AOS-W 6.3.1.21

Release Notes

Revision History

The following table lists the revision history of this document.

Table 1: *Release History*

Revision	Change Description
Revision 01	Initial release.

AOS-W 6.3.1.21 is a software patch release that includes fixes to the issues identified in previous AOS-W releases.

See the Upgrade Procedures on page 23 for instructions on how to upgrade your switch to this release.

Contents Overview

- New Features on page 9 provides a description of features and enhancements introduced in this release of AOS-W.
- Regulatory Updates on page 10 describes the regulatory updates in this release of AOS-W.
- Resolved Issues on page 11 describes the issues resolved in this release of AOS-W.
- Known Issues and Limitations on page 12 describes the known and outstanding issues identified in this release of AOS-W.
- Upgrade Procedures on page 23 describes the procedures for upgrading a switch to this release of AOS-W.

For information regarding prior releases, refer to the corresponding Release Notes on https://service.esd.alcatel-lucent.com/.

Important Points to Remember

If you modify the configuration of an Access Point (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.

AP Settings Triggering a Radio Restart

Changing the following settings triggers the radio to restart on the OAW-AP220 Series access points. When the radio restarts, wireless services will be briefly interrupted. Clients will automatically reconnect to the network when the radio is up and running.

Table 2: *Profile Settings in AOS-W 6.3.x*

Profile	Description
802.11a/802.11g Radio Profile	• Channel • 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

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 to use with the AOS-W 6.3.1.21 Web User Interface (WebUI):

- Microsoft Internet Explorer 10.x and 11.0 on Windows 7 and Windows 8
- Mozilla Firefox 23 or higher on Windows Vista, Windows 7, 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	
• 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

There are no new features in this release of AOS-W.

Chapter 3
Regulatory Updates

There are no regulatory updates in this release of AOS-W.

This release includes fixes for vulnerability documented in CVE-2015-7547.

This chapter describes the known and outstanding issues identified in this release of AOS-W.

AirGroup

Table 4: *AirGroup Known Issues*

Bug ID	Description
103241 105632	**Symptom:** The multicast Domain Name System (mDNS) process crashes in the switch. The log files for the event listed the reason as: **Serial BB0001702 not found in serialnumber database**. **Scenario:** This issue is observed when disabling the **ipv6 nd ra** command on the VLAN interface of the switch. **nd** stands for Neighbor Discovery and **ra** stands for Router Advertisement. This issue is observed in switches running AOS-W 6.3.1.x or AOS-W 6.4.x. **Platform:** All platforms. **Reported Version:** AOS-W 6.4.3.0. **Workaround:** None.

Air Management-IDS

Table 5: *Air Management-IDS Known Issues*

Bug ID	Description
104711	**Symptom:** A Real Time Location Server (RTLS) receives multiple station messages with invalid client MAC Organizationally Unique Identifiers (OUIs), on switches with OAW-AP105 access points. **Scenario:** This issue is observed when corrupt block acknowledgment frames are transmitted by OAW-AP105 access points to its clients. As a result, the switch creates client entries with invalid MAC addresses. This issue is observed in OAW-4504 switches and OAW-AP105 access points running AOS-W 6.3.1.5 or later versions. **Platform:** OAW-4504 switches and OAW-AP105 access points. **Reported Version:** AOS-W 6.3.1.5. **Workaround:** None.
105701 109972 113561	**Symptom:** The value of Signal to Noise Ratio (SNR) is high for neighboring APs and monitored clients in AM (Air Monitor) tables. **Scenario:** This issue is observed when the hardware is unable to determine the RSSI; as a result it is set to zero and SNR becomes invalid. This issue is observed in OAW-AP200 Series access points running AOS-W 6.4.3. **Platform:** OAW-AP200 Series access points. **Reported Version:** AOS-W 6.3.1.13.

AP-Datapath

Table 6: *AP-Datapath Known Issues*

Bug ID	Description
98786 100770	**Symptom:** The Maximum Transmission Unit (MTU) showed by the output of the show ap bss-table command is not the value configured in the system profile. **Scenario:** This issue is observed in OAW-AP225 access points running AOS-W 6.4.1.0. **Platform:** OAW-AP225 access points. **Reported Version:** AOS-W 6.4.1.0. **Workaround:** None.
135862	**Symptom:** On configuring the Maximum Transmission Unit (MTU) in ap system-profile, the **show ap bss-table** command displays an incorrect MTU value. **Scenario:** This issue is observed when MTU update message gets lost. This issue is observed in OAW-AP135 and OAW-AP225 access points running AOS-W 6.3.x. **Platform:** OAW-AP135 and OAW-AP225 access points. **Reported Version:** AOS-W 6.3.1.9. **Workaround:** None.

AP-Platform

Table 7: *AP-Platform Known Issues*

Bug ID	Description
92668 122094	**Symptom:** An internal system error occurs at file **sapd_sysctl.c function sapd_sysctl_read_param line 97**. The log file lists Error reading **/proc/sys/dev/wifi1/turboqam_enable : Invalid argument**. **Scenario:** This issue is observed after executing the **very-high-throughput-rates-enable** command in the 802.11g radio profile. This issue is observed on all access points that do not support Very High Throughput (VHT) on 2.4 GHz. This includes all the 802.11n-capable access points, OAW-AP60, OAW-AP61, OAW-AP65, OAW-AP68, OAW-AP70, and OAW-AP85access points. **Platform:** OAW-AP60, OAW-AP61, OAW-AP65, OAW-AP68, OAW-AP70, OAW-AP85, OAW-AP90 Series, OAW-AP100 Series, OAW-AP110 Series, and OAW-AP120 Series access points. **Reported Version:** AOS-W 6.3.1.9. **Workaround:** Issue the issue the no very-high-throughput-rates-enable command in the 802.11g radio profile.
108299 108352 113793	**Symptom:** Wireless clients fail to connect to a remote AP after AP failover. The **show auth-tracebuf** command displays the following event: **received eapol-pkt before assos**. **Scenario:** This issue occurs due to an AP failover in a master-local setup with the following configurations: 1. A local management switch (LMS) is configured. 2. At least one virtual AP is configured with **rap-operation** parameter set to **always** or **persistent**. **Platform:** All AP platforms. **Reported Version:** AOS-W 6.4.2.0. **Workaround:** Reboot the remote AP.
110139	**Symptom:** An AP terminating on a backup switch fails to fallback to the master switch although it loses connectivity with the backup switch. However, after the AP reboots, it connects to the master switch. **Scenario:** This issue is observed when **Control Plane Security** is disabled. This issue is not limited to a specific switch model or AOS-W release version. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.13. **Workaround:** None.

AP-Wireless

Table 8: *AP-Wireless Known Issues*

Bug ID	Description
103991 105074 105212 105628 106467 108995 110880 111201 113192	**Symptom:** A multicast video stream freezes on Windows Media Player clients. **Scenario:** This issue occurs when the number of clients on an AP exceeds 20. This issue is observed in switches running AOS-W 6.4.0.2. **Platform:** All platforms. **Reported Version:** AOS-W 6.4.0.2. **Workaround:** Reduce the energy drop timeout of the 5 GHz radio to the same value as the 2 GHz radio.
104694 109975	**Symptom:** A high memory utilization is observed in OAW-AP225 access point when clients associate to this AP. **Scenario:** This issue occurs when packets are locked in the Broadcast/Multicast queue of the AP, resulting in high memory utilization. This issue is observed in OAW-AP225 access points running the beta version of AOS-W 6.4.2.3 or AOS-W 6.3.x. **Platform:** OAW-AP225 access points. **Reported Version:** AOS-W 6.4.2.3. **Workaround:** None.
107197	**Symptom:** The calls made between Vocera badges that are connected using a 2.4 GHz radio are of bad quality sometimes. **Scenario:** This issue is observed in the OAW-AP225 access point running AOS-W 6.3.1.6. **Platform:** OAW-AP225 access points. **Reported Version:** AOS-W 6.3.1.6. **Workaround:** None.

Base OS Security

Table 9: *Base OS Security Known Issues*

Bug ID	Description
109038	**Symptom:** A local switch crashes on multiple processes and reboots due to an authentication memory leak. The log files for the event lists the reason for the crash as **Nanny rebooted machine - fpapps process died**. **Scenario:** This issue is observed in switches deployed in a master-local topology and running AOS-W 6.4.2.0. **Platform:** All platforms. **Reported Version:** AOS-W 6.4.2.0. **Workaround:** None.
109776	**Symptom:** AOS-W fails to classify the device-type correctly for the BlackBerry Z10 device. **Scenario:** This issue is observed because AOS-W does not update its keyword parsing function with the BlackBerry Z10 device. This issue is observed in switches running AOS-W 6.3.1.x or AOS-W 6.4.x. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.9. **Workaround:** None.
109835	**Symptom:** The **Tunnel-Private-Group-ID** RADIUS attribute is displayed incorrectly in the logs when this attribute is sent by the RADIUS server with the **Tag** field set. **Scenario:** This issue is not specific to any switch or AOS-W release version. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.8. **Workaround:** None.
109838	**Symptom:** The switch displays an incorrect number of net destinations in the WebUI. **Scenario:** This issue occurs when there is a space preceding the net destination name. This issue is observed in switches running AOS-W 6.3.x. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.12. **Workaround:** None.

Captive Portal

Table 10: *Captive Portal Known Issues*

Bug ID	Description
107681 109842	**Symptom:** Users experience a delay in Captive Portal login page or Captive Portal authentication page. **Scenario:** This issue occurs when the clients are connected to an AP in split-tunnel forwarding mode with mode **device classification** enabled (default). This issue is observed in switches running AOS-W 6.3.1.8. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.8. **Workaround:** Execute the **clear aaa device-id-cache** command to clear the AAA device cache entries periodically.
114606	**Symptom:** Wireless clients fail to access the Captive Portal page. **Scenario:** This issue is seen when the DHCP server is configured with a low DHCP lease time and the **no firewall prohibit-ip-spoofing** parameter is configured in the switch. The DHCP lease time of the IP that is assigned to one client expires and it is re-assigned to another client. But a copy of the old user entry remained in the switch. Due to the MAC address mismatch between the new client and the old user entry, the client fails to access the Captive Portal page. This issue is observed in switches running AOS-W 6.3.1.2 or AOS-W 6.4.x. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.2. **Workaround:** None.

Switch-Datapath

Table 11: *Switch-Datapath Known Issues*

Bug ID	Description
99251	**Symptom:** Users are not getting redirected to the Captive Portal page. **Scenario:** This issue occurs when the switch IP is added as a whitelist IP. As a result, the policy to redirect the traffic does not take effect and the Captive Portal stops working. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.3. **Workaround**: Add a redirect policy above the whitelist entry.
110705	**Symptom:** The switch stops responding and reboots unexpectedly. The log files for the event listed the reason as **datapath exception**. **Scenario:** This issue occurs when a Point-to-Point Tunneling Protocol (PPTP) client connects and passes the traffic through the PPTP tunnel. This issue is observed on OAW-4650 and OAW-4750 switches running AOS-W 6.3.1.12 or 6.3.1.13. **Platform:** OAW-4650 and OAW-4750 switches. **Reported Version:** AOS-W 6.3.1.13. **Workaround:** None.
114426	**Symptom:** The client is able to pass traffic even though the static IP client is connected to a wired RAP port and the **enforce-dhcp** parameter is enabled in the AAA profile. **Scenario:** This issue is observed in RAPs but is not limited to any specific switch model. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.9. **Workaround:** None.

Table 11: *Switch-Datapath Known Issues*

Bug ID	Description
114563 114684 115868 116324 117331 128226	**Symptom:** A switch stops responding and reboots. The log files for the event listed the reason as **datapath timeout**. **Scenario:** This issue is observed in OAW-4x50 Series switches when the Aggregate MAC Service Data Unit (AMSDU) feature was enabled and when the crypto engine was interrupted. **Platform:** OAW-4x50 Series switches. **Reported Version:** AOS-W 6.4.2.4. **Workaround:** None.
126589	**Symptom:** A switch stops responding and reboots repeatedly. **Scenario:** This issue is observed in Xsec opmode for WLAN. This issue is observed in OAW-4x50 Series switches running AOS-W 6.3.1.x. **Platform:** OAW-4x50 Series switches. **Reported Version:** AOS-W 6.3.1.18. **Workaround:** Use a different opmode instead of Xsec.

Switch-Platform

Table 12: *Switch-Platform Known Issues*

Bug ID	Description
89696 91093	**Symptom**: A switch crashes and reboots. The log files for the event lists the reason for the crash as **Soft Watchdog Reset.** **Scenario**: This issue is observed in large traffic along with multicast packets. This issue is observed in OAW-40xx Series and OAW-4x50 Series switches. **Platform:** OAW-40xx Series and OAW-4x50 Series switches. **Reported Version:** AOS-W 6.4.0.0. **Workaround:** None
93172 107749	**Symptom:** Configuring Virtual Router Redundancy Protocol (VRRP) v2 instance on untrusted port causes VRRP flaps. **Scenario:** This issue is caused by bandwidth policing. This issue does not occur when the VRRP instance is configured on a trusted port. This issue is observed in switches running AOS-W 6.3.x or AOS-W 6.4.0.0. **Platform:** All platforms. **Reported Version:** AOS-W 6.4.0.0. **Workaround:** None.
105295 115105	**Symptom:** Switch stops responding and reboots. **Scenario:** The issue occurs when an the process that manages the command-line interface crashes due to memory corruption. This issue is observed in OAW-S3 switches and is not limited to a specific AOS-W release version. **Platform:** OAW-S3 switches. **Reported Version:** AOS-W 6.3.1.5. **Workaround:** None.

DHCP

Table 13: *DHCP Known Issues*

Bug ID	Description
108349	**Symptom:** When a client connects to a Wi-Fi network, there is a delay in getting an IP address from the DHCP server. **Scenario:** The switch drops the first DHCP packet that is relayed from the client and a delay occurs when the **ip helper-address** and the **DHCPoption 82** parameters are configured on the VLAN interface. This issue is observed in switches running AOS-W 6.1.3.x or AOS-W 6.3.x. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.7. **Workaround:** None.

Guest Provisioning

Table 14: *Guest Provisioning Known Issues*

Bug ID	Description
107175 114462	**Symptom:** Guest users fail to get an IP address from an external DHCP server. **Scenario:** This issue occurs under the following circumstances: • Guest provisioning users have **guest-access-email** enabled. • The **util_proc** process crashes on the switch. This issue is not limited to any specific switch model or AOS-W release version. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.9. **Workaround:** None.

Hardware Management

Table 15: *Hardware Management Known Issues*

Bug ID	Description
90324 94684	**Symptom:** Switch restarts unexpectedly as an internal process that monitors hardware inventory was losing file descriptors. **Scenario:** This issue is observed in switches running AOS-W 6.3.1.0. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.0. **Workaround:** None.

Licensing

Table 16: *Licensing Known Issues*

Bug ID	Description
106241 114557 117964	**Symptom:** The local switch displays an incorrect AP license usage. **Scenario:** On executing the **show ap license-usage** and **show active ap** commands, there is a discrepancy between the number of AP licenses used and the number of active APs on the local switch. This issue occurs when centralized licensing is enabled on the switch and is observed in switches running AOS-W 6.3.1.9 in a master-local topology. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.9. **Workaround:** None.

Local Database

Table 17: *Local Database Known Issues*

Bug ID	Description
95277	**Symptom:** Any RAP whitelist entry with special characters fails to synchronize with any switch, and synchronization fails for subsequent whitelist entries. **Scenario:** This issue is observed where RAP and CPsec whitelist entries are synchronized and the **description** field of a remote whitelist entry contains an apostrophe ('). This is observed in switches running AOS-W 6.3.1.2. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.2. **Workaround:** Remove the apostrophe (') from the whitelist entry description.

Master-Redundancy

Table 18: *Master-Redundancy Known Issues*

Bug ID	Description
104636 104989	**Symptom:** A local database fails to synchronize after 1010th attempt. The logs for the event listed the reason as **Last failure cause: Standby switch did not acknowledge the local user database transfer**. **Scenario:** Internal code errors in the process that manages database synchronization causes this issue. This issue is observed in a master-standby topology running AOS-W 6.3.x. **Platform:** OAW-4650 switches. **Reported Version:** AOS-W 6.3.1.8. **Workaround:** If custom Captive Portal data is not available, disable custom captive portal data synchronization by executing the **no database synchronize captive-portal-custom** command. If custom Captive Portal data is available, perform the following steps: 1. In **configuration** mode, execute the **database synchronize captive-portal-custom** command. 2. In **enable** mode, execute the **database synchronize** command to manually synchronize the database. The Captive Portal custom pages will be synchronized with the standby switch. 3. In **configuration** mode, execute the **no database synchronize captive-portal-custom** command. **NOTE:** Repeat steps 1-3 whenever the Captive Portal custom page changes.

RADIUS

Table 19: *RADIUS Known Issues*

Bug ID	Description
110230 118793	**Symptom:** The **Class Identifier** attribute is not present in the RADIUS accounting messages that are sent from the switch to the RADIUS accounting server. **Scenario:** This issue is observed in wireless networks that use 802.1X authentication. This issue is observed in switches running AOS-W 6.4.1.0. **Platform:** All platforms. **Reported Version:** AOS-W 6.4.1.0. **Workaround:** None.

Remote AP

Table 20: *Remote AP Known Issues*

Bug ID	Description
99466	**Symptom:** The output of the **show iap table** command incorrectly displays the status of IAP (branch) as UP with older tunnel inner IP, after the process that manages AP IKE exchanges fails to respond and crashes. **Scenario:** This issue is observed in switches running AOS-W 6.3.1.3. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.3. **Workaround:** None.

Station Management

Table 21: *Station Management Known Issues*

Bug ID	Description
102035	**Symptom:** The Station Management (STM) process crashes in a local switch. **Scenario:** This issue is observed in switches running AOS-W 6.3.1.1 when a corrupt or malformed packet has a wrong STA number. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.1. **Workaround:** None.

109619	**Symptom:** Users are unable to associate with an AP and the log files for the event lists the reason as **AP is resource constrained**.
	Scenario: This issue is observed when 802.11r is enabled in the SSID profile and the user is connected to the AP for the first time. This issue is observed in OAW-4x50 switches running AOS-W 6.3.1.10.
	Platform: OAW-4x50 switches.
	Reported Version: AOS-W 6.3.1.10.
	Workaround: Disable 802.11r capability from the SSID profile. The CLI commands are as follows:
	`(host) (config) #wlan ssid-profile default`
	`(host) (SSID Profile "default") #no dot11r-profile`

TACACS

Table 22: *TACACS Known Issues*

Bug ID	Description
105653	**Symptom:** The management authentication does not work when it is configured with a TACACS server. **Scenario:** This issue occurs when there is a delay in response from the TACACS server due to network congestion. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.5. **Workaround:** None.

VRRP

Table 23: *VRRP Known Issues*

Bug ID	Description
109968	**Symptom:** After reboot, the VRRP master with preemption disabled regains the master state when the uplink switch is running Rapid Spanning Tree Protocol (RSTP). **Scenario:** This issue is observed when a VRRP master with STP disabled, connects to an intermediate device with RSTP enabled. Since RSTP is enabled on an intermediate switch and disabled on the switch, the switch takes approximately 30 seconds to converge the link. While the port on the switch is UP, it failsover to the master as it does not receive VRRP advertisement packets. This issue is observed in OAW-S3 switches running AOS-W 6.3.1.13. **Platform:** OAW-S3 switches. **Reported Version:** AOS-W 6.3.1.13. **Workaround:** Enable or disable STP on both the devices.

WebUI

Table 24: *WebUI Known Issues*

Bug ID	Description
97281	**Symptom:** Users are unable to configure the extended ACLs using the WebUI. **Scenario:** This issue is observed when the Policy Enforcement Firewall (PEF) license is not installed. This issue is not limited to any specific switch model or AOS-W release version. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.3. **Workaround:** Configure ACLs from the CLI.

Web Server

Table 25: *Web Server Known Issues*

Bug ID	Description
115304	**Symptom:** During an SSL handshake for HTTPS connection establishment, a switch sends **Unrecognized name** alert to clients. Any HTTPS client or Web browser that treats this warning as a fatal error terminates the SSL handshake and does not establish the HTTPS connection with the switch. **Scenario:** This issue is observed only when a custom certificate is used for Web Server and Captive Portal. This issue does not affect the widely used Web browsers like, Chrome, Firefox, or Internet Explorer. However, custom applications that use .net framework are affected. This issue is observed in switches running AOS-W 6.3.x or later versions. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.2. **Workaround:** None.

Wi-Fi Multimedia

Table 26: *Wi-Fi Multimedia Known Issues*

Bug ID	Description
101501 107735	**Symptom:** The quality of the Lync calls is poor and the Mean Opinion Score (MOS) is low when multiple users are in power saving mode and some of the users receive downstream UDP traffic at 10 Mbps. **Scenario:** This issue is observed in OAW-AP200 Series and OAW-AP220 Series access points in tunnel and decrypt tunnel forwarding mode running AOS-W 6.3.1.8, AOS-W 6.4.0.3, or AOS-W 6.4.1.0. **Platform:** OAW-AP200 Series and OAW-AP220 Series access points. **Reported Version:** AOS-W 6.4.0.3. **Workaround:** None.

Chapter 6
Upgrade Procedures

This chapter details the software upgrade procedures. It is recommended 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

- AOS-W 6.3.1 is not recommended for customers with OAW-AP120 Series access points that routinely see over 85 clients associated to an AP. Please contact support if you have any questions.
- Beginning from AOS-W 6.3.1, the local file upgrade option in the OAW-4306 Series switch WebUI has been disabled.
- The local file upgrade option in the OAW-4x50 Series switch WebUI does not work when upgrading from AOS-W 6.2 or later. When this option is used, the switch displays the error message “Content Length exceed limit” and the upgrade fails. All other upgrade options work as expected.
- AirGroup
  - Starting from AOS-W 6.3, AirGroup is enabled by default. Upgrading the access switch from any version of AOS-W to AOS-W 6.3 converts the access switch to integrated mode switch. To continue to be in overlay mode, you must disable AirGroup on the access switch running AOS-W 6.3.
  - If you migrate from an overlay mode to an integrated mode, you must remove the already configured redirect ACLs from the user roles, and remove the L2 GRE tunnel from the access switch. It is recommended that you remove the overlay switch from the network or disable AirGroup on it.
- AOS-W 6.3 does not allow you to create redundant firewall rules in a single ACL. AOS-W considers 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 versions and your configuration contains an ACL with redundant firewall rules, upon upgrading, only the last rule remains.

For example, in the following ACL, both ACE entries could not be configured in AOS-W 6.3. When a second ACE entry is done, 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
```

- When upgrading the software in a multiswitch network (one that uses two or more 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 26.)
- RFPlan and RFLocate are deprecated on the switch. Use VisualRF Plan or VisualRF in OV3600 as replacements for RFPlan and RFLocate. VisualRF adds significant features including 802.11ac support, simplified work flows, and improved accuracy. If you are currently running RFPlan or RFLocate, contact your system engineer before upgrading. The upgrade removes these features from the switch.

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 30 MB of data or more.
- In the Common Criteria evaluated configuration, software loading through SCP (secure copy) is the only supported option. Loading software through TFTP, FTP, or the WebUI 'Local File' option is not valid.
- Always upgrade the nonboot partition first. If problems occur during the upgrade, you can restore the flash, and switch back to the boot partition. Upgrading the nonboot partition gives you a smoother downgrade path should it be required.
- Before you upgrade to the current AOS-W release, 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 6.3.x User Guide*.

- The command **ip radius nas-ip** takes precedence over the command **per-server nas-ip**.

Memory Requirements

All 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, it is recommended that the following compact memory best practices are followed:

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

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 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 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 25 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 25 to back up the flash directory to a file named **flash.tar.gz**, and then issue 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 25 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

Back Up and Restore 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 the **Save Configuration** button 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. Click **Restore**.

Back Up and Restore 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. Ensure you are in **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. Use 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 with the **copy** command:

   ```
   (host) # copy tftp: <tftphost> <filename> flash: flashbackup.tar.gz
   (host) # copy usb: partition <partition-number> <filename> flash: flashbackup.tar.gz
   ```
4. Use 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 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 25.

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 multi-switch system to the current AOS-W release:

1. Load the software image onto all switches (including redundant master switches). The Master Switch should be rebooted and allowed ample time to boot up first. The Master Standby Switch should be rebooted next followed by the Local Switches.
2. In a Master - Local deployment, all switches need to be running the same AOS-W version. Switches in a Master - Local deployment do not support different AOS-W.
3. Verify that the Master, Master - Standby, and all Local switches are upgraded properly.

Upgrading to 6.3.x

Upgrading the OAW-4306 Series Switches to AOS-W 6.3.x

Customers upgrading the OAW-4306 Series switches must note the following:

- Ensure that memory and flash space requirements are met before starting the upgrade process. See Memory Requirements on page 25 for details.
- User scalability on both the OAW-4306 switch and the OAW-4306G switch has been revised to 128 and 150 users, respectively.
- The following AOS-W 6.3.x features are not supported on the OAW-4306 Series switches.
  - AppRF
  - AirGroup
  - ClearPass Profiling with IF-MAP
  - IAP-VPN

Install Using the WebUI

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 25.

When you navigate to the **Configuration** tab of the switch's WebUI, the switch may display an error message **Error getting information: command is not supported on this platform**. 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 the current AOS-W release.

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

Follow step 2 to step 11 of the procedure described in Upgrading From a Recent Version of AOS-W to install the interim version of AOS-W, and then repeat step 1 to step 11 of the procedure to download and install AOS-W 6.3.

Upgrading From a Recent Version of AOS-W

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

- 6.0.1.0 or later

- 5.0.3.1 or later (If you are running AOS-W 5.0.3.1 or the latest 5.0.x.x, review Upgrading With OAW-RAP5 and OAW-RAP5WN APs on page 28 before proceeding further.)
- 3.4.4.1 or later

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

1. Download the current AOS-W release 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 file **Alcatel.sha256** 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 if 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 onto the switch at the factory. Therefore, even if you do not manually verify the SHA hash of a software image, the switch does 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. Select the **Upload Local File** option, then click **Browse** to navigate to the saved image file on your PC or workstation.
6. Select the downloaded image file.
7. In the **partition to upgrade** field, select the non-boot partition.
8. In the **Reboot Switch After Upgrade** option field, the best practice is to select **Yes** to automatically reboot after upgrading. If you do not want the switch to reboot immediately, select **No**. Note however, that the upgrade does not take effect until you reboot the switch.
9. In **Save Current Configuration Before Reboot** field, select **Yes**.
10. Click **Upgrade**.
11. When the software image is uploaded to the switch, a popup window displays the message **Changes were written to flash successfully**. Click **OK**. If you chose to automatically reboot the switch in step 7, 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 > Switch > Switch Summary** 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 **Monitoring > Network > Network Summary** to determine if your APs are up and ready to accept clients.
3. 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 25 for information on creating a backup.

Upgrading With OAW-RAP5 and OAW-RAP5WN APs

If you have completed the first upgrade, hop to the latest version of AOS-W and your WLAN includes OAW-RAP5/OAW-RAP5WN APs. Do not proceed until you complete the following process. Once complete, proceed

to step 5 on page 28. Note that this procedure can only be completed using the switch's command line interface.

1. Check the provisioning image version on your OAW-RAP5/OAW-RAP5WN APs by executing the **show ap image version** command.
2. 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.
3. For each of the OAW-RAP5/OAW-RAP5WN APs noted in the step 2, upgrade the provisioning image on the backup flash partition by executing the following command:

   ```
   apflash ap-name <Name_of_RAP> backup-partition
   ```

   The OAW-RAP5/OAW-RAP5WN reboots to complete the provisioning image upgrade.
4. When all the OAW-RAP5/OAW-RAP5WN APs with a 3.3.2.x-based RN provisioning image have successfully upgraded, verify the provisioning image by executing the following command:

   ```
   show ap image version
   ```

   The flash (Provisioning/Backup) image version string should now show a version that does not contain the letters "rn", for example, 5.0.4.8.

If you skip the above process or fail to complete the flash (Provisioning/Backup) image upgrade to 5.0.4.x and the OAW-RAP5/OAW-RAP5WN was reset to factory defaults, the RAP cannot connect to a switch running AOS-W 6.3.1 and upgrade its production software image.

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 25.

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 the current AOS-W release.

- For AOS-W 3.x.versions earlier than AOS-W 3.4.4.1, download the latest version of AOS-W 3.4.5.x.
- For AOS-W 3.x or AOS-W 5.0.x versions earlier than AOS-W 5.0.3.1, download the latest version of AOS-W 5.0.4.x.
- For AOS-W versions 6.0.0.0 or 6.0.0.1, download the latest version of AOS-W 6.0.1.x.

Follow step 2 - step 7 of the procedure described in Upgrading from a Recent version of AOS-W to install the interim version of AOS-W, and then repeat step 1 to step 7 of the procedure to download and install AOS-W 6.3.

Upgrading from a Recent version of AOS-W

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

- 6.0.1.0 or later
- 5.0.3.1 or later. (If you are running AOS-W 5.0.3.1 or the latest 5.0.x.x, review Upgrading With OAW-RAP5 and OAW-RAP5WN APs on page 28 before proceeding further.)
- 3.4.4.1 or later

To install the AOS-W software image from a PC or workstation using the Command-Line Interface (CLI) on the switch:

1. Download the latest version of AOS-W from the customer support site.
2. Open a Secure Shell session (SSH) on your master (and local) switch(es).

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. Use the **show image version** command to check if the AOS-W images 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. Use 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 only available on the OAW-4x50 Series switches.

6. Execute the **show image version** command to verify that the new image is loaded.

   ```
   (host)# show image version
   ```

7. Reboot the switch.

   ```
   (host) #reload
   ```

8. Execute the **show version** command to verify that the upgrade is complete.

   ```
   (host)# show version
   ```

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

1. Log in to the CLI to verify that all your switches are up after the reboot.
2. Execute the **show ap active** command to determine if your APs are up and ready to accept clients.
3. Execute the **show ap database** command to verify that the number of access points and clients are what you would 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 25 for information on creating a backup.

Installing the FIPS Version of AOS-W 6.3.1.x

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

Instructions on Installing FIPS Software

NOTE

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

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

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

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

Downgrading

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

WARNING

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

CAUTION

If you do not downgrade to a previously-saved pre-6.1 configuration, some parts of your deployment may not work as they previously did. For example, when downgrading from AOS-W 6.3.1.0 to 5.0.3.2, changes made to WIPS in AOS-W 6.x prevents 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 think you have encountered this issue, use 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 pre-upgrade software version, you must perform the following steps:

1. Back up your switch. For details, see Backing up Critical Data on page 25.
2. Verify that control plane security is disabled.
3. Set the switch to boot with the previously-saved pre-6.3 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 displays 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-6.3 flash backup from the file stored on the switch. Do not restore the AOS-W 6.3.1.0 flash backup file.

- If you installed any certificates while running AOS-W 6.3.1.0, 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 filename (other than default.cfg) for Flash File System.
2. Set the switch to boot with your preupgrade configuration file by navigating to the **Maintenance > Switch > Boot Parameters** page.
   a. Select the saved preupgrade configuration file from the configuration File menu.
   b. Click **Apply**.
3. Determine the partition on which your previous software image is stored by navigating to the **Maintenance > Switch > 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).
   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 > Switch > 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 > Switch > Reboot Switch** 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 > Switch > 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 0, the backup system partition, contains the backup release AOS-W 6.1.3.5. Partition 1, the default boot partition, contains the AOS-W 6.3.1.6 image.

```
(host)#show image version
---------------------------------
Partition               : 0:0 (/dev/hda2)
Software Version        : AOS-W 6.3.1.6(Digitally Signed - Production Build)
Build number            : 43088
Label                   : 43088
```

```
Built on                : Mon Apr 07 16:46:24 2014
----------------------------------
Partition               : 0:1 (/dev/hda2)**Default boot**
Software Version        : AOS-W 6.1.3.6(Digitally Signed - Production Build)
Build number            : 43301
Label                   : 43301
Built on                : Friday Apr 18 20:41:12 2014
```

4. Set the backup system partition as the new boot partition.
   ```
   (host)# boot system partition 0
   ```
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 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. It is strongly recommended 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) 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.