.4.4.3	AOS-W 6.4.4.6

Table 7: *Resolved Issues in 6.4.4.6*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
133564	**Symptom**: An Access Point (AP) rebooted unexpectedly. The log file for the event listed the reason as **Reboot caused by kernel page fault at virtual address 0000000100000007, epc == ffffffff80268c20, ra == ffffffff80268ba8**. This issue is resolved by allocating memory pages from the cache and marking them as reserved. **Scenario**: This issue occurred because the memory pages were allocated from the freelist for polling. This issue was observed in an OAW-AP125 AP running AOS-W 6.4.4.3.	AP-Platform	OAW-AP125 access points	AOS-W 6.4.4.3	AOS-W 6.4.4.6
133667 134471 135526	**Symptom**: Clients with Realtek chips experienced low throughput when the **g radio basic rates** or **g tx rates** included 802.11b rate. This issue is resolved by removing the ACK timeout configuration and using the default value in the wireless driver. **Scenario**: This issue occurred because a small ACK timeout value allowed an Access Point (AP) to ignore the **Binding Acknowledgment** (BA) message sent by a client with Realtek chip. This issue was not limited to any specific switch model and was observed in switches running AOS-W 6.4.4.3.	AP-Wireless	All platforms	AOS-W 6.4.4.3	AOS-W 6.4.4.6
134279	**Symptom**: The eth1 port of an OAW-AP225 Access Point (AP) displayed the link status as **UP** although the link status was **DOWN**. The fix ensures that the switch displays the correct physical link status of the AP. **Scenario**: This issue was observed under the following circumstances: ● OAW-AP225 detects POE+ power. ● On detecting POE+ power, the eth1 port on the AP is enabled with full functionality. ● The switch sends LLDP POE with 13.0W power. ● As the power is less, the periodic timer shuts the eth1 port on the AP. But the **show ap debug system-status** command displayed the link status as **UP** although the link status was **DOWN**. This issue was observed in OAW-AP225 access point running AOS-W 6.4.3.x or AOS-W 6.4.4.x.	AP-Platform	OAW-AP225 access points	AOS-W 6.4.3.5	AOS-W 6.4.4.6

Table 7: *Resolved Issues in 6.4.4.6*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
134507	**Symptom**: The call count remained even after a Session Initiation Protocol (SIP) session was terminated by a BYE request. This issue is resolved by not decrementing the call count if it is already 0. **Scenario**: This issue occured when mobile IP was configured, a client roamed from a Home Agent (HA) to Foreign Agent (FA), received a SIP call while in FA, and returned to the HA. This issue was observed in switches running AOS-W 6.4.3.1.	Unified Communication and Collaboration	All platforms	AOS-W 6.4.3.1	AOS-W 6.4.4.6
134534	**Symptom**: Real-time Transport Protocol (RTP) was sent on the wrong Virtual Local Area Network (VLAN) for a client that roamed in to a Foreign Agent (FA). This issue is resolved by ensuring that the **datapath** module always creates a session with a redirect flag **R** for a visitor client on the FA. **Scenario**: This issue occurred when a Voice over Internet Protocol (VoIP) client roamed in to FA during active sessions and the switch created a session entry on the FA without a redirect flag **R** if the L3 user entry was missing for the client. This Issue may be observed with non-VOIP clients too. This issue was observed in switches running AOS-W 6.4.3.x or AOS-W 6.4.4.x.	Mobility	All platforms	AOS-W 6.4.3.1	AOS-W 6.4.4.6
134723	**Symptom**: A wired client did not complete wired Extensible Authentication Protocol (EAP) authentication in bridge mode after associating with an Access Point (AP). This issue is resolved by forwarding the packets to an internal port. **Scenario**: This issue occurred because an AP dropped the undersized Extensible Authentication Protocol over LAN (EAPoL) frames. This issue was observed in an OAW-AP205H AP running AOS-W 6.4.3.6.	AP-Platform	OAW-AP205H access points	AOS-W 6.4.3.6	AOS-W 6.4.4.6
135044	**Symptom**: An Access point (AP) crashed and rebooted frequently. The log file for the event listed the reason as **- CPU 0 Unable to handle kernel paging request at virtual address 00000000000000c8, epc == ffffffff80227b98, ra == ffffffff80227ba0**. This issue is resolved by making changes to the kernel. **Scenario**: This issue was observed in OAW-AP120 Series access points running AOS-W 6.4.4.4.	AP-Wireless	OAW-AP120 Series access points	AOS-W 6.4.4.4	AOS-W 6.4.4.6

Table 7: *Resolved Issues in 6.4.4.6*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
135089	**Symptom**: An Access Point (AP) crashed and rebooted unexpectedly. The log file for the event listed the reason as **AP Reboot caused by kernel panic: Fatal exception**. This issue is resolved by adding protection to the kernel against memory corruption or wrong access. **Scenario**: This issue occurred because of memory corruption or wrong access. This issue was observed in OAW-AP320 Series access points running AOS-W 6.4.4.4.	AP-Platform	OAW-AP320 Series access points	AOS-W 6.4.4.4	AOS-W 6.4.4.6
135121	**Symptom**: A switch crashed and 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 enhancing the Internet Protocol version 6 (IPv6) firewall to drop packets with the wrong application payload. **Scenario**: This issue occurred when unnecessary padding between the IPv6 and Transmission Control Protocol (TCP) header created wrong application payload. 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.	Switch-Datapath	All platforms	AOS-W 6.4.4.3	AOS-W 6.4.4.6
135131	**Symptom**: Clients randomly failed to send or receive traffic when associated to a Service Set Identifier (SSID). This issue is resolved by eliminating a memory leak in the **authentication** process. **Scenario**: This issue occurred because the **authentication** process ran out of memory. This issue was observed in switches running AOS-W 6.3.1.x, AOS-W 6.4.2.x, AOS-W 6.4.3.x, or AOS-W 6.4.4.x.	Base OS Security	All platforms	AOS-W 6.4.4.4	AOS-W 6.4.4.6
135290	**Symptom**: The Adaptive Radio Management (ARM) history entries showed that a RADAR-contaminated channel was used within the non-occupancy period (30 minutes). This issue is resolved by adding a channel to the candidate list of channels only if it is not contaminated. **Scenario**: This issue occurred because a random channel was selected from a candidate list of channels without verifying if that channel was already under RADAR detection. This issue was observed in an OAW-AP274 Access Point (AP) running AOS-W 6.4.4.0.	AP-Wireless	OAW-AP274 access points	AOS-W 6.4.4.0	AOS-W 6.4.4.6

Table 7: *Resolved Issues in 6.4.4.6*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
135411	**Symptom**: An Access Point (AP) did not send frames in the 2.4 GHz channel. Improvements in the wireless driver of the AP resolves this issue. **Scenario**: This issue occurred when quiet timers were enabled and a firmware cold reset was performed. This issue was observed in OAW-AP320 Series access points running AOS-W 6.4.4.4.	AP-Wireless	OAW-AP320 Series access points	AOS-W 6.4.4.4	AOS-W 6.4.4.6
135678	**Symptom**: A switch randomly dropped **SIP INVITE** messages due to which users were unable to resume a Session Initiation Protocol (SIP) call which was placed on hold. This issue is resolved by sending the SIP signaling packets back to datapath after they are processed, irrespective of whether the processing succeeded or failed. **Scenario**: This issue occurred when SIP ALG failed due to which a switch dropped the subsequent **SIP INVITE** messages. This issue was observed in switches running AOS-W 6.4.3.x or AOS-W 6.4.4.x.	Unified Communication and Collaboration	All platforms	AOS-W 6.4.4.4	AOS-W 6.4.4.6
135855	**Symptom**: The **authentication** process crashed while updating the netdestination. This issue is resolved by handling the netdestination update properly for web-cc-based policies. **Scenario**: This issue was observed when the **authentication** process attempted to update the netdestination on the web-cc reference in the session Access Control List (ACL) policy. This issue was observed in switches running AOS-W 6.4.2.12, AOS-W 6.4.3.x, or AOS-W 6.4.4.x.	Base OS Security	All platforms	AOS-W 6.4.2.12	AOS-W 6.4.4.6
135884 136028 136531	**Symptom**: The **syslog** module sent messages to the Bluetooth Low Energy (BLE) relay process. This issue is resolved by preventing the **syslog** module from sending a message to BLE relay process because the BLE relay process is disabled in OAW-M3 or OAW-4306 Series switches. **Scenario**: This issue was observed in OAW-M3 and OAW-4306 Series switches running ArubaOS 6.4.3.4.	Bluetooth Low Energy	OAW-M3 or OAW-4306 Series switches	AOS-W 6.4.3.4	AOS-W 6.4.4.6

Table 7: *Resolved Issues in 6.4.4.6*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
135949	**Symptom**: Bridge users were unable to pass traffic. The fix ensures that the bridge users are able to pass traffic. **Scenario**: This issue was observed when a vast number of users connected to a decrypt-tunnel forwarding mode Virtual Access Point (VAP) profile and then disconnected. The Access Point (AP) added L2 user entry for the decrypt-tunnel forwarding mode users. The AP did not delete the L2 user entries when the decrypt-tunnel forwarding mode client disconnected. The user entries reached the maximum threshold and when the client tried to connect to the bridge VAP, the AP could not create user entries for the bridge users. This issue was observed in switches running AOS-W 6.3.1.x, AOS-W 6.4.2.x, AOS-W 6.4.3.x, or AOS-W 6.4.4.x.	AP-Datapath	All platforms	AOS-W 6.4.3.6	AOS-W 6.4.4.6
135959	**Symptom**: When the **Nat Outside** parameter was configured in the WebUI, the master switch failed to push this configuration to the Branch office Switch (BoC). The fix ensures that the master switch pushes the **Nat Outside** configuration of the uplink VLAN to the branch office switch. **Scenario**: This issue was observed in OAW-40xx Series switches running AOS-W 6.4.4.4.	WebUI	OAW-40xx Series switches	AOS-W 6.4.4.4	AOS-W 6.4.4.6
136108	**Symptom**: An Access Point (AP) rebooted unexpectedly. The log file for the event listed the reason as **Reboot caused by kernel panic: Rebooting the AP because of FW ASSERT**. Improvements in the wireless driver of the AP resolves this issue. **Scenario**: This issue was observed in an OAW-AP325 AP running AOS-W 6.4.4.4.	AP-Wireless	OAW-AP325 access points	AOS-W 6.4.4.4	AOS-W 6.4.4.6

Table 7: *Resolved Issues in 6.4.4.6*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
136109	**Symptom**: An Access Point (AP) rebooted unexpectedly. The log file for the event listed the reason as **Reboot caused by kernel panic: Fatal exception in interrupt**. This issue is resolved by avoiding memory corruption. **Scenario**: This issue occurred because of memory corruption. This issue was observed in an OAW-AP325 AP running AOS-W 6.4.4.4.	AP-Datapath	OAW-AP325 access points	AOS-W 6.4.4.4	AOS-W 6.4.4.6
137956	**Symptom**: An Access Point (AP) crashed and rebooted unexpectedly. The log file for the event listed the reason as **Reboot caused by kernel panic: Fatal exception in interrupt**. Improvements in the wireless driver of the AP resolves this issue. **Scenario**: This issue was observed in an OAW-AP325 AP running AOS-W 6.4.4.4.	AP-Wireless	OAW-AP325 access points	AOS-W 6.4.4.4	AOS-W 6.4.4.6
138772	**Symptom**: An Access Point (AP) operated in the 802.3af mode. This issue is resolved by comparing the allocated power to the optimization power and enabling the Ethernet port when the allocated power is sufficient. **Scenario**: This issue occurred when AP power optimization option was enabled. This issue was observed in a OAW-AP225 or OAW-AP325 AP running AOS-W 6.4.4.5.	AP-Platform	OAW-AP225 or OAW-AP325 access points	AOS-W 6.4.4.5	AOS-W 6.4.4.6

Known Issues

This chapter describes the known and outstanding issues identified in AOS-W 6.4.4.6.

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)

NOTE

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

Table 8: *Known Issues in 6.4.4.6*

Bug ID	Description	Component	Platform	Reported Version
123458	**Symptom:** An Access Point (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 Voice over Internet Protocol (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 an AP running ArubaOS 6.4.3.3. or later versions of AOS-W. **Workaround:** None.	AP-Platform	All platforms	AOS-W 6.4.3.3
123748 138762	**Symptom:** When a switch is rebooted, an Access Point (AP) that is connected to the switch reboots continuously. **Scenario:** This issue is observed in an OAW-AP225 AP running AOS-W 6.4.2.5. **Workaround:** None.	AP-Platform	OAW-AP225 access points	AOS-W 6.4.2.5
124136	**Symptom:** A client fails to connect to an SSID. The log file for the event lists the reason as **Capability requested by STA unsupported by AP**. **Scenario:** This issue occurs during a failover in a High Availability (HA) setup, when no Virtual Local Area Network (VLAN) is assigned for a Virtual Access Point (VAP) profile and the VAP is configured in tunnel mode. **Workaround:** Configure a VLAN ID in the VAP profile by using the **vlan** CLI command.	AP-Wireless	All platforms	AOS-W 6.4.2.5
124275	**Symptom:** All clients obtain IP addresses from the same Virtual Local Area Network (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 Virtual Access Point (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
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 details 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

Table 8: *Known Issues in 6.4.4.6*

Bug ID	Description	Component	Platform	Reported Version
125862	**Symptom:** A user fails to add a Virtual Local Area Network (VLAN) to the port channel by using the switch WebUI. **Scenario:** This issue is observed in both master and local switches running AOS-W 6.4.x in master-standby-local topology. **Workaround:** Add the VLAN to the port channel by using the switch CLI.	WebUI	All platforms	AOS-W 6.4.2.5
126713	**Symptom:** A switch continues to forward authentication requests to a server that is out of service. **Scenario:** This issue occurs when an authentication server goes out of service after authenticating a user and the same server is reused for authentication in the next instance. The authentication server stored in user context is reused even if the server is out of service. This issue is observed in switches running AOS-W 6.4.2.5. **Workaround:** None.	Base OS Security	All platforms	AOS-W 6.4.2.5
127848	**Symptom:** A Remote Access Point (RAP) fails to reconnect its Point-to-Point Protocol over Ethernet (PPPoE) connection to the backup Local Management Switch (LMS) when the primary LMS is not available. **Scenario:** This issue is observed in an OAW-AP205 or OAW-AP274 Access Point (AP) running AOS-W 6.4.4.0. **Workaround:** None	Remote AP	OAW-AP205 or OAW-AP274 access points	AOS-W 6.4.4.0
128552	**Symptom:** A client that is connected to an Access Point (AP) loses connectivity for a short period of time on each day at the same time. **Scenario:** This issue is observed when a station is in hardware sleep and does not send a deauthentication request. This issue is observed in an OAW-AP215 Access Point (AP) running AOS-W 6.4.2.8. **Workaround:** None.	AP-Platform	OAW-AP215 access points	AOS-W 6.4.2.8
128916 132353 133884 138015	**Symptom:** A switch denies access to users. The log file for the event lists the reason as **drop pkt as ip not assigned through dhcp**. Users are not added to the station/user-table in the switch. **Scenario:** This issue is observed in switches running AOS-W 6.3.1.16. **Workaround:** None.	Switch-Datapath	All platforms	AOS-W 6.3.1.16

Table 8: *Known Issues in 6.4.4.6*

Bug ID	Description	Component	Platform	Reported Version
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
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 with the \\ (backslash) characters at the end of the command is executed. 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

131445	**Symptom:** When a client roams using 802.11r fast handoff, it gets an IP address from a Virtual Local Area Network (VLAN) mapped in the Virtual Access Point (VAP) profile although it is supposed to get an IP address from a VLAN derived from the Vendor-Specific Attribute (VSA).
	Scenario: This issue is observed for an 802.1X authenticated client when it roams using 802.11r fast handoff. This issue is observed in switches running AOS-W 6.3.x or AOS-W 6.4.x.
	Workaround: Disable the 802.11r capability from the SSID profile by using the following CLI commands:
	`(host) (config) #wlan ssid-profile default`
	`(host) (SSID Profile "default") #no dot11r-profile`
		Base OS Security	All platforms	AOS-W 6.4.3.4

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
131972	**Symptom:** The **datapath** process stops responding and crashes in a switch. **Scenario:** This issue occurs when Dynamic Multicast Optimization (DMO) and Internet Group Management Protocol (IGMP) snooping is enabled in a switch. This issue is observed in switches running AOS-W 6.4.3.4. **Workaround:** None.	Switch-Datapath	All platforms	AOS-W 6.4.3.4

Table 8: *Known Issues in 6.4.4.6*

Bug ID	Description	Component	Platform	Reported Version

132382	**Symptom:** A user fails to add a username with the **‘** (apostrophe) character in the RAP whitelist database by using the WebUI.
	Scenario: This issue occurs because of a previous entry that is enclosed in the **'** (apostrophe) character. This issue is observed in master switches running AOS-W 6.4.2.x in master-standby topology.
	Workaround: Do not use the **'** character in the username field when making changes by using the WebUI. Alternately, use the CLI command to update the user name:
	`(host) #whitelist-db rap add mac-address <mac address of the AP>`
	`ap-group <AP group name> ap-name <Name of the AP>`
	`description <description> fullname <username with apostrophe>`
		WebUI	All platforms	AOS-W 6.4.2.3

132714	**Symptom:** When a user tries to add a static Address Resolution Protocol (ARP) entry, a switch displays the **Cannot add static ARP entry** error message. The log file of 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
133266	**Symptom:** A local switch reboots unexpectedly. The log file for the event lists the reason as **Reboot Cause: Datapath timeout (Intent:cause:register 56:86:50:2)**. **Scenario:** This issue is observed in OAW-4650 switches running AOS-W 6.4.3.6. **Workaround:** None.	Switch-Datapath	OAW-4650 switches	AOS-W 6.4.3.6
133366	**Symptom:** The logs generated from the **Station Management Module** (STM) process flood a switch. **Scenario:** This issue is observed in OAW-4750 switches running AOS-W 6.4.3.5. **Workaround:** None.	Station Management	OAW-4750 switches	AOS-W 6.4.3.5
134646	**Symptom:** When an authenticated Captive Portal (CP) user is added using the XML-API, an accounting-stop message with wrong values is generated and the framed IP is 0.0.0.0. **Scenario:** This issue is observed in switches running AOS-W 6.4.2.12. **Workaround:** None.	XML API	All platforms	AOS-W 6.4.2.12

Table 8: *Known Issues in 6.4.4.6*

Bug ID	Description	Component	Platform	Reported Version
134884 135077	**Symptom:** The **Uptime** value of an Access Point (AP) is displayed incorrectly in the **Monitoring > Controller > Access Points** page of the WebUI. **Scenario:** This issue occurs when the an AP is in the **UP** state for more than 35 days in a switch. This issue is observed in switches running AOS-W 6.4.2.14. **Workaround:** Execute the following CLI command to view the correct **Uptime** value (in the **tot-t** column of the output) of the APs: `(host) #show ap bss-table`	WebUI	All platforms	AOS-W 6.4.2.14
135097	**Symptom:** A switch rebooted 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 race condition in aging session when the session has type 2 contract. This issue is observed in switches running ArubaOS 6.4.3.6. **Workaround:** None.	Switch-Datapath	All platforms	AOS-W 6.4.3.6
135132	**Symptom:** An Access Point (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
135569	**Symptom:** An Access Point (AP) crashes unexpectedly. The log file for the event lists the reason as **Kernel panic - not syncing: Fatal exception in interrupt**. **Scenario:** This issue occurrs when spectrum monitoring is enabled in an AP. When the AP radio changes from spectrum mode to normal mode on the home channel, it may experience 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 is observed in 100 Series access points running AOS-W 6.4.3.6 or later versions of AOS-W. **Workaround:** None.	AP-Wireless	100 Series access points	AOS-W 6.4.4.4
136027	**Symptom:** When a master switch fails, an Access Point (AP) fails to establish a tunnel to the backup switch. **Scenario:** This issue occurs in a High Availability (HA) topology with redundant switches. This issue is observed in switches running AOS-W 6.4.2.5. **Workaround:** None.	HA-Lite	All platforms	AOS-W 6.4.2.5

Table 8: *Known Issues in 6.4.4.6*

Bug ID	Description	Component	Platform	Reported Version
136444	**Symptom:** A master switch fails to synchronize the Network Time Protocol (NTP) authentication and key configuration with the standby switch. **Scenario:** This issue occurs in a master-standby topology. This issue is observed in switches running AOS-W 6.4.3.5. **Workaround:** None.	Configuration	All platforms	AOS-W 6.4.3.5
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 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
137549	**Symptom:** The **no export-route** parameter under the **aaa authentication vpn** command does not work as expected. **Scenario:** This issue occurs because of an incorrect profile checking. This issue is observed in switches running AOS-W 6.4.2.13. **Workaround:** None.	OSPF	All platforms	AOS-W 6.4.2.13
138196 138482 138560 139345	**Symptom:** The **authentication** process stops responding and crashes in a switch. **Scenario:** This issue occurs because of memory corruption. This issue is observed in local switches running AOS-W 6.4.3.6 in master-local topology. **Workaround:** None.	Base OS Security	All platforms	AOS-W 6.4.3.6

Chapter 6 Upgrade Procedure

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

CAUTION

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

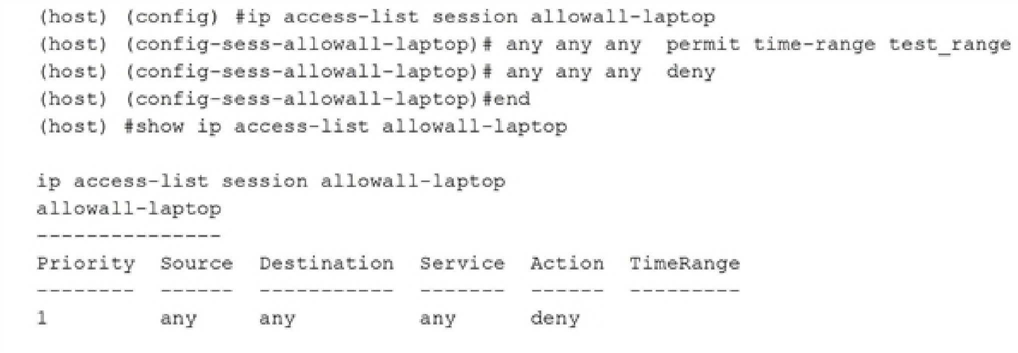
Topics in this chapter include:

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 36.)

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.

CAUTION

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 35 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 35 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 35 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 35.

NOTE

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 6.4.4.6

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 6.4.4.6

The following sections provide the procedures for upgrading the switch to AOS-W 6.4.4.6 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 34.

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 6.4.4.6.

- 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 6.4.4.6 on page 37 to install the interim version of AOS-W, and then repeat steps 1 through 11 of the procedure to download and install AOS-W 6.4.4.6

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 6.4.4.6 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 > 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

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 35 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

CAUTION

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 34.

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 6.4.4.6 on page 37.

Follow steps 2 through 7 of the procedure described in Upgrading to AOS-W 6.4.4.6 on page 37 to install the interim version of AOS-W, and then repeat steps 1 through 7 of the procedure to download and install AOS-W 6.4.4.6

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 6.4.4.6 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>
```

NOTE

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 35 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 6.4.4.6 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 6.4.4.6 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 35.
2. Verify that the control plane security is disabled.
3. Set the switch to boot with the previously saved pre-AOS-W 6.4.4.6 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 6.4.4.6 flash backup from the file stored on the switch. Do not restore the AOS-W 6.4.4.6 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 6.4.4.6, the changes do not appear in RF Plan in the downgraded AOS-W version.
   - If you installed any certificates while running AOS-W 6.4.4.6, 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 6.4.4.6 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.