AOS-W 6.4.4.9

Alcatel·Lucent
Enterprise

Release Notes

Contents

Revision History

The following table provides the revision history of this document.

Table 1: *Revision History*

Revision	Change Description
Revision 01	Initial release.
Revision 01	Updated scenario of bug ID 140582.

AOS-W 6.4.4.9 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 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

This chapter describes the new features and/or enhancements introduced in AOS-W 6.4.4.9.

Base OS Security

PAPI Security

Starting from AOS-W 6.4.4.9, a minor security enhancement is made to the Process Application Programming Interface (PAPI) messages. This enhancement allows PAPI endpoints to authenticate the sender by performing a sanity check of the incoming messages using MD5 (hash). **All PAPI endpoints—access points, Mobility Access Switches, switches, Analytics and Location Engine (ALE), AirWave, and HPE switches—must have the same secret key.**

The PAPI enhanced security configuration provides protection to Alcatel-Lucent devices, AirWave, and ALE against malicious users sending fake messages that results in security challenges.

Switch-Platform

Number of VLANs and VLAN interfaces

Starting from AOS-W 6.4.4.9, as part of memory optimization on OAW-4306 Series switches, the number of VLANs and VLAN interfaces are reduced to 64 from 128 to save memory.

Upgrading to AOS-W 6.4.4.9 will reduce the number of VLANs to 64. If your network configuration, before the upgrade includes more than 64 VLANs, the VLAN information will be lost after upgrading to AOS-W 6.4.4.9.

Station Management

Delete Stale Entries in Local Switch

Starting from AOS-W 6.4.4.9, stale entries in a local switch can be deleted. This setting appears in the switch CLI.

In the CLI

A new **clear gap-db stale-ap ap-name** command is introduced. Use this command to delete stale entries like access points that are shown as DOWN in the **show ap database** command.

The following parameters are introduced in the **clear gap-db stale-ap ap-name** command:

Table 4: *Delete Stale Entries*

Parameter	Description
`<ap-name>`	Name of the AP to be deleted.
`lms {lms-ip <lms-ip>} | {lms-ip6 <lms-ip6>}`	IP address of the Local Management Switch (LMS) where an AP entry exists: • `lms-ip <lms-ip>` is the IP address of the LMS. • `lms-ip6 <lms-ip6>` is the IPv6 address of the LMS.

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 6.4.4.9:

- DRT-1.0_55859

Chapter 4
Resolved Issues

This chapter describes the issues resolved in AOS-W 6.4.4.9.

Table 5: *Resolved Issues in 6.4.4.9*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
122384 123108 123806 124083 124434 124751 124966 125439 125498 125605 126163 126857 127839 130619 130671 134405 134406 135432 135712 136902 137507 137867	**Symptom:** A switch crashed frequently because of out of memory issue. This issue is resolved by dropping the incoming monitoring updates when the buffer is full. **Scenario:** This issue occurred when the **station management** process queued a large number of monitoring updates. This issue was observed in switches running AOS-W 6.3.x or AOS-W 6.4.x.	Station Management	All platforms	AOS-W 6.3.1.9	AOS-W 6.4.4.9
126793 128230 131927 132149 132304 134889 137322 140746	**Symptom:** An AP crashed unexpectedly. The log file for the event listed the reason as **kernel panic: PC is at nss_core_handle_napi**. The fix ensures that the AP works as expected. **Scenario:** This issue occurred because of corrupted Network Switching Subsystem (NSS) descriptor. This issue was observed in OAW-AP324 access points running AOS-W 6.4.4.1.	AP-Wireless	OAW-AP324 access points	AOS-W 6.4.4.1	AOS-W 6.4.4.9

Table 5: *Resolved Issues in 6.4.4.9*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
128979	**Symptom:** A RAP did not connect to a switch and did not recover. The fix ensures that the RAP reboots and recovers even if the Peripheral Component Interconnect (PCI) fails to initialize. **Scenario:** This issue occurred when a radio card was not detected and the RAP sent a hello request without a MAC address to a switch. This issue was observed in RAP 100 Series running AOS-W 6.4.3.3.	AP-Platform	RAP OAW-AP100 Series	AOS-W 6.4.3.3	AOS-W 6.4.4.9
129043	**Symptom:** A switch rebooted unexpectedly. The log file for the event listed the reason as **datapath timeout**. This issue is resolved by adding Aggregate MAC Service Data Unit (AMSDU) support for IPv6 access points and passing the fragments with forward opcode. **Scenario:** This issue occurred because the switches did not support AMSDU deaggregation for IPv6 access points. This issue was observed in both master and local switches running AOS-W 6.4.3.4 in master-local topology.	Switch-Datapath	All platforms	AOS-W 6.4.3.4	AOS-W 6.4.4.9
129096	**Symptom:** The Lightweight Directory Access Protocol (LDAP) connection in a switch reset unexpectedly. The switch was unable to authenticate or query the users using the LDAP server. This issue is resolved by enabling the **chase-referrals** parameter in **LDAP-authentication--server-profile**. **Scenario:** This issue was observed when a search request from a switch to an LDAP server was redirected to another LDAP server that did not support anonymous queries. This issue was not limited to any specific switch model or AOS-W version.	LDAP	All platforms	AOS-W 6.4.2.12	AOS-W 6.4.4.9
130983 136014 141304	**Symptom:** The Policy Based Routing (PBR) configuration in a standby switch was not retained after saving and reloading the standby switch. This issue is resolved by implementing changes to save, restore, and update the local PBR configuration to handle configuration clean-up and forward referencing on full configuration synchronization. **Scenario:** This issue was observed in standby switches running AOS-W 6.4.4.1 in master-standby topology.	Policy Based Routing	All platforms	AOS-W 6.4.4.1	AOS-W 6.4.4.9

Table 5: *Resolved Issues in 6.4.4.9*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
131511	**Symptom:** A Simple Network Management Protocol (SNMP) server did not receive SNMP traps from a switch when a Link Aggregation Control Protocol (LACP) link failed. The fix ensures that an SNMP server receives SNMP traps from a switch. **Scenario:** This issue occurred because of a delay in electing a member in an LACP interface when one member failed. This issue was observed in switches running AOS-W 6.4.3.4.	SNMP	All platforms	AOS-W 6.4.3.4	AOS-W 6.4.4.9
132230	**Symptom:** An SNMP server timed out the connection with a switch randomly. The fix ensures that the SNMP server is independent of the MODEM reinitialization. **Scenario:** This issue occurred because the MODEM connected to a switch was in standby mode and reinitialized every 2 minutes. This issue was observed in OAW-4010 switches running AOS-W 6.4.2.5 or AOS-W 6.4.2.12.	SNMP	OAW-40xx Series switches	AOS-W 6.4.2.5	AOS-W 6.4.4.9
132613 136113 136802 141635 141637 141643	**Symptom:** An AP crashed unexpectedly. The fix ensures that the AP works as expected. **Scenario:** This issue occurred because of memory slab corruption. This issue was observed in OAW-AP120 Series access points running AOS-W 6.4.4.6.	AP-Platform	OAW-AP120 Series access points	AOS-W 6.4.4.6	AOS-W 6.4.4.9
134417	**Symptom:** A client failed to obtain an IP address from an external DHCP server. This issue is resolved by fixing an internal buffer leak. **Scenario:** This issue occurred because a switch dropped the DHCP return message from the DHCP server due to an internal buffer leak. This issue was observed in OAW-4306 Series or OAW-M3switches running AOS-W 6.4.2.x.	Switch-Datapath	OAW-4306 Series and OAW-M3 switches	AOS-W 6.4.2.8	AOS-W 6.4.4.9
134668	**Symptom:** The log file of a switch showed wrong threshold limit. This issue is resolved by using the current entries to compute the threshold limit. **Scenario:** This issue occurred because the maximum number of entries was used to compute the threshold limit. This issue was observed in switches running AOS-W 6.4.4.2.	Switch-Datapath	All platforms	AOS-W 6.4.4.2	AOS-W 6.4.4.9

Table 5: *Resolved Issues in 6.4.4.9*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
135132	**Symptom:** An AP stopped responding and rebooted unexpectedly. The fix ensures that the AP functions as expected. **Scenario:** This issue occurred when spectrum monitoring was enabled on an AP. When the radio of the AP changes from spectrum mode to normal mode on the home channel, it may experience a phenomenon called a stuck beacon. Stuck beacon is a driver-level error indicating that the chipset failed to complete a Tx function. This issue was observed in 100 Series access points running AOS-W 6.4.3.6 or later versions.	AP-Wireless	100 Series access points	AOS-W 6.4.3.6	AOS-W 6.4.4.9
136349	**Symptom:** A switch sent the IP address in the port field and 0.0.0.0 as the remote address, resulting in security warnings. The fix ensures that a switch sends the same IP address in remote address field. **Scenario:** This issue was observed when TACACS+ accounting was enabled for command execution and a user logged in using Secure Shell (SSH). This issue was observed in switches running AOS-W 6.4.3.6.	TACACS	All platforms	AOS-W 6.4.3.6	AOS-W 6.4.4.9
136501	**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 (Intent:cause:register 56:86:50:2)**. The fix ensures that the **datapath** process does not crash and the switch works as expected. **Scenario:** This issue occurred because of memory corruption. This issue was observed in OAW-4550 switches running AOS-W 6.4.3.4.	Base OS Security	OAW-4550 switches	AOS-W 6.4.3.4	AOS-W 6.4.4.9
138268	**Symptom:** An AP displayed the **I** flag when connected to a layer 3 switch. The fix ensures that the power change detection is not mandated based on the AP state. **Scenario:** This issue occurred in access points connected to a layer 3 switch with Link Layer Discovery Protocol (LLDP) enabled on the switch port. This issue was observed in OAW-4x50 Series switches running AOS-W 6.4.3.4.	AP-Platform	OAW-4x50 Series switches	AOS-W 6.4.3.4	AOS-W 6.4.4.9

Table 5: *Resolved Issues in 6.4.4.9*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
138647	**Symptom:** A system-defined net-destination Virtual Router Redundancy Protocol (VRRP) IP address did not handle multiple VRRP IP addresses. This issue is resolved by saving multiple VRRP IP addresses as a list in net-destination and handling modify messages appropriately. **Scenario:** This issue occurred because a system-defined net-destination stored only single VRRP IP address and did not handle modification of VRRP IP address. Hence, when more than one VRRP IP address was configured, the Access Control List (ACL) filters were not created for any VRRP IP address. This issue was observed in switches running AOS-W 6.3.1.18.	Switch-Platform	All platforms	AOS-W 6.3.1.18	AOS-W 6.4.4.9
139192	**Symptom:** A RAP with a 340U MODEM for cellular uplink failed to boot. This issue is resolved by applying a script on 340U modems that do not have a LINUX patch. **Scenario:** This issue was observed in remote access points running AOS-W 6.5.0.0 and using 340U MODEM for cellular uplink.	Remote Access Point	All platforms	AOS-W 6.5.0.0	AOS-W 6.4.4.9
139424	**Symptom:** A false RADAR event was detected on the Dynamic Frequency Selection (DFS) channel and an AP was moved to another channel. The fix ensures that a false RADAR event is not detected in the ETSI domain and the AP works as expected. **Scenario:** This issue was observed in OAW-AP320 Series access points running AOS-W 6.4.4.5.	AP-Wireless	OAW-AP320 Series access points	AOS-W 6.4.4.5	AOS-W 6.4.4.9
140249	**Symptom:** Some access points were unable to modify the Maximum Segment Size (MSS) value. The fix ensures that the access points are able to set the value of Maximum Transmission Unit (MTU) correctly. **Scenario:** This issue was observed when the MTU of a Point-to-Point Protocol over Ethernet (PPPoE) server was set to a value lesser than 1492. This issue was observed in OAW-AP200 Series access points connected to switches running AOS-W 6.4.4.6.	Remote Access Point	OAW-AP200 Series access points	AOS-W 6.4.4.6	AOS-W 6.4.4.9

Table 5: *Resolved Issues in 6.4.4.9*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
140290	**Symptom:** Tunneled-node clients failed to pass traffic when connected to a wired port of a Mobility Access Switch or a switch directly. The fix ensures that a switch initiates 802.1X authentication for tunneled-node clients. **Scenario:** This issue occurred because a switch did not trigger 802.1X authentication for wired users. This issue was observed in switches running AOS-W 6.4.1.0 or later versions.	Multiplexer	All platforms	AOS-W 6.4.2.15	AOS-W 6.4.4.9
140309 144264 144898	**Symptom:** An AP crashed unexpectedly. The fix ensures that the AP works as expected. **Scenario:** This issue occurred because of memory corruption. This issue was observed in OAW-AP120 Series access points running AOS-W 6.4.4.8.	AP-Platform	OAW-AP120 Series access points	AOS-W 6.4.4.8	AOS-W 6.4.4.9
140383	**Symptom:** The **authentication** process in a switch crashed multiple times. The fix ensures that authentication is not performed on the wired port of an AP. **Scenario:** This issue occurred when authentication was performed on the wired port of an AP. This issue was observed in OAW-4x50 Series switches running AOS-W 6.4.3.7.	Base OS Security	OAW-4x50 Series switches	AOS-W 6.4.3.7	AOS-W 6.4.4.9
140582	**Symptom:** Some Vocera clients showed Searching For Server (SFS) events after associating with an AP. The fix ensures that Vocera clients work as expected. **Scenario:** A session between a Vocera server and Vocera client had a Deny (**D**) flag and the switch dropped such packets. The dropped packets led to SFS events for the client. Typically, the **D** flag does not appear for such sessions and this issue is not observed if PINOT is disabled in OAW-M3 switches. This issue was observed in OAW-M3 switches running AOS-W 6.4.2.13.	Unified Communications and Collaboration	OAW-M3 switches	AOS-W 6.4.2.13	AOS-W 6.4.4.9

Table 5: *Resolved Issues in 6.4.4.9*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
141031	**Symptom:** Spare Ethernet ports got local IP address in bridge mode and were allowed Internet access even though the LAN connection was disconnected. The fix ensures that after an AP reboots, the Ethernet interface retains the RAP backup configuration. **Scenario:** This issue occurred when a remote AP that had a LAN port (E1) setup for tunnel mode during switch configuration, reset the port to bridge mode when the RAP did not establish an IPsec VPN to the switch. This issue was observed because the tunnel node ports were not disabled and were allowed access beyond RAP when the RAP was unable to connect to a switch. This issue was observed in remote access points running AOS-W 6.3.1.9.	Remote Access Point	All platforms	AOS-W 6.3.1.9	AOS-W 6.4.4.9
141073 144233 144932	**Symptom:** The tacacs-accounting configuration did not synchronize to local, branch, and standby switches from the master switch. The fix ensures that the tacacs-accounting configuration synchronizes to local, branch, and standby switches. **Scenario:** This issue occurred because of an error in the **running-config** command order. This issue was observed in switches running AOS-W 6.4.4.8.	Base OS Security	All platforms	AOS-W 6.4.4.8	AOS-W 6.4.4.9
141239	**Symptom:** A Motorola MC75A0 handheld scanner failed to associate to OAW-AP325 access points. This fix ensures that the device connects to an OAW-AP325 access point. **Scenario:** This issue occurred when the device always sent a deauthentication message before sending the authentication message to an AP. The AP sent a deauthentication message to a client after receiving an association request. This issue was observed in OAW-AP325 access points running AOS-W 6.4.4.5.	AP-Wireless	OAW-AP325 access points	AOS-W 6.4.4.5	AOS-W 6.4.4.9

Table 5: *Resolved Issues in 6.4.4.9*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
141272	**Symptom:** When a client tried to use USB as the backup uplink for a OAW-40xx Series switch, the switch was detected but the State was unreachable. The fix ensures that the USB MODEM is not in Airplane mode when there is a new connection. If a USB MODEM goes into a bad state, execute the **usb reclassify** command or physically reconnect the USB MODEM. **Scenario:** This issue was observed in OAW-40xx Series switches running AOS-W 6.4.3.1.	Switch-Platform	OAW-40xx Series switches	AOS-W 6.4.3.1	AOS-W 6.4.4.9
141646	**Symptom:** An AP responded to the Address Resolution Protocol (ARP) request for the gateway IP address 192.168.11.1. This issue is resolved by using the correct process to program the br0 VLAN information when the IP address of the AP and the IP address of the LMS lie in the range of 192.168.11.0/24. **Scenario:** This issue occurred because of an endian issue when the IP address of the AP and the IP address of th LMS belonged to the same range—that is, 192.168.11.0/24. The AP failed to use 172.16.11.0/24 as the IP address of the DHCP server on the br0 interface and created a permanent ARP entry for 192.168.11.0/24. This issue was observed in OAW-AP200 Series access points running AOS-W 6.4.4.6.	AP-Datapath	OAW-AP200 Series access points	AOS-W 6.4.4.6	AOS-W 6.4.4.9
141678	**Symptom:** For a Session Initiation Protocol (SIP) client with **VoIP CAC** enabled, when the VoIP CAC threshold was reached, a switch did not block the SIP Invite to the called party. This allowed the called party to get call rings. This issue is resolved by successfully blocking the SIP Invite to the called party. **Scenario:** This issue occurred when the **send-sip-status-code** option to reject SIP calls with error codes was configured in the CAC profile. When the configured CAC threshold was reached, the newly initiated calls were blocked with the SIP error messages (SIP 486) being sent to the client or the server. But the switch did not block the SIP Invite being sent to the called party. This issue was observed in switches running AOS-W 6.4.x or AOS-W 6.5.x.	Unified Communications and Collaboration	All platforms	AOS-W 6.4.4.6	AOS-W 6.4.4.9

Table 5: *Resolved Issues in 6.4.4.9*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
141693 143220 144785	**Symptom:** A RAP with 340U MODEM for cellular uplink crashed continuously. This issue is resolved by: • Applying newer firmware without LINUX patch on OAW-AP205H access points. • Applying LINUX patch and adding a delay after mode switch to allow population of new device ID on RAP-155 remote access points. **Scenario:** This issue was observed when OAW-AP205H access points and OAW-RAP155 remote access points running AOS-W 6.5.0.0 used 340U MODEM for cellular uplink.	Remote Access Point	OAW-AP205H access points and OAW-RAP155 remote access points	AOS-W 6.5.0.0	AOS-W 6.4.4.9
141902	**Symptom:** The **mDNS** process in a local switch crashed unexpectedly. This issue is resolved by changing the output format of the **show airgroup cppm-server radius statistics** and **show airgroup cppm-server rfc3576 statistics** commands. **Scenario:** This issue occurred only when the network had more than seven RADIUS servers and the **show airgroup cppm-server radius statistics** or **show airgroup cppm-server rfc3576 statistics** command was executed. These commands showed different RADIUS/RFC3576 server statistics and when the number of servers was more than seven, the number of columns increased and corrupted the memory. This issue was observed in switches running AOS-W 6.4.4.5.	AirGroup	All platforms	AOS-W 6.4.4.5	AOS-W 6.4.4.9
142197	**Symptom:** A client faced connectivity issue when an AP switched channels randomly. This issue is resolved by deleting a timer before it is started in AP mode only. **Scenario:** This issue occurred under the following circumstances: • Multiple OAW-AP225 access points did not have wireless association for a long duration. • Excessive channel switching occurred because of RADAR detect trigger. • 5 GHz radio did not accept associations and transmission of frames was stalled until the AP was rebooted. This issue was observed in OAW-AP225 access points running AOS-W 6.4.2.14.	AP-Wireless	OAW-AP225 access points	AOS-W 6.4.2.14	AOS-W 6.4.4.9

Table 5: *Resolved Issues in 6.4.4.9*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
142310	**Symptom:** The status of the Instant Access Point (IAP) table in a switch showed DOWN for some Instant Access Points even though IPsec and client traffic were running. This issue is resolved by deleting the old session if a switch has an existing session for an allocated inner IP address. **Scenario:** This issue occurred when the elected master of an IAP cluster went offline and a new IAP was elected as the master. The switch had two security associations with same inner IP address but different outer IP addresses. This issue was observed in switches running AOS-W 6.4.4.4.	Remote Access Point	All platforms	AOS-W 6.4.4.4	AOS-W 6.4.4.9
142330 142786 142870	**Symptom:** The Airwave WebUI showed **802.11ag** as the connection mode for some clients, while the controller WebUI showed **802.11g** as the connection mode for the same clients. This issue is resolved by removing the second mapping of the connection mode to the SNMP MIB value if the connection mode is already mapped in the **authentication** process. **Scenario:** The issue occurred when the connection mode was mapped twice, once each by the **authentication** process and **SNMP** process resulting in a wrong value. This issue was observed in switches running AOS-W 6.4.4.5.	SNMP	All platforms	AOS-W 6.4.4.5	AOS-W 6.4.4.9
142376 142378	**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 (SOS Assert) (Intent:cause:register 54:86:50:2)**. The fix ensures that the **datapath** process does not crash and the switch works as expected. **Scenario:** This issue occurred under the following circumstances: • When the ARP entry for an IP address was aged out or forcefully deleted while traffic was running. • When jumbo processing was enabled and a management multi-buffer IP frame was received. This issue was observed in switches running AOS-W 6.4.4.5.	Switch-Datapath	All platforms	AOS-W 6.4.4.5	AOS-W 6.4.4.9
142682 144337	**Symptom:** An AP crashed and 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 works as expected. **Scenario:** This issue was observed in switches running AOS-W 6.4.4.8.	AP-Platform	All platforms	AOS-W 6.4.4.8	AOS-W 6.4.4.9

Table 5: *Resolved Issues in 6.4.4.9*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
143185	**Symptom:** A Virtual Intranet Access (VIA) client failed to connect to a switch. This issue is resolved by clearing the IP addresses from the Layer 2 Tunneling Protocol (L2TP) used pool when a Security Association (SA) is deleted for a VIA client. **Scenario:** This issue occurred when a VIA client did not get an IP address from the L2TP pool because the L2TP pool was exhausted. This issue was observed in switches running AOS-W 6.4.3.7.	L2TP	All platforms	AOS-W 6.4.3.7	AOS-W 6.4.4.9
143278	**Symptom:** The search feature in the **Dashboard > Clients** page of the WebUI did not work for an IP address. This issue is resolved by adding the IP address of the clients and access points in the dashboard search. **Scenario:** This issue was observed in switches running AOS-W 6.4.4.6.	WebUI	All platforms	AOS-W 6.4.4.6	AOS-W 6.4.4.9
143744	**Symptom:** The **Acct-Input-Octets** and **Acct-Output-Octets** always showed 0 in RADIUS accounting messages. This issue is resolved by converting the byte order before writing it into the RADIUS accounting message. **Scenario:** This issue occurred for users in split-tunnel forwarding mode. This issue was observed in OAW-AP205 access points running AOS-W 6.4.3.6.	AP-Platform	OAW-AP205 access points	AOS-W 6.4.3.6	AOS-W 6.4.4.9

Table 5: *Resolved Issues in 6.4.4.9*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
143967	**Symptom:** An administrator failed to configure SHA1-96 hash within IKEv2 ISAKMP policy in a switch running FIPS build. This issue is resolved by allowing SHA1-96 hash configuration for FIPS build. **Scenario:** This issue was observed in switches running AOS-W 6.3.x.x-FIPS or AOS-W 6.4.x.x-FIPS.	IPsec	All platforms	AOS-W 6.3.1.5-FIPS	AOS-W 6.4.4.9
144723 144724 144894	**Symptom:** An AP crashed unexpectedly. The fix ensures that the AP works as expected. **Scenario:** This issue occurred because of a memory corruption. This issue was observed in OAW-AP125 access points running AOS-W 6.4.4.8.	AP-Platform	OAW-AP125 access points	AOS-W 6.4.4.8	AOS-W 6.4.4.9
144725 144860 144861 144862 144896 144897	**Symptom:** An AP crashed unexpectedly. The fix ensures that the AP works as expected. **Scenario:** This issue occurred because of low memory. This issue was observed in OAW-AP125 access points running AOS-W 6.4.4.8.	AP-Platform	OAW-AP125 access points	AOS-W 6.4.4.8	AOS-W 6.4.4.9

This chapter describes the known and outstanding issues identified in AOS-W 6.4.4.9.

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 6: *Known Issues in 6.4.4.9*

Bug ID	Description	Component	Platform	Reported Version
123399	**Symptom:** The AppRF feature fails to classify certain Domain Name System (DNS) traffic. **Scenario:** This issue occurs when a wrongly formed DNS packet undergoes a Deep Packet Inspection (DPI) lookup. The packet misses the DNS rule due to a DNS mismatch and is categorized as a Thunder application. After categorization, a Thunder rule is installed as a dynamic rule that forces all subsequent DNS packets to be wrongly classified as Thunder. This issue is observed in switches running AOS-W 6.4.2.x, AOS-W 6.4.3.x, or AOS-W 6.4.4.x. **Workaround:** None.	Switch-Datapath	All platforms	AOS-W 6.4.4.8
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 version. **Workaround:** None.	AP-Platform	All platforms	AOS-W 6.4.4.3
124275	**Symptom:** A client obtains an IP address 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
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

Table 6: *Known Issues in 6.4.4.9*

Bug ID	Description	Component	Platform	Reported Version
126385	**Symptom:** Clients did not connect to an SSID although the access point is connected to a switch. **Scenario:** This issue occurs when access points work in active-backup mode with VAP in bridge mode. This issue is observed in access points running AOS-W 6.4.2.12. **Workaround:** None.	AP-Platform	All platforms	AOS-W 6.4.2.12
127660	**Symptom:** There is no option to configure a Network Access Server (NAS) IP address in the **Configuration > BRANCH > Smart Config** page of the WebUI. **Scenario:** This issue is observed in switches running AOS-W 6.4.4.1. **Workaround:** None.	WebUI	All platforms	AOS-W 6.4.4.1
127848	**Symptom:** A 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 ArubaOS 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 switch does 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
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 **userrole**. **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

Table 6: *Known Issues in 6.4.4.9*

Bug ID	Description	Component	Platform	Reported Version
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 6.4.4.8
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 switches 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
137031	**Symptom:** Clients are unable to associate to 2.4 GHz radio of the OAW-AP225 access points intermittently. **Scenario:** This issue occurs when the AP LACP profile is configured only on the master switch and not on the local switch. This issue is observed in OAW-AP225 access points running AOS-W 6.4.2.0. **Workaround:** None.	AP-Platform	OAW-AP225 access points	AOS-W 6.4.2.0
137196	**Symptom:** A switch fails to respond and reboots unexpectedly. The log file for the event lists the reason as **Reboot Cause: Datapath timeout**. **Scenario:** This issue occurs when Virtual Internet Access (VIA) is used with Secure Socket Layer (SSL) fallback. This issue is not limited to any specific switch model or AOS-W version. **Workaround:** None.	Base OS Security	All platforms	AOS-W 6.4.0.3
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
138637	**Symptom:** Profinet and Precision Time Protocol (PTP) devices fail to communicate with a switch. **Scenario:** This issue occurs because a switch drops all packets with 802.1Q header. This issue is observed in switches running AOS-W 6.4.3.7. **Workaround:** None.	AP-Wireless	All platforms	AOS-W 6.4.3.7

Table 6: *Known Issues in 6.4.4.9*

Bug ID	Description	Component	Platform	Reported Version
138868 139336	**Symptom:** When an image is sent using the WhatsApp application, the switch classifies the traffic and blocks the transmission. But on sending text messages, the switch does not block the traffic. **Scenario:** The WhatsApp traffic classification is not functional as the latest version of the WhatsApp application is not classified as WhatsApp in the switch. This issue is observed in OAW-40xx Series or OAW-4x50 Seriesswitches running AOS-W 6.4.3.7. **Workaround:** None.	Switch-Datapath	OAW-40xx Series and OAW-4x50 Seriesswitches	AOS-W 6.4.3.7
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 running AOS-W 6.4.4.x. **Workaround:** None.	Station Management	OAW-AP320 Series access points	AOS-W 6.4.4.3
140049	**Symptom:** An AP takes longer time to boot. **Scenario:** This issue occurs when CPsec is enabled in a switch. This issue is observed in switches running AOS-W 6.4.3.3-FIPS. **Workaround:** None.	IPsec	All platforms	AOS-W 6.4.3.3-FIPS
140057 142265	**Symptom:** An AP is unable to establish a Generic Route Encapsulation (GRE) tunnel with a switch. **Scenario:** This issue occurs when the AP is not broadcasting the SSID but remote BSS-table is able to see the BSSID/SSID. This issue is observed when the STM receives a VLAN delete message and deletes all VAPs with the same VLAN in the station VLAN array and the switch brings down the VAP without notifying the AP. **Workaround:** None.	Station Management	All platforms	AOS-W 6.4.2.14
140327	**Symptom:** Memory usage of the **authentication** process in a switch increases gradually. **Scenario:** This issue occurs because of a memory leak. This issue is observed in switches running AOS-W 6.4.3.3. **Workaround:** None.	Base OS Security	All platforms	AOS-W 6.4.3.3

Table 6: *Known Issues in 6.4.4.9*

Bug ID	Description	Component	Platform	Reported Version
141686	**Symptom:** A branch switch does not communicate with the master switch. **Scenario:** This issue occurs when the **ip nat outside** option is enabled on the uplink of the branch switch and the IP address of the master switch is different from the public IP address. This issue occurs because the crypto SA between the branch switch and the master switch is unstable and the configuration packets from the branch switch are source network address translated. **Workaround:** None.	Branch Switch	All platforms	AOS-W 6.4.4.0
143444	**Symptom:** A switch drops some packets. **Scenario:** This issue occurs because a switch drops all VLAN o priority tagged packets. This issue is observed in switches running AOS-W 6.4.3.7. **Workaround:** None.	Switch-Datapath	All platforms	AOS-W 6.4.3.7
144703	**Symptom:** The LLDP packets from a client are dropped. **Scenario:** This issue occurs when spanning tree is enabled on the Eth2 (POE enabled) port of a RAP. This issue is observed in remote access points running AOS-W 6.4.3.9. **Workaround:** None.	Remote Access Point	All platforms	AOS-W 6.4.3.9

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 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.

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.

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 6.4.4.9

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 6.4.4.9

The following sections provide the procedures for upgrading the switch to AOS-W 6.4.4.9 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 6.4.4.9.

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 6.4.4.9 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 6.4.4.9.

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 6.4.4.9 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 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

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 6.4.4.9 on page 37.

Follow steps 2 through 7 of the procedure described in Upgrading to AOS-W 6.4.4.9 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 6.4.4.9.

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 6.4.4.9 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 35 for information on creating a backup.

Downgrading

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

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

If you downgrade to a pre-6.1 configuration that was not previously saved, some parts of your deployment may not work as they previously did. For example, when downgrading from AOS-W 6.4.4.9 to 5.0.3.2, changes made to WIPS in AOS-W 6.x prevent the new predefined IDS profile assigned to an AP group from being recognized by the older version of AOS-W. This unrecognized profile can prevent associated APs from coming up, and can trigger a profile error. These new IDS profiles begin with *ids-transitional* while older IDS profiles do not include *transitional*. If you have encountered this issue, execute the **show profile-errors** and **show ap-group** commands to view the IDS profile associated with the AP group.

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

Before You Begin

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

1. Back up your switch. For details, see Backing up Critical Data on page 35.
2. Verify that the control plane security is disabled.
3. Set the switch to boot with the previously saved pre-AOS-W 6.4.4.9 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 6.4.4.9 flash backup from the file stored on the switch. Do not restore the AOS-W 6.4.4.9 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 6.4.4.9, the changes do not appear in RF Plan in the downgraded AOS-W version.
   - If you installed any certificates while running AOS-W 6.4.4.9, 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 6.4.4.9 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.