AOS-W 6.3.1.16

Release Notes

AOS-W 6.3.1.16 is a software patch release that includes fixes to the issues identified in previous releases. For more information on the features described in the following sections, see the *AOS-W 6.3.x User Guide* and *AOS-W 6.3.x CLI Reference Guide*.

See the Upgrade Procedures on page 196 for instructions on how to upgrade your switch to this release.

Contents Overview

- Features in 6.3.1.x Releases on page 26 describes features and enhancements added in AOS-W 6.3.1.x.
- Regulatory Updates on page 46 lists the regulatory updates in AOS-W 6.3.1.x.
- Resolved Issues on page 54 describes issues resolved in AOS-W 6.3.1.x.
- Known Issues and Limitations on page 150 describes known issues and the workaround for issues identified in AOS-W 6.3.1.x.
- Upgrade Procedures on page 196 describes the procedures for upgrading a switch to AOS-W 6.3.1.x.

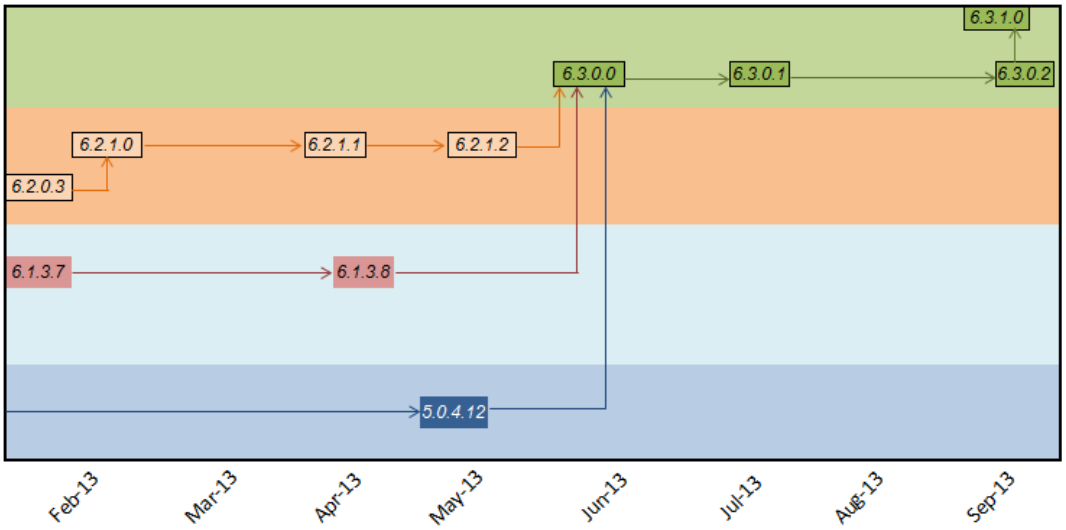
Release Mapping

This version of AOS-W is based off the 6.3.1.0 release. AOS-W 6.3.1.0 includes features and bug fixes from the following releases:

- 6.2.1.2 and all earlier 6.2.x.x releases
- 6.1.3.8 and all earlier 6.1.x.x and 6.0.x.x releases
- 5.0.4.12 and all earlier 5.0.x.x releases

The following illustration shows the patch and maintenance releases that are included in AOS-W 6.3.1.16.

Figure 1 *AOS-W Releases and Code Stream Integration*



Important Points to Remember

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.

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 once the radio is back up and running.

Table 1: *Profile Settings*

Command	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

Table 1: *Profile Settings*

Command	Description
	▪ 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 6.3.1.16 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 higher on Mac OS

Contacting Support

Table 2: *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

This chapter describes features introduced in AOS-W 6.3.1.x. For more information about features introduced in AOS-W 6.3.1.x, refer to the *AOS-W 6.3.x User Guide*.

Features Enhanced in AOS-W 6.3.1.16

This section describes the features enhanced in AOS-W 6.3.1.16.

WebUI Changes

Starting from AOS-W 6.3.1.16, the switch supports the **web-server profile** command in the **Configuration > Management > General** page of the WebUI.

Modified Commands

The following commands are modified in AOS-W 6.3.1.16.

show running-config

The default **dot1x high-watermark** and **dot1x low-watermark** values are removed from the **show running-config** command.

tar logs tech-support

The **show dot1x watermark history** command is added as part of the **techsupport.log** file.

Features Enhanced in AOS-W 6.3.1.15

This section describes the features enhanced in AOS-W 6.3.1.15.

New Commands

The following commands are introduced in AOS-W 6.3.1.15.

show web-server statistics

This command displays the web server statistics. This command helps troubleshoot Captive Portal scale issues.

Example

```
(host) #show web-server statistics

Web Server Statistics:
----------------------
Current Request Rate:            1 Req/Sec
Current Traffic Rate:            1 KB/Sec
Busy Connection Slots:           7
Available Connection Slots:      68
Total Requests Since Up Time:    284
Total Traffic Since Up Time:     1122 KB
Avg. Request Rate Since Up Time: 1 Req/Sec
Avg. Traffic Rate Since Up Time: 6144 Bytes/Sec
Server Scoreboard:               _____________KKKKKK_W_____________

Scoreboard Key:
```

```
_ - Waiting for Connection, s - Starting up
R - Reading Request, W - Sending Reply
K - Keepalive, D - DNS Lookup
C - Closing connection, L - Logging
G - Gracefully finishing, I - Idle cleanup of worker
. - Open slot with no current process
```

The output of this command includes the following parameters.

Parameter	Description
`Current Request Rate`	HTTP/HTTPS request rate measured immediately within the last one second.
`Current Traffic Rate`	HTTP/HTTPS data transfer rate measured immediately within the last one second.
`Busy Connection Slots`	Number of simultaneous HTTP/HTTPS sessions currently being served. Each session occupies one slot from the total available slots configured in the **web-max-clients** parameter.
`Available Connection Slots`	Number of simultaneous HTTP/HTTPS sessions that can be served, in addition to what is being served currently.
`Total Requests Since Up Time`	Total number of HTTP/HTTPS requests received by the web server since the server was up.
`Total Traffic Since Up Time`	Total number of HTTP/HTTPS traffic handled by the web server since the server was up.
`Avg. Request Rate Since Up Time`	Lifetime average of HTTP/HTTPS request rate. This value is calculated by dividing the total number of requests received by the web server up-time.
`Avg. Traffic Rate Since Up Time`	Lifetime average of HTTP/HTTPS traffic rate. This value is calculated by dividing the total of HTTP/HTTPS traffic by the web server up-time.
`Server Scoreboard`	Displays information for each worker thread of the web server.

Modified Commands

The following commands are modified in AOS-W 6.3.1.15.

firewall attack-rate

Starting from AOS-W 6.3.1.15, the CLI help text displays the rate as **Rate (per 30 second)** for the following commands:

- **firewall attack-rate cp**
- **firewall attack-rate ping**
- **firewall attack-rate session**
- **firewall attack-rate tcp-syn**

show web-server profile

Starting from AOS-W 6.3.1.15, the **show web-server** command is renamed to **show web-server profile**.

The following parameter is introduced as part of the output of the **show web-server profile** command:

Parameter	Description	Range	Default
`Enable bypass captive portal landing page`	Bypasses captive portal landing page. This enhancement is added to reduce the load on the switch for non-browser applications on smart devices like iPhone, iPad, and more.	—	false

web-server profile

Starting from AOS-W 6.3.1.15, the **web-server** command is renamed to **web-server profile**.

The following parameter is introduced in the **web-server profile** command:

Parameter	Description	Range	Default
`bypass-cp-landing-page`	Bypasses captive portal landing page. This enhancement is added to reduce the load on the switch for non-browser applications on smart devices like iPhone, iPad, and more.	—	enabled

Features Enhanced in AOS-W 6.3.1.14

This section describes the features enhanced in AOS-W 6.3.1.14.

Security Bulletin

As part of CVE-2014-3566 security vulnerabilities and exposures, **SSLv3** transport layer security is disabled in AOS-W starting from version 6.3.1.14.

Clients exclusively using SSLv3 will fail to access the Captive Portal and the switch WebUI. It is recommended to use TLSv1.0, TLSv1.1, or TLSv1.2 transport layer security.

To address this vulnerability, the following changes are introduced under the **web-server ssl-protocol** command.

Parameter	Description	Range	Default
`ssl-protocol`	Specifies the Secure Sockets Layer (SSL) or Transport Layer Security (TLS) protocol version used for securing communication with the web server: • TLS v1.0 • TLS v1.1 • TLS v1.2	—	tlsv1 tlsv1.1 tlsv1.2

Features Enhanced in AOS-W 6.3.1.13

This section describes the features enhanced in AOS-W 6.3.1.13.

UML295 Support

AOS-W 6.3.1.13 introduces support of the UML295 USB modem remote access points.

Features Enhanced in AOS-W 6.3.1.11

This section describes the features enhanced in AOS-W 6.3.1.11.

The **ap-power-mode** parameter under **ap provisioning-profile** is renamed to **ap-poe-power-optimization**.

Use the following commands to configure an AP to run in reduced power mode using the CLI:

```
(host) (config) #ap provisioning-profile default
(host) (Provisioning profile "default") #ap-poe-power-optimization enabled
```

Use the following command to verify the configuration using the CLI:

```
(host) (config) #show ap provisioning-profile default
Provisioning profile "default"
------------------------------
Parameter                                                    Value
---------                                                    -----
Remote-AP                                                    No
Master IP/FQDN                                               N/A
PPPOE User Name                                              N/A
PPPOE Password                                               N/A
PPPOE Service Name                                           N/A
USB User Name                                                N/A
USB Password                                                 N/A
USB Device Type                                              none
USB Device Identifier                                        N/A
USB Dial String                                              N/A
USB Initialization String                                    N/A
USB TTY device data path                                     N/A
USB TTY device control path                                  N/A
USB modeswitch parameters                                    N/A
Link Priority Ethernet                                       0
Link Priority Cellular                                       0
Cellular modem network preference                            auto
Username of AP so that AP can authenticate to 802.1x using PEAP  N/A
Password of AP so that AP can authenticate to 802.1x using PEAP  N/A
Uplink VLAN                                                  0
USB power mode                                               auto
AP POE Power optimization                                    enabled
```

Features Enhanced in AOS-W 6.3.1.10

This section describes the features enhanced in AOS-W 6.3.1.10.

AP Power Mode on OAW-AP220 Series

Starting with AOS-W 6.3.1.10, a new configuration parameter **ap-power-mode** is introduced. This parameter is available under the **ap provisioning-profile** command. When this parameter is set to **overridden**, the switch disables the USB and the Ethernet (eth1) ports of OAW-AP220 Series access points. Once the ports are disabled, the AP runs in reduced power mode.

Overriding the AP power mode sets the maximum power request for LLDP TLV to 17.1W instead of 19.0W.

In the CLI

Use the following commands to configure an AP to run in reduced power mode using the CLI:

```
(host) (config) #ap provisioning-profile default
(host) (Provisioning profile "default") #ap-power-mode overridden
```

Use the following command to verify the configuration using the CLI:

```
(host) (config) #show ap provisioning-profile default
Provisioning profile "default"
```

```
------------------------------
Parameter                                                    Value
---------                                                    -----
Remote-AP                                                    No
Master IP/FQDN                                               N/A
PPPOE User Name                                              N/A
PPPOE Password                                               N/A
PPPOE Service Name                                           N/A
USB User Name                                                N/A
USB Password                                                 N/A
USB Device Type                                              none
USB Device Identifier                                        N/A
USB Dial String                                              N/A
USB Initialization String                                    N/A
USB TTY device data path                                     N/A
USB TTY device control path                                  N/A
USB modeswitch parameters                                    N/A
Link Priority Ethernet                                       0
Link Priority Cellular                                       0
Cellular modem network preference                            auto
Username of AP so that AP can authenticate to 802.1x using PEAP  N/A
Password of AP so that AP can authenticate to 802.1x using PEAP  N/A
Uplink VLAN                                                  0
USB power mode                                               auto
AP power mode                                                overridden
```

Important Points to Remember

- By default, the AP operates in normal mode with the USB and Ethernet ports enabled.
- Changing the **ap-power-mode** parameter requires a reboot of the AP.
- In case the AP has an external DC power source, the USB and Ethernet (eth1) ports are not disabled even after setting the **ap-power-mode** to **overridden**.

Features Enhanced in AOS-W 6.3.1.9

This section describes the features enhanced in AOS-W 6.3.1.9.

Channel 144 in Regulatory Domain Profile

If Dynamic Frequency Selection (DFS) channels are enabled in the regulatory domain profile, an AP can use channel 144 as a primary or secondary channel. However, most clients do not support channel 144. Hence, when enabling DFS channel in FCC:

- If the AP is deployed in 20 MHz mode, do not use channel 144 in the regulatory domain profile.
- If the AP is deployed in 40 MHz mode, do not use channel 140-144 in the regulatory domain profile.
- If the AP is deployed in 80 MHz mode, do not use channel 132-144 in the regulatory domain profile.

This is because most older clients do not support channel 144, even though they support DFS channel. An AP in 80 MHz or 40 MHz mode chooses:

- Channel 144 as the primary channel – Here, most clients do not connect to the AP.
- Channel 140 as the primary channel and channel 144 as secondary channel – Here, most 802.11n clients do not connect to the AP over 40 MHz.

Commands Modified in AOS-W 6.3.1.9

Table 3: *Modified Commands*

Command	Description
show ap debug system-status	Changed the format of the **System Status Script** output to: **function-name(line-num): new-total-drops/total-drops new-priority-drops/total-priority-drops** Example: **wlc_dotxstatus(40576): 5034/3231117 4272/1907873** This change helps to determine if priority (voice or video) frames are dropped from the AP Wi-Fi driver drop-list. **NOTE:** The **System Status Script** is displayed for OAW-AP200 Series access points.

Features Enhanced in AOS-W 6.3.1.7

This section describes the features enhanced in AOS-W 6.3.1.7.

ARM 3.0 Enhancements

The ARM 3.0 Client Match Handoff Assist is triggered immediately after receiving the probe report and now the access point waits for 4 minutes (default value) before deauthenticating.

In the ARM profile, after 80 MHz support is disabled for OAW-AP225, one of the APs still remains on the 80 MHz channels and does not change to 40 MHz. Run the **show ap active** command to view a list of active APs.

The **Client Match Band Steer G Max Signal** parameter is added in the ARM profile to prevent clients from moving back and forth between 802.11a and 802.11g radios, and thereby reducing the oscillation frequency. By default, the value of the parameter is set to 45-dBm, this can be adjusted based on the customer's requirement.

Following is the CLI command to configure the new parameter:

```
(config) #rf arm-profile default
(Adaptive Radio Management (ARM) profile "default") #cm-band-g-max-signal ?
<cm-band-g-max-signal>  Max Signal Level of the G Band radio that can
                        trigger a Client Match band steer move (-dBm)
```

The default value of the client match threshold is modified to streamline the client match. To implement these changes, the default values of following parameters have been modified:

- Client Match Sticky Client Check SNR (default value is changed to 18 from 25)
  - `rf arm-profile <> cm-sticky-snr`
- Client Match Sticky Min Signal (default value is changed to 65 from 70)
  - `rf arm-profile <> cm-sticky-min-signal`
- Client Match Load Balancing Client Threshold (default value is changed to 30 from 10)
  - `rf arm-profile <> cm-lb-client-thresh`

Support for 340U and 341U Modems

Support for Sierra 340U and 341U modems is enabled on OAW-RAP3WN, OAW-RAP108, OAW-RAP109, and OAW-RAP155 remote access points.

Support for Multicast Rate

A new parameter, **multicast rate**, is added to configure and set the transmission rate for multicast packets in the VI (video priority) queues. This feature allows the multicast rate to be decoupled from the basic and

supported rates. This results in higher multicast rates without affecting minimum 802.11a/b/g rates used for clients.

Use the following CLI commands to configure the new parameter:

```
 #show wlan ssid-profile default | include Multicast
Multicast Rate                                    default
(config) #wlan ssid-profile default
(SSID Profile "default") #multicast-rate?
multicast-rate          Set multicast rate
(SSID Profile "default") #multicast-rate ?
12                      12 Mbps
18                      18 Mbps
24                      24 Mbps
36                      36 Mbps
48                      48 Mbps
54                      54 Mbps
6                       6 Mbps
9                       9 Mbps
default                 default (lowest configured rate)
```

Commands Modified in AOS-W 6.3.1.7

The following commands are introduced or modified in AOS-W 6.3.1.7.

Table 4: *Modified Commands*

Command	Description
`firewall attack-rate arp <1-16384> {blacklist|drop} grat-arp <1-16384> {blacklist| drop}`	The **arp** and **grat-arp** parameters are introduced in AOS-W 6.3.1.7. Sets rates which, if exceeded, can indicate a denial of service attack. • **arp**: Monitor/police ARP attack (non Gratuitous ARP). • **grat-arp**: Monitor/police Gratuitous ARP attack. **NOTE:** <1-16384> denotes the number of arp or grat-arp requests per 30 seconds.
`user-role <name> captive-portal {<STRING>|chec k-for-accounting}`	The **check-for-accounting** parameter is introduced in AOS-W 6.3.1.7. If disabled, RADIUS accounting is done for an authenticated user irrespective of the captive-portal profile in the role of an authenticated user. If enabled, accounting is not done as long as the user's role has a captive portal profile associated to it. Accounting will start when Auth/XML-Add/CoA changes the role of an authenticated user to a role which does not have a captive portal profile. This parameter is enabled by default.

Features Enhanced in AOS-W 6.3.1.4

This section describes the features enhanced in AOS-W 6.3.1.4.

AOS-W-OmniVista Cross-Site Request Forgery Mitigation

To defend against Cross-Site Request Forgery (CSRF) attacks, an enhancement is added to use randomly generated session-ID in HTTP transactions with the AOS-W WebUI. As a consequence, OmniVista must be upgraded to OmniVista 7.7.10 so that it includes the session-ID in its requests.

Upgrade Recommendations

- Upgrade to OmniVista 7.7.10 to maintain full functionality.

- Upgrade switches to AOS-W 6.3.1.4 to mitigate CSRF. Switches that are not upgraded continue to work with the upgraded OmniVista 7.7.10 as switches with an older AOS-W software image ignore the session-ID in the request.

Fixed Software Versions

- AOS-W 6.3.1.4
- OmniVista 7.7.10

Frequently Asked Questions

Q. What happens if I upgrade AOS-W but not OmniVista?

A. If the switch is upgraded to the AOS-W version mentioned above, OmniVista must also be upgraded to OmniVista 7.7.10 to maintain full functionality. If this OmniVista patch is not applied, client monitoring, AppRF information, and push certificate will not work on the switch with the upgraded AOS-W software image.

Q. What happens if I upgrade to OmniVista 7.7.10 but not all switches to AOS-W 6.3.1.4?

A. If you upgrade to OmniVista 7.7.10, switches that are not upgraded continue to work with the upgraded OmniVista 7.7.10 as switches with older AOS-W software image ignore the session-ID in the request.

Q. Where can I find more information on CSRF?

A. http://en.wikipedia.org/wiki/Cross-site_request_forgery

Default Behavior Changes

Under the **wlan ssid-profile** command, the **eapol-rate-opt** parameter is enabled by default.

Features Enhanced in AOS-W 6.3.1.3

This section describes the features enhanced in AOS-W 6.3.1.3.

Change in User Idle Timeout Behavior

Starting from AOS-W 6.2, the split-tunnel and bridge users are timed out based on the **aaa user idle-timeout** value and not based on the value set in the **L2 ageout**. As a result of this change, users with a captive-portal user role associated to an AP in split-tunnel forwarding mode assume their pre-captive-portal authentication role for a short duration.

To avoid the occurrence of this issue, you can set the value of **aaa user idle-timeout** parameter in each captive portal profile, provided you are using AOS-W 6.3 or later.

EAP-MD5 Support

The switch does not support EAP-MD5 authentication for wireless clients.

Features Enhanced in AOS-W 6.3.1.0

This section describes the features enhanced in AOS-W 6.3.1.0.

AP-Platform Support for Spectrum Analysis

Starting with AOS-W 6.3.1.0, OAW-AP120 Series access points do not support the spectrum analysis feature, and cannot be configured as a spectrum monitor or hybrid AP.

6.3.1.0 Feature Support

All features that were considered "beta quality" in AOS-W 6.3.0.0 are now fully supported in AOS-W 6.3.1.0.

Feature Support by Switch-Platform

The table below lists the AOS-W 6.3 features supported by hardware platform.

Table 5: *6.3 Feature Support by Platform*

Features	Switch			
	OAW-4550/4650/4750 Series	OAW-4704/OAW-S3	OAW-4604/OAW-4504XM	OAW-4306G/OAW-4306
AirGroup	Yes	Yes	Yes	No
AppRF 1.0/Firewall Visibility	Yes	Yes	Yes	No
IF-MAP	Yes	Yes	Yes	No
AP Image Preload	Yes	Yes	No	No
Centralized Image Upgrade	Yes	Yes	Yes	No
OAW-IAP-VPN	Yes	Yes	Yes	No
RF Planning (Switch)	No	No	No	No
Access Points	All Access Points Supported			

AP Support

AOS-W 6.3.x.x will be the last release to support the a/b/g only APs listed below. AOS-W 6.3 will be supported until October 31, 2018. Individual AP support dates will vary based on their end of sale date. -

Table 6: *AP Support*

AP Model	End of Sale Dates (Standard Variants)	Last AOS-W Version Supported
OAW-AP60, OAW-AP61, OAW-AP65, OAW-AP65WB, OAW-AP70 (All Variants)	31-May-2011	AOS-W 6.3
OAW-AP85 (All Variants)	30-Apr-2013	AOS-W 6.3
OAW-RAP2WG	31-Oct-2013	AOS-W 6.3
OAW-RAP5WN	31-Oct-2013	AOS-W 6.3
OAW-RAP5	31-Jan-2012	AOS-W 6.3

Changes to Switch Communication with OmniVista/ALE

This release of AOS-W provides support for profile-based AMON message filtering for the configured management servers such as OmniVista and Analytics Location Engine (ALE). Using this feature, you can filter

the AMON messages sent to a configured destination server (OmniVista or ALE) based on the message types enabled in the profile.

It is now mandatory to include the filtering profile while configuring the management server. The management server type **XC** in AOS-W 6.3 is now updated to ALE. In addition, the AOS-W 6.3.1 upgrade script automatically applies the pre-defined profile (default-amp and default-ale) for both OmniVista and XC servers. For more information on configuring the management server and applying message filtering, see the *AOS-W 6.3.x CLI Reference Guide*.

If you delete a management server profile that is applied to a destination server, you must re-apply a different profile to the server or re-create the same profile for the message filtering process to continue.

Adaptive Radio Management

Dynamic Scanning Enhancements

The Adaptive Radio Management (ARM) feature is improved with an enhanced scanning technique to better identify the best channels for AP channel assignments. In previous releases, when ARM performed a 40 MHz or 80 MHz scan of a channel with a high level of noise or interference (such as that caused by a video bridge), ARM also reported a high noise floor for the entire 40 MHz or 80 MHz channel set. This could prevent ARM from assigning an AP to a secondary channel.

Starting with AOS-W 6.3.1, if ARM reports a high noise floor on a channel within a 40 MHz channel pair or 80 MHz channel set, ARM performs an additional 20 MHz scan on each channel within that channel pair or set, to determine the actual noise floor of each affected channel. This allows ARM to avoid assigning the over utilized channel, while still allowing channel assignments to the other unaffected channels in that channel pair or set.

Enhanced Client Health Metric

An AP's client health is the efficiency at which that AP transmits downstream traffic to a particular client. This value is determined by comparing the amount of time the AP spends transmitting data to a client to the amount of time that would be required under ideal conditions, that is, at the maximum Rx rate supported by client, with no data retries. Starting with AOS-W 6.3.1, OAW-AP220 Series access points support the client health metric introduced in AOS-W 6.3.

A client health metric of 100% means the actual airtime the AP spends transmitting data is equal to the ideal amount of time required to send data to the client. A client health metric of 50% means the AP is taking twice as long as is ideal, or is sending one extra transmission to that client for every packet. A metric of 25% means the AP is taking four times longer than the ideal transmission time, or sending 3 extra transmissions to that client for every packet.

The client health metric appears on the **Dashboard > Performance** page of the switch WebUI, or in the output of the CLI command **show ap debug client-health**.

Cellular Handoff Assist

When both the client match and cellular handoff assist features are enabled, the cellular handoff assist feature can help a dual-mode, 3G/4G-capable Wi-Fi device such as an iPhone, iPad, or Android client at the edge of Wi-Fi network coverage switch from Wi-Fi to an alternate 3G/4G radio that provides better network access.

This feature is disabled by default, and is recommended only for Wi-Fi hotspot deployments. Enable this feature using the ARM profile in the WebUI, or through the following command in the command-line interface:

```
rf arm <profile> cellular-handoff-assist
```

AP-Platform

Support for the OAW-AP110 Series

OAW-AP114 and OAW-AP115 wireless access points support the IEEE 802.11n standard for high-performance WLAN. These dual radio access points use 3x3 MIMO (Multiple-in, Multiple-out) technology and other high-throughput mode techniques to deliver high-performance, 802.11n 2.4 GHz and 5 GHz functionality, while simultaneously supporting existing 802.11a/b/g wireless services.

Link Aggregation Support on OAW-AP220 Series

OAW-AP220 Series access points support link aggregation using either standard port-channel (configuration based) or Link Aggregation Control Protocol (protocol signaling based). OAW-AP220 Series access points can optionally be deployed with LACP configuration to benefit from the higher (greater than 1 Gbps) aggregate throughput capabilities of the two radios.

To enable and configure LACP on OAW-AP220 Series access points, configure the **LMS IP** parameter and the **GRE Striping IP** parameter in the **AP System profile**. The **GRE Striping IP** value must be an IPv4 address owned by the switch that has the specified **LMS IP**. The **GRE Striping IP** does not belong to any physical or virtual interface on the switch, but the switch can transmit or receive packets using this IP. For more information on Link Aggregation Support on OAW-AP220 Series, see the *AOS-W 6.3.x User Guide*.

LACP configuration is not applicable to the other AP models.

OAW-AP220 Series Functionality Improvements when Powered Over 802.3af (POE)

Internal AP power optimization allows for increased functionality in the OAW-AP220 Series when powered over 802.3af power. Starting in AOS-W 6.3.1, the OAW-AP220 Series will have full 802.11ac functionality when powered over 802.3af power. On standard 802.3af power, the USB port and second Ethernet port will be disabled. The 2.4 GHz radio runs with a single stream. The 5 GHz 11ac radio runs with full functionality. All features of the OAW-AP220 Series functions on 802.3at or POE+ power.

RAP Mode Support on OAW-AP220 Series

This release of AOS-W allows OAW-AP220 Series access points to be deployed as remote APs (RAPs).

Netgear Cellular Modem Support

AOS-W 6.3.1 introduces support for the Netgear 313U, 320U, and 330U 4G USB cellular modems on OAW-RAP155 remote access points.

Franklin Wireless U770 4G Modem Support

AOS-W 6.3.1 introduces support of the Franklin Wireless U770 4G USB cellular modem for the Sprint LTE service on the OAW-RAP3WN, OAW-RAP5WN, OAW-RAP108, and OAW-RAP109.

OAW-AP220 Series Legacy Feature Support

The following legacy features have been added to the OAW-AP220 Series:

- **max-tx-fail:** The number of consecutive unacknowledged transmit frames from a client, that when reached, the AP internally clears up the client state under the assumption that the client is not reachable.
- **probe response threshold:** Indicates the signal strength of the incoming probe request packet, below which the AP will not respond and send probe responses.

OAW-AP220 Series access points running AOS-W 6.3.1.x have the following limitations:

- OAW-AP220 Series access points cannot be configured as mesh nodes.

- OAW-AP220 Series access points do not support:
  - AOS-W 6.3.x.x-FIPs software images
  - 3G/4G USB Modems
  - Call admission control (CAC) and TSPEC handling features configurable in the VoIP Call Admission Control profile.

Dashboard Monitoring

AirGroup Enhancements

The **Dashboard** tab of the switch WebUI contains an **AirGroup** link that displays the information about AirGroup clients and servers. In previous releases that supported the AirGroup feature, this information was not available in the WebUI, and could only be displayed using the **show airgroup users** and **show airgroup servers** commands in the command-line interface,

Lync Interoperation with Microsoft Lync Server SDN API

AOS-W 6.3.1.0 supports Microsoft® Lync SDN API 1.2. This Microsoft® plug-in works with Microsoft® Lync server to export details about voice or video calls, desktop sharing, and file transfer to the switch's web server. AOS-W 6.3.1.0 also includes the following enhancements:

- Microsoft® Lync supports mobile devices running Windows, Android and iOS operating systems.
- The Lync SDN API 1.2 can communicate with the web server over HTTP and HTTPS protocols.
- The **web-server web-lync-listen-port** command now includes the **http** and **https** configuration parameters.

MIB and Trap Enhancements

The following traps are introduced in AOS-W 6.3.1:

- wlsxAPActiveUplinkChanged
- wlsxCertExpired
- wlsxCertExpiringSoon

For more information on these traps, download the **aruba-mibs_6.3.1.0_40232.tar** from the support site and view the **aruba-trap.my** file.

Security

Support for RADIUS Framed-IP-Address for VPN Clients

IP addresses are usually assigned to VPN clients from configured local address pools. This feature provides another way to do this by using the Framed-IP-Address attribute that is returned from a RADIUS server to assign the address.

VPN clients use different mechanisms to establish VPN connections with the switch such as IKEv1, IKEv2, EAP or a user certificate. Regardless of how the RADIUS server is contacted for authentication, the Framed-IP-Address attribute is assigned the IP address as long as the RADIUS server returns the attribute. The Framed-IP-Address value always has a higher priority than the local address pool.

Advertisement of VPN Client Host Routes Through OSPF

This feature allows VPN client addresses to be exported to OSPF, and to be advertised as host routes (/32). Exporting applies to any VPN client address regardless of how it is assigned.

Use this command to export the VPN client's assigned address to OSPF using IPC.ai

```
(host) (config) #aaa authentication vpn default
(host) (VPN Authentication Profile "default") #
(host) (VPN Authentication Profile "default") # export-route
```

Use the **show ip ospf database** command to show LSA types that are generated.

Off-Loading a Switch RAP Whitelist to CPPM

This feature allows a global whitelist to be maintained on ClearPass Policy Manager (CPPM) instead of on an individual switch. When a RAP or an OAW-IAP attempts to authenticate, the switch constructs a radius access request message for CPPM to validate. On a successful authentication, CPPM sends back a radius accept message along with the appropriate Vendor Specific Attributes (VSA).

For RAPs, the appropriate VSAs are **Aruba-AP-Group** and **Aruba-Location-Id**.

This feature allows whitelist entries to be maintained externally in CPPM for RAPs. The switch, if configured to use an external server, can send a RADIUS access request to a CPPM server. The RAP MAC address is used as a username and password to construct the access request packet and the CPPM validates the RADIUS message and returns the relevant parameters for the authorized RAPs.

If the RAP was initially an Instant AP (OAW-IAP), then the RADIUS access request is sent to the CPPM server with the OAW-IAP Ethernet address as the username. CPPM verifies if the corresponding entry exists in its local database. Depending on the configured policy, CPPM sends an access reject or accept with attributes that are applicable to the switch.

Serviceability

OAW-AP220 Series Serviceability Enhancements

The following enhancements have been added to the OAW-AP220 Series to improve AP troubleshooting, and used under the supervision Alcatel-Lucent Technical Support.

- **Packet Capture Raw Mode:** Raw packet capture mode is now supported on the OAW-AP220 Series. To enable raw packet capture, use the ap packet-capture raw-start.
- **Crash Dump Improvements:** The number of associated clients at the time of the crash has been added to the AP kernel crash information. This enhancement is seen in the output of the command show ap debug crash-info.
- **Driver Log Improvements:** The log buffer and show command buffer length has been increased from 4k to 16k. This will prevent the logs from rolling over and causing a loss of information. This enhancement is seen in the output of the **show ap debug driver-log** command.

Spectrum Analysis

Enhanced Support for Spectrum Monitor and Hybrid AP Modes

OAW-AP220 Series and OAW-AP110 Series access points can now be configured as spectrum monitors (AP radios that gather spectrum data but do not service clients), or as hybrid APs (APs that serve clients as access points while analyzing spectrum analysis data for the channel the radio uses to serve clients).

Features Introduced in AOS-W 6.3.0.0

This section lists the features introduced in AOS-W 6.3.0.0.

Support for the OAW-AP220 Series

On the OAW-AP220 Series, regardless of what is configured on the switch, the DTIM value for all virtual APs (VAP) is set to one (1).

In AOS-W 6.3, the MPDU Aggregation option under the HT SSID Profile does not affect the OAW-AP220 Series. This means that aggregation is always enabled on the OAW-AP220 Series and disabling the MPDU Aggregation option will have no effect. If you need to disable aggregation, you must disable High Throughput and Very High Throughput in the 802.11a and 802.11g radio profiles under RF Management.

The new OAW-AP220 Series of access points support 802.11ac on the 5 GHz band using 80 MHz channels. The following new features and configuration parameters have been introduced to support configuration of Very High Throughput (VHT) settings.

Table 7: *WLAN HT-SSID Profile Settings for VHT*

Parameter	Description
80MHz-enable	Enables or disables the use of 80 MHz channels on Very High Throughput (VHT) APs.
very-high-throughput-enable	Enable/Disable support for Very High Throughput (802.11ac) on the SSID. Default: Enabled
vht-supported-mcs-map	Modulation Coding Scheme (MCS) values or ranges of values for spatial streams 1 through 3. Valid values for the maximum MCS settings are 7, 8, 9 or a dash (-) if a spatial stream is not supported. If a MCS is not valid for a particular combination of bandwidth and number of spatial streams, it will not be used. Default: 9,9,9
vht-txbf-explicit-enable	Enable or disable VHT Explicit Transmit Beamforming. When this feature is enabled, the AP requests information about the MIMO channel and uses that information to transmit data over multiple transmit streams using a calculated steering matrix. The result is higher throughput due to improved signal at the beamformee (the receiving client). If this setting is disabled, all other transmit beamforming settings will not take effect. Default: Enabled
vht-txbf-sounding-interval	Time interval in seconds between channel information updates between the AP and the beamformee client. Default 25 seconds

RF 802.11a/g Radio Profiles

The following parameters were added to the RF 802.11a radio profile:

Table 8: *802.11a Radio Settings for VHT*

Parameter	Description
very-high-throughput-enable	Enable/Disable support for Very High Throughput (802.11ac) on the radio. Default: Enabled

RF ARM Profile Changes

The following parameter was added to the RF ARM profile:

Table 9: *RF ARM Settings for VHT*

Parameter	Description
80MHz-support	If enabled, this feature allows ARM to assign 80 MHz channels on APs that support VHT. Default: Enabled

Regulatory Domain Profile Changes

The following parameter was added to the regulatory domain profile:

Table 10: *Regulatory Domain Settings for VHT*

Parameter	Description
valid-11a-80mhz-channel-group	This parameter defines which 80MHz channels on the "a" band are available for assignment by ARM and for switch to randomly assign if user has not specified a channel. The channel numbers below correspond to channel center frequency. • Possible choices in US: 42, 58, 106, 122, 138, 155 • Possible choices in EU: 42, 58, 106, 122 • Possible choices in JP: 42, 58, 106, 122 • Possible choices global: 42, 58, 106, 122, 138, 155

Centralized Licensing

Centralized licensing simplifies licensing management by distributing AP, PEFNG, RF Protect, xSec and ACR licenses installed on one switch to other switches on the network. One switch acts as a centralized license database for all other switches connected to it, allowing all switches to share a pool of unused licenses. The primary and backup licensing server can share a single set of licenses, eliminating the need for a redundant license set on the backup server. Local licensing client switches maintain information sent from the licensing server, even if licensing client switch and licensing server switch can no longer communicate.

You can use the centralized licensing feature in a master-local topology with a redundant backup master, or in a multi-master network where all the masters can communicate with each other (for example, if they are all connected to a single OmniVista server). In the master-local topology, the master switch acts as the primary licensing server, and the redundant backup master acts as the backup licensing server. In a multi-master network, one switch must be designated as a primary server and a second switch configured as a backup licensing server.

Enable and configure this feature using the **Configuration > Switch** > **Centralized Licenses** tab in the WebUI, or using the **licensingprofile** commands in the command-line interface.

Primary and Backup Licensing Servers

Centralized licensing allows the primary and backup licensing server switches share a single set of licenses. If you do not enable this feature, the master and backup master switch each require separate, identical license sets. The two switches acting as primary and backup license servers must use the same version of AOS-W, and must be connected on the same broadcast domain using the Virtual Router Redundancy Protocol (VRRP). Other client switches on the network connect to the licensing server using the VRRP virtual IP address configured for that set of redundant servers. By default, the primary licensing server uses the configured virtual IP address. However, if the switch acting as the primary licensing server becomes unavailable, the secondary licensing server will take ownership of the virtual IP address, allowing licensing clients to retain seamless connectivity to a licensing server.

Only one backup licensing server can be defined for each primary server.

Communication between the License Server and License Clients

When you enable centralized licensing, information about the licenses already installed on the individual client switches are sent to the licensing server, where they are added into the server's licensing table. The information in this table is then shared with all client switches as a pool of available licenses. When a client switch uses a

license in the available pool, it communicates this change to the licensing server master switch, which updates the table before synchronizing it with the other clients.

Client switches do not share information about factory-installed or built-in licenses to the licensing server. A switch using the centralized licensing feature will use its built-in licenses before it consumes available licenses from the license pool. As a result, when a client switch sends the licensing server information about the licenses that client is using, it only reports licenses taken from the licensing pool, and disregards any built-in licenses used. For example, if a switch has a built-in 16-AP license and twenty connected APs, it disregards the built-in licenses used, and reports to the licensing server that it is using only four AP licenses from the license pool.

When centralized licensing is first enabled on the licensing server, its licensing table only contains information about the licenses installed on that server. When the clients contact the server, the licensing server adds the client licenses to the licensing table, and then it sends the clients back information about the total available licenses for each license type. In the following example, the licenses installed on two client switches are imported into the license table on the license server. The licensing server then shares the total number of available licenses with other switches on the network.

When a new AP associates with a licensing client, the client sends updated licensing information to the server. The licensing server then recalculates the available total, and sends the revised license count back to the clients. If a client uses an AP license from the license pool, it also consumes a PEFNG and RF Protect license from the pool, even if that AP has not enabled any features that would require that license.

AirGroup

AirGroup is a unique enterprise-class capability that leverages zero configuration networking to allow mobile device technologies, such as the AirPrint wireless printer service and the AirPlay mirroring service, to communicate over a complex access network topology.

With AirGroup:

- End users can register their personal devices and define a group of other users, such as friends and roommates, who are allowed to share their registered devices.
- Administrators can register and manage an organization's shared devices (like printers and conference room Apple TVs). An administrator can grant global access to each device, or limit access to users with a specified user name, role, or user location.

For more information on AirGroup, see the *AOS-W 6.3 User Guide*.

High Availability: Fast Failover

AOS-W 6.3 introduces the High Availability: Fast Failover feature. This WLAN redundancy solution allows a campus AP to rapidly fail over from an active to a standby switch without needing to rebootstrap, and significantly reduces network downtime and client traffic disruption during network upgrades or unexpected failures. APs using the High Availability: Fast Failover feature regularly communicate with the standby switch, so the standby switch has only a light workload to process if an AP failover occurs. This results in very rapid failover times, and a shorter client reconnect period. Previous redundancy solutions (like a backup-LMS) put a heavy load on the backup switch during failover, resulting in slower failover performance.

This feature supports failover for campus APs in tunnel forwarding mode only. It does not support failover for remote APs or campus APs in bridge forwarding mode.

A switch using this feature can have one of three high availability roles – active, standby or dual. An **active** switch serves APs, but cannot act as a failover standby switch for any AP except the ones that it serves as active. A **standby** switch acts as a failover backup switch, but cannot be configured as the primary switch for any AP. A **dual** switch can support both roles, and acts as the active switch for one set of APs, and also acts as a standby switch for another set of APs.

The High Availability: Fast Failover feature supports redundancy models with an active switch pair, or an active/standby deployment model with one backup switch supporting one or more active switches. Each of these clusters of active and backup switches comprises a high-availability group. Note that all active and backup switches within a single high-availability group must be deployed in a single master-local topology.

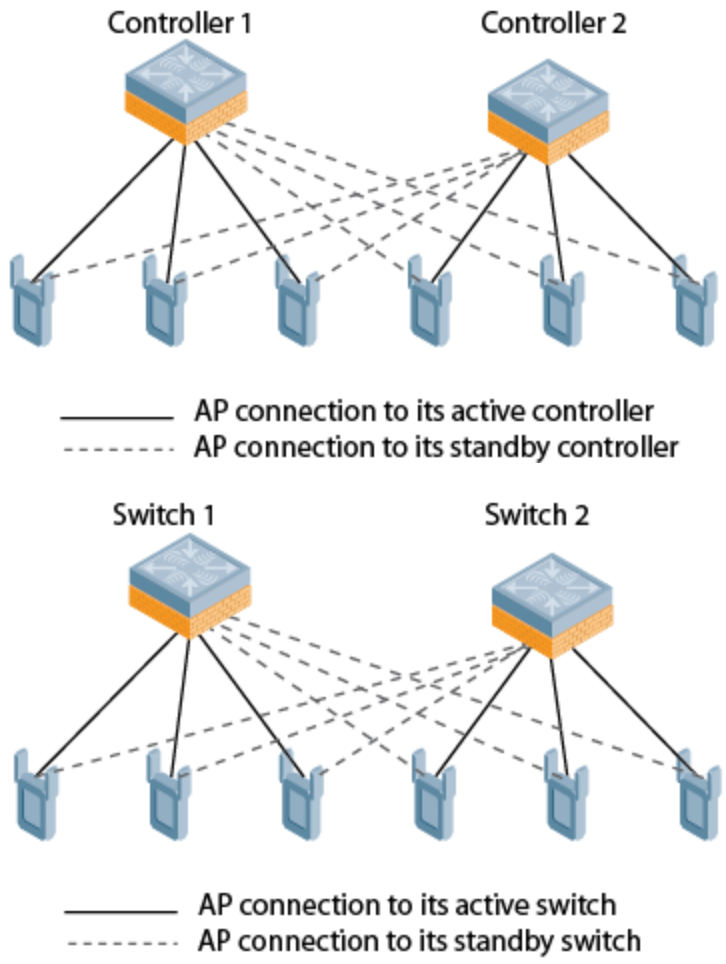
High Availability groups support the following deployment modes.

- Active/Active Deployment model on page 42
- 1:1 Active/Standby Deployment model on page 42
- N:1 Active/Standby Deployment model on page 43

Active/Active Deployment model

In this model, two switches are deployed in dual mode. Switch one acts as standby for the APs served by switch two, and vice-versa. Each switch in this deployment model supports approximately 50% of its total AP capacity, so if one switch fails, all the APs served by that switch would fail over to the other switch, thereby providing high availability redundancy to all APs in the cluster.

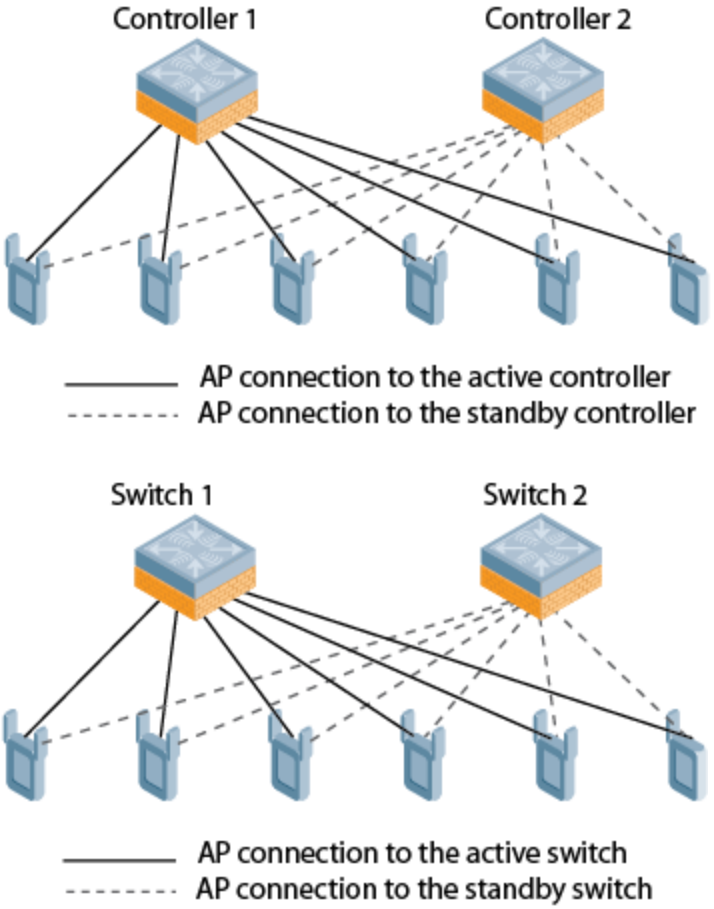
Figure 2 *Active-Active HA Deployment*



1:1 Active/Standby Deployment model

In this model, the active switch supports up to 100% of its rated AP capacity, while the other switch in standby mode is idle. If the active switch fails, all APs served by the active switch would failover to the standby switch.

Figure 3 *1:1 Active/Standby Deployment*



N:1 Active/Standby Deployment model

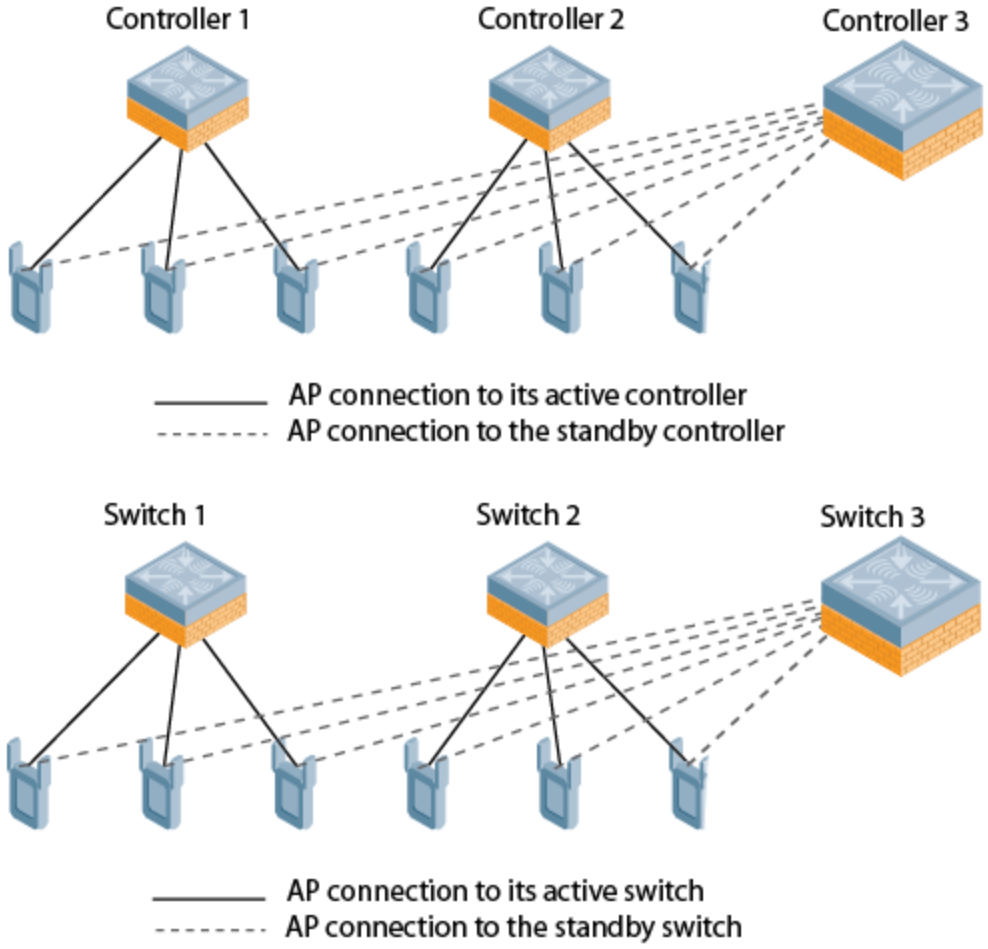
In this model, the active switch supports up to 100% of its rated AP capacity, while the other switch in standby mode is idle. If an active switch fails, all APs served by the active switch would failover to the standby switch.

NOTE

This model requires that the AP capacity of the standby switch is able to support the total number of APs distributed across all active switches in the cluster.

In the cluster shown in the example below, the standby switch has enough AP capacity to support the total number of APs terminating on the active switches. (Switch 1 and Switch 2)

Figure 4 *1:1 Active/Standby Deployment*



AP Communication with Switches

The High Availability: Fast Failover features works across Layer-3 networks, so there is no need for a direct Layer-2 connection between switches in a high-availability group.

When the AP first connects to its active switch, the active switch provides the IP address of a standby switch, and the AP attempts to establish a tunnel to the standby switch. If an AP fails to connect to the first standby switch, the active switch selects a new standby switch for that AP, and the AP will attempts to connect to that standby switch.

An AP will failover to its backup switch if it fails to contact its active switch through regular heartbeats and keepalive messages, or if the user manually triggers a failover using the WebUI or CLI.

Configure the High Availability feature in the WebUI using the **Configuration > Advanced Services > All Profiles > HA profile** page or using **the ha-group-profile** command in the command-line interface.

The following regulatory updates are introduced in AOS-W 6.3.1.x releases.

Periodic regulatory changes may require modifications to the list of channels supported by AP. For a complete list of channels supported by AP using a specific country domain, access the switch command-line interface and issue the command **show ap allowed-channels country-code <country-code> ap-type <ap-model>**.

Regulatory Updates in AOS-W 6.3.1.16

The following table describes regulatory updates introduced in AOS-W 6.3.1.16.

Table 11: *Regulatory Domain Updates*

Regulatory Domain	Regulatory Changes
Mauritius	Support added for OAW-AP135 access points.
Maritime, Maritime Offshore	Support added for OAW-AP114, OAW-AP115, AP-103, AP-103H, OAW-AP274, OAW-AP275, OAW-AP224, OAW-AP225 access points and OAW-RAP155, OAW-RAP155P, OAW-RAP108, OAW-RAP109 remote access points.

Regulatory Updates in AOS-W 6.3.1.15

There are no regulatory updates introduced in AOS-W 6.3.1.15.

Regulatory Updates in AOS-W 6.3.1.14

The following table describes regulatory updates introduced in AOS-W 6.3.1.14.

Table 12: *Regulatory Domain Updates*

Regulatory Domain	Regulatory Changes
Macedonia	Support added for OAW-AP225 access points.

Regulatory Updates in AOS-W 6.3.1.13

The following table describes regulatory updates introduced in AOS-W 6.3.1.13.

Table 13: *Regulatory Domain Updates*

Regulatory Domain	Regulatory Changes
Papua New Guinea	Support added for OAW-AP225 access points.
Bolivia	Support added for OAW-AP225 access points.
Botswana	Support added for OAW-AP225 access points.

Table 13: *Regulatory Domain Updates*

Regulatory Domain	Regulatory Changes
Sri Lanka	Support added for OAW-AP105, OAW-AP135, and OAW-AP225 access points.
Namibia	Support added for OAW-AP224 and OAW-AP225 access points.

Regulatory Updates in AOS-W 6.3.1.12

There are no regulatory updates introduced in AOS-W 6.3.1.12.

Regulatory Updates in AOS-W 6.3.1.11

There are no regulatory updates introduced in AOS-W 6.3.1.11.

Regulatory Updates in AOS-W 6.3.1.10

The following table describes regulatory updates introduced in AOS-W 6.3.1.10.

Table 14: *Regulatory Domain Updates*

Regulatory Domain	Regulatory Changes
Bahamas	Support added for OAW-AP224 and OAW-AP225 access points.
Colombia	FCC DFS channels added to OAW-AP224 and OAW-AP225 access points.
Dominica Republic	FCC DFS channels added to OAW-AP224 and OAW-AP225 access points.
Hong Kong	Channels 141-165 enabled for OAW-AP124, and OAW-AP125 access points.
Israel	Support ended for 802.11g 40MHz (indoor and outdoor) 8-12 and 9-13.
Maritime, Maritime Offshore	Support added for OAW-AP124, OAW-AP125, OAW-AP134, OAW-AP135, OAW-AP104, OAW-AP105, OAW-AP120, OAW-AP121, OAW-AP92, and OAW-AP93 access points.
Mauritius	Support added for OAW-AP224 and OAW-AP225 access points.
Philippines	Support added for OAW-RAP108, OAW-AP224, and OAW-AP225 access points.
Puerto Rico	FCC DFS channels added to OAW-AP224 and OAW-AP225 access points.
Venezuela	Support added for OAW-AP225 access points.
Vietnam	Support added for OAW-AP225 and OAW-AP115 access points.

Regulatory Updates in AOS-W 6.3.1.9

The following table describes regulatory updates introduced in AOS-W 6.3.1.9.

Table 15: *Regulatory Domain Updates*

Regulatory Domain	Change
Venezuela, Bahamas, Vietnam, Nicaragua	Added support for OAW-AP225 access points.
Bahamas	Added support for OAW-AP224 access points.
Vietnam	Added support for OAW-AP115 access points.
Macau, Saudi Arabia, Mexico	Added support for OAW-RAP108 and OAW-RAP109 access points.

Regulatory Updates in AOS-W 6.3.1.8

There are no regulatory updates introduced in AOS-W 6.3.1.8.

Regulatory Updates in AOS-W 6.3.1.7

The following table describes regulatory enhancements introduced in AOS-W 6.3.1.7.

Table 16: *Regulatory Domain Updates*

Regulatory Domain	Change
Albania	Added support for OAW-AP135 access points.
Indonesia	Added support for OAW-RAP108 access points.
Montenegro	Added support for OAW-AP224 and OAW-AP225 access points.
Puerto Rico, Dominican Republic, Philippines, Paraguay	Added support for OAW-AP114 access points.
Dominican Republic, Philippines, Paraguay	Added support for OAW-AP115 access points.
Albania, Argentina, Croatia, Montenegro, Serbia, Philippines, Algeria	Added support for OAW-AP104 access points.
Albania, Papua New Guinea	Added support for OAW-AP105 access points.
Saudi Arabia	Added support for OAW-AP124 and OAW-AP125 access points.
Argentina, Macedonia	Added support for OAW-RAP155 and OAW-RAP155P access points.
Albania, Bosnia, Herzegovina, China, Croatia, Puerto Rico, Serbia, Argentina, Philippines	Added support for OAW-RAP3WN and OAW-RAP3WNP access points.
Indonesia	Added support for OAW-AP175P access points.

Regulatory Domain	Change
Albania, Montenegro	Added support for OAW-AP134 access points.
Lithuania, Thailand, Algeria	Added support for OAW-AP92 access points.
Algeria, Thailand	Added support for OAW-AP93 access points.

Regulatory Updates in AOS-W 6.3.1.6

There are no regulatory updates introduced in AOS-W 6.3.1.6.

Regulatory Updates in AOS-W 6.3.1.5

The following table describes regulatory updates introduced in AOS-W 6.3.1.5.

Table 17: *Regulatory Domain Updates*

Regulatory Domain	Updates
India	Added support for OAW-AP175DC access points.
Indonesia	Added support for OAW-AP109 access points.
Senegal	Added support for OAW-AP134 and OAW-AP135 access points.

Regulatory Updates in AOS-W 6.3.1.4

The following table describes regulatory enhancements introduced in AOS-W 6.3.1.4.

Table 18: *Regulatory Domain Updates*

Regulatory Domain	Updates
India	Added support for OAW-AP175DC access points.
Indonesia	Added support for OAW-AP109 access points.
Senegal	Added support for OAW-AP134 and OAW-AP135 access points.

Regulatory Updates in AOS-W 6.3.1.3

The following table describes regulatory enhancements introduced in AOS-W 6.3.1.3.

Table 19: *Regulatory Domain Updates*

Regulatory Domain	Updates
Australia, Chile, China, Hong Kong, India, Indonesia, Israel, Japan, New Zealand, Malaysia, Mexico, Qatar, Russia, Singapore, South Africa, Saudi Arabia, Taiwan, Thailand, Ukraine	Added support for OAW-RAP155 and OAW-RAP155P access points.
Argentina, Brazil Egypt, Israel, Mexico, Russia, South Africa, South Korea, Trinidad and Tobago, Ukraine	Added support for OAW-AP114 and OAW-AP115 access points.
China	Added support for the OAW-AP114 access points.
Argentina, Brazil, Chile, India, Indonesia, Israel, Mexico, Russia, Taiwan, Trinidad and Tobago Ukraine	Added support for the OAW-AP225 access points.
Argentina, Brazil, Chile, China, India, Israel, Mexico, Russia, Taiwan, Trinidad and Tobago Ukraine	Added support for the OAW-AP224 access points.
Argentina, Uruguay, Vietnam	Added support for OAW-AP92 and OAW-AP93 access points.
Uruguay	Added support for OAW-AP104 access point.
Argentina, Chile, Israel	Added support for OAW-RAP108 and OAW-RAP109 access points.
Chile, Israel	Added support for OAW-RAP3WN and OAW-RAP3WNP access points.
Costa Rica	Added support for OAW-AP134 and OAW-AP135 access points.

Regulatory Updates in AOS-W 6.3.1.2

The following table describes regulatory enhancements introduced in AOS-W 6.3.1.2.

Table 20: *Regulatory Domain Updates*

Regulatory Domain	Change
Australia, Saudi Arabia, New Zealand, Singapore, Taiwan, Qatar, UAE, Columbia, Thailand, Chile, Hong Kong, Malaysia, Hong Kong	Added support for OAW-AP114 and W-OAW-AP115 access points.
Thailand	Added support for OAW-AP109 access points.
Taiwan	Added support for OAW-AP108 and OAW-AP109 access points.
China	Added support for OAW-AP115 access points.

Regulatory Updates in AOS-W 6.3.1.1

There are no regulatory updates introduced in AOS-W 6.3.1.1.

Regulatory Updates in AOS-W 6.3.1

The following table describes regulatory updates introduced in AOS-W 6.3.1.

Table 21: *Regulatory Domain Updates*

Regulatory Domain	Change
FCC DFS Support	Added support for OAW-AP224, OAW-AP225, OAW-RAP108, and OAW-RAP109 access points.
United States, Japan, Canada, all European countries	Added support for OAW-AP114 and OAW-AP115 access points.
Chad, Mali	AOS-W 6.3.1 introduces support for the Chad (TD) and Mali (ML) country domains. These domains follow the EU country domain settings.
Brazil, Mexico, South Africa, Algeria, Bosnia and Herzegovina, Dominican Republic, Ukraine, South Korea, Macedonia, Malaysia, Puerto Rico	Added support for the OAW-AP104 access points.
Algeria, Colombia, Bolivia, Ecuador, El Salvador, Colombia, Guatemala, Nicaragua, Panama, Puerto Rico, Venezuela, Zambia	Added support for the OAW-AP105 access points.
Algeria, Colombia, Russia	Added support for OAW-AP92 and OAW-AP93 access points.
Columbia, Dominican Republic, Mexico, Puerto Rico, Singapore	Added support for the OAW-AP93H access points.
India	Added support for the 5 GHz band on OAW-AP175P access points.
Russia, Indonesia, Bolivia, Bosnia, Columbia, Croatia, Dominican Republic, El Salvador, Guatemala, Macedonia, Panama, Puerto Rico, Ukraine, Bermuda, Venezuela, Trinidad and Tobago	Added support for the OAW-AP175P access points.
Bermuda, Bosnia and Herzegovina, Colombia, Croatia, Dominican Republic, Macedonia, Russia	Added support for the OAW-AP175DC access points.
Malaysia, Brazil, Venezuela, Bermuda, Bosnia and Herzegovina, Colombia, Croatia, Dominican Republic, Uganda, Macedonia, Russia	Added support for the OAW-AP175AC access points.
Azerbaijan, Belarus, Bosnia and Herzegovina, Colombia, Croatia, Kazakhstan, Peru, Russia, Trinidad and Tobago	Added support for the OAW-AP135 access points.
Argentina	Added support for the OAW-RAP5WN access points.
Macau	Added support for the following access points: • OAW-AP92 • OAW-AP93 • OAW-AP104 • OAW-AP105 • OAW-AP134 • OAW-AP135 • OAW-AP68 (2.4 GHz only)

Regulatory Domain	Change
	• OAW-AP175 • OAW-AP175AC • OAW-AP175DC • OAW-RAP2WG (2.4 GHz only) • OAW-RAP3WN (2.4 GHz only) • OAW-RAP3WNP (2.4 GHz only) • OAW-RAP5WN (5 GHz only)
Thailand	Added support for the following access points: • OAW-AP92 • OAW-AP93 • OAW-AP93H • OAW-AP104 • OAW-AP105 • OAW-AP134 • OAW-AP135 • OAW-AP175P • OAW-AP175AC • OAW-AP175DC • OAW-RAP3WN • OAW-RAP3WNP
South Korea, Saudi Arabia, UAE, India, Puerto Rico, Columbia, Dominican Republic, Macau, Pakistan, Qatar	Added support for OAW-RAP108 and OAW-RAP109 access points.
Canada	Channel 165 is no longer supported on OAW-AP105 access points. DFS channels are enabled for the following access points: • OAW-AP175P • OAW-AP175AC • OAW-AP175DC
Egypt	Removed support for DFS channels on the OAW-AP125 access points.
Cyprus	Added support for DFS channels on the OAW-AP125 access points.
Bolivia, Sri Lanka	Removed support for the OAW-AP135 access points.

The following example shows indoor, outdoor and DFS channels supported by OAW-AP105 in the **United States** domain.

```
(host) #show ap allowed-channels country-code us ap-type 105
Allowed Channels for AP Type 105 Country Code "US" Country "United States"
-------------------------------------------------------------------------
PHY Type                 Allowed Channels
--------                 ----------------
802.11g (indoor)         1 2 3 4 5 6 7 8 9 10 11
802.11a (indoor)         36 40 44 48 52 56 60 64 100 104 108 112 116 132 136 140 149 153 157 1
61 165
802.11g (outdoor)        1 2 3 4 5 6 7 8 9 10 11
802.11a (outdoor)        52 56 60 64 100 104 108 112 116 132 136 140 149 153 157 161 165
802.11g 40MHz (indoor)   1-5 2-6 3-7 4-8 5-9 6-10 7-11
802.11a 40MHz (indoor)   36-40 44-48 52-56 60-64 100-104 108-112 132-136 149-153 157-161
802.11g 40MHz (outdoor)  1-5 2-6 3-7 4-8 5-9 6-10 7-11
802.11a 40MHz (outdoor)  52-56 60-64 100-104 108-112 132-136 149-153 157-161
802.11a (DFS)            52 56 60 64 100 104 108 112 116 132 136 140
```

The following issues are resolved in AOS-W 6.3.1.x releases.

Resolved Issues in AOS-W 6.3.1.16

AOS-W 6.3.1.16 is a software patch release that includes fixes for CVE-2015-0286 and CVE-2015-0292. Additionally, the following issues are resolved in AOS-W 6.3.1.16.

AP-Datapath

Table 22: *AP-Datapath Fixed Issues*

Bug ID	Description
112086 107502	**Symptom:** Clients connected to a Remote AP (RAP) in bridge forwarding mode lost connectivity and showed the wrong ESSID in the switch user table due to a corrupt AP bridge table. The issue is resolved by ensuring that the AP reads the offline Virtual APs (VAP) VLAN information in the AOS-W 6.1 format. **Scenario:** This issue was observed when the switch was upgraded from AOS-W 6.1 to 6.3. This issue occurred as there was a difference between the offline VAPs format in AOS-W 6.1 and 6.3. As a result, APs could not read the offline information stored in the AOS-W 6.1 format. This issue was observed in switches running AOS-W 6.3. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.14.

AP-Platform

Table 23: *AP-Platform Fixed Issues*

Bug ID	Description
98691 99575 112864	**Symptom:** The status of an AP showed as DOWN in the master switch although it was UP in the local switch. This issue is resolved by making internal code changes. **Scenario:** This issue was observed in a master-local topology when the master and local switches were upgraded to AOS-W 6.3.1.5. This issue was observed in OAW-4550/4650/4750 Series switches running AOS-W 6.3.1.4. **Platform:** OAW-4550/4650/4750 Series. **Reported Version:** AOS-W 6.3.1.4.
106364	**Symptom:** OAW-AP124 rebooted randomly. The log files listed the reason for the reboot as **PCI ERROR [MR_WABT]: PCI master abort detected on write**. This issue is resolved by making internal code changes. **Scenario:** This issue was observed in OAW-AP124 access points when connected to a switch as a campus AP or to a mesh network. This issue was observed in OAW-S3 switches running AOS-W 6.3.1.5. **Platform:** OAW-S3 switch. **Reported Version:** AOS-W 6.3.1.3.
110157	**Symptom:** The **show ap radio-database** command did not display the E flag for 802.11ac channel bonding. This issue is resolved by implementing internal code changes. **Scenario:** This issue was observed in switches running AOS-W 6.3.x and 6.4.x. **Platform:** All platforms. **Reported Version:** AOS-W 6.4.2.2.

Table 23: *AP-Platform Fixed Issues*

Bug ID	Description
111261	**Symptom:** OAW-AP114/OAW-AP115 sent a pause frame when the ingress packet-flow was high. This issue is resolved by disabling L2 flow control on OAW-AP114/OAW-AP115. **Scenario:** This issue occurred on OAW-AP114/OAW-AP115 access points connected to OAW-4650 switches running AOS-W 6.3.1.17. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.17.

AP-Wireless

Table 24: *AP-Wireless Fixed Issues*

Bug ID	Description
105089	**Symptom:** The wireless clients experienced packet loss when connected to the OAW-AP135/OAW-AP105 where the multicast was using Dynamic Multicast Optimization (DMO). This issue is resolved by reducing the retry tx rate for OAW-AP135/OAW-AP134/OAW-AP105/OAW-AP104 at DMO mode. **Scenario:** This issue was observed in OAW-AP135/OAW-AP105 where the DMO enabled an SSID profile and the client did not send an ACK pack when receiving high 11n rate data. **Platform:** OAW-AP135 **Reported Version:** AOS-W 6.4.1.0
109191 111963 112018	**Symptom:** Multiple OAW-AP220 Series access points stopped responding and rebooted. The log files for the event listed the reason as **kernel panic: Fatal exception in interrupt**. Improvements in the wireless driver of the AP fixed this issue. **Scenario:** This issue was caused due to fragmented multicast packets. This issue was observed in OAW-AP220 Series access points running AOS-W 6.3.1.x. **Platform:** OAW-AP220 Series. **Reported Version:** AOS-W 6.3.1.13.
111019	**Symptom:** Broadcom-based access points did not reset client idle time to zero on null data packets. The fix ensures that the idle time is reset on receiving null/qos-null data packets. **Scenario:** This issue was observed in OAW-AP225 access points connected to OAW-4306G switches running AOS-W 6.4.2.3. **Platform:** OAW-AP225 access point. **Reported Version:** AOS-W 6.4.2.3.
111913	**Symptom:** Clients frequently lost connectivity to OAW-AP105 access point because the AP detected a false RADAR and moved to another channel. The fix ensures that RADAR chirp detection support is added for OAW-AP105 to avoid false RADAR detection. **Scenario:** This issue was observed in OAW-AP105 access points operating on DFS channels. This issue was observed in OAW-AP104, OAW-AP105, OAW-AP92, and OAW-AP93 access points connected to OAW-S3 switches running AOS-W 6.1.3.11. **Platform:** OAW-AP104, OAW-AP105, OAW-AP92, and OAW-AP93 access points. **Reported Version:** AOS-W 6.1.3.11.
112246	**Symptom:** The **show ap remote bss-table** command displayed the EIRP value as 0. This issue is resolved by adding actual EIRP and maximum EIRP in SAPD message. **Scenario:** This issue occurred when a new VAP was added and the **show ap remote bss-table** command was run. This issue was observed in switches running AOS-W 6.x and was not specific to any switch model. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.10.
112293	**Symptom:** OAW-AP65 access point failed to send 802.11a radio signals. The fix ensures that the access points send 802.11a radio signals. **Scenario:** This issue was observed in OAW-AP65 access points running AOS-W 5.0.4.11. **Platform:** OAW-AP65 access point. **Reported Version:** AOS-W 5.0.4.11.

ARM

Table 25: *ARM Fixed Issues*

Bug ID	Description
111543	**Symptom:** Adaptive Radio Management (ARM) failed to work for the Egypt country domain. Changes in the internal code ensures that ARM works correctly for the Egypt country domain. **Scenario:** This issue was seen when 40 MHz assignment was enabled in the ARM profile. This issue was observed in 802.11n and 802.11ac-capable access points running AOS-W 6.3.1.14. **Platform:** 802.11n and 802.11ac-capable access points. **Reported Version:** AOS-W 6.3.1.14.

Base OS Security

Table 26: *Base OS Security Fixed Issues*

Bug ID	Description
109982 111254	**Symptom:** The **extifmgr** process crashed while sending IF-MAP requests. This issue is resolved by implementing internal code changes. **Scenario:** This issue was observed in OAW-40xx Series, OAW-4x04 Series, and OAW-S3 switches running AOS-W 6.3.x and 6.4.x. **Platform:** OAW-40xx Series, OAW-4x04 Series, and OAW-S3 switches. **Reported Version:** AOS-W 6.4.2.2
111116	**Symptom:** When IP mobility was enabled, users were able to get a DHCP IP even if they failed MAC authentication. This issue is resolved by adding a check to ensure that there is a valid **L3** role and **L3acl** before downloading datapath. **Scenario:** This issue was observed in switches running AOS-W 6.4.2 and earlier versions. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.13.
113359	**Symptom:** An increase in memory was observed for the authentication process in the switch. Freeing memory from the authentication process resolved this issue. **Scenario:** This issue was observed when an AP associated with the switch. This issue was observed in switches running AOS-W 6.3.1.x. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.3.

Switch-Datapath

Table 27: *Switch-Datapath Fixed Issues*

Bug ID	Description
102315	**Symptom:** When packets were reordered, the first fragment was received last, but all the fragments were sent out. As a result, the fragment context could not be released, resulting in very low download speed over site-to-site VPN. This issue is resolved by deleting the fragment context immediately instead of them going through the aging process. **Scenario:** This issue was observed in a WAN between master and local switches. This issue was observed in all switches running AOS-W 6.2.x version onwards. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.7.
108007	**Symptom:** An AP was not able to connect to a master switch. The fix ensures that the PAPI packet reassembly is handled appropriately. **Scenario:** This issue was observed when OAW-AP225 tried to connect to a OAW-4704 switch running AOS-W 6.3.1.9. This issue was observed in a topology where the AP and the master switch were in different locations and connected through an IPsec tunnel. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.9.

Licensing

Table 28: *Licensing Fixed Issues*

Bug ID	Description
103538	**Symptom:** The switch generated the following license warning message: **300145: <WARN> |licensemgr| Licenses sent by the server will expire in 29 days**. These were false warning messages and the fix ensures that the switch generates legitimate warning messages only. **Scenario:** This issue was observed when the switch was upgraded to AOS-W 6.3.1.8 or later versions. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.8.

Remote AP

Table 29: *Remote AP Fixed Issues*

Bug ID	Description
107527	**Symptom:** A wired bridge user was mapped with incorrect ACLs even though the wired bridge user was mapped with the correct user role. This issue is resolved by overloading the ingress field with wired port and fetching the correct AAA profile. **Scenario:** This issue was observed in RAPs connected to switches running AOS-W 6.3.1.8. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.8.
109380	**Symptom:** When the **show ap debug usb ap-name <ap name>** command was executed on a RAP, the output did not display Supported Network Services, Firmware Version, or ESN Number. The fix ensures that these values are displayed when the **show ap debug usb ap-name <ap name>** is executed. **Scenario:** This issue was observed in UML-295 modems connected to OAW-RAP5WN/OAW-RAP155 running AOS-W 6.3.1.12. **Platform:** RAPs supporting UML-295 modems. **Reported Version:** AOS-W 6.3.1.12.
113845	**Symptom:** The **show user-table** command output occasionally does not display a bridge-mode. Implementing code changes resolves this issue. **Scenario:** This issue was observed when the chipset driver did not send deauthentication frame with reason client-match when the client was in power save mode. **Platform:** All RAPs. **Reported Version:** AOS-W 6.3.1.10.

SNMP

Table 30: *SNMP Fixed Issues*

Bug ID	Description
111767	**Symptom:** SNMP configuration errors like **Configuration error: Only support physical Interface 24577 in snmpGetIfEthTable, snmp_switch.c:591** were logged. This issue is resolved by disabling debug log. **Scenario:** This issue occurred when SNMP debug was enabled using the **logging level warnings system subcat snmp** command or when an SNMP walk was performed. This issue was observed in switches running AOS-W 6.3.1.0, but was not specific to any switch model. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.0.

VRRP

Table 31: *VRRP Fixed Issues*

Bug ID	Description
111451	**Symptom:** On adding the sixty-third VRRP instance on the switch, the WebUI and CLI got stuck showing the VRRP instance in an infinite loop. This issue is fixed by changing a software logic error. **Scenario:** This issue was seen because of a software logic error. This issue was seen in switches running AOS-W 6.3.1.x or 6.4.x. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.8.

WMM

Table 32: *WMM Fixed Issues*

Bug ID	Description
111647	**Symptom:** The count of Tx WMM [VO] dropped packets increased without a voice client. The Tx WMM [VO] dropped packets count was determined from BAR frame Tx statistics. When a BAR frame was transmitted but a corresponding BA frame was not received from a client, the Tx WMM [VO] dropped packets count was incremented. This issue is resolved by: • Counting only the data frames into Tx WMM [priority] dropped statistics if a frame transmission fails. • Not counting the transmitting management or control frame into Tx WMM [VO] or Tx WMM [BE] statistics. **Scenario:** This issue occurred in OAW-AP135 and OAW-AP125 access points connected to switches running AOS-W 6.3.1.9. **Platform:** OAW-AP135 and OAW-AP125. **Reported Version:** AOS-W 6.3.1.9.

Resolved Issues in AOS-W 6.3.1.15

AOS-W 6.3.1.15 is a software patch release that includes a fix for CVE-2015-1388. Additionally, the following issues are resolved in AOS-W 6.3.1.15.

AirGroup

Table 33: *AirGroup Fixed Issues*

Bug ID	Description
108014	**Symptom:** Occasionally, an incorrect last queried time was displayed in the output of the **show airgroup user verbose** command. This issue is resolved by implementing internal code changes. **Scenario:** This issue was observed when an invalid mDNS or DLNA packet was received and the default last queried time was displayed. This issue was not limited to a specific switch model or AOS-W release version. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.9.
108316	**Symptom:** When a refresh query is sent by the switch, some printers did not respond with the complete set of records (SRV/A/AAAA/TXT). This issue is resolved by making changes to the way the switch queries for printer information. **Scenario:** This issue was observed when the switch sent an mDNS query, but some HP and Epson printers did not send a reply with all the records (SRV/A/AAAA/TXT). This issue was observed in switches running AOS-W 6.3.x versions. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.6.
109808	**Symptom:** During an initial or refresh query, mDNS used the switch IP as the source IP and as a result some servers were not discovered. This issue is resolved by using the VLAN IP as the source IP for mDNS queries. **Scenario:** This issue was observed in OAW-4550 switches running AOS-W 6.3.1.13. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.13.
110283	**Symptom:** The discovery of the printer proxy servers failed and the clients did not connect to AirPrint printers. This issue is resolved by improvements to how the switch queries for printer information. **Scenario:** This issue was observed in OAW-4604 switches running AOS-W 6.3.1.13. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.13.

AP-Platform

Table 34: *AP-Platform Fixed Issues*

Bug ID	Description
107806	**Symptom:** When a wireless client associated with a bridge forwarding mode SSID, some of the Gratuitous ARP (GARP) packets from the client had an incorrect VLAN tag ID. This issue is resolved by sending GARP packets with the VLAN ID when the client successfully associates with the bridge forwarding mode SSID. **Scenario:** To support mobility, the AP counterfeited GARP requested for the clients, but the GARP request did not use the VLAN tag ID. This issue was observed in switches running AOS-W 6.2.1.7. **Platform:** OAW-4x50 switches. **Reported Version:** AOS-W 6.2.1.7.

AP-Wireless

Table 35: *AP-Wireless Fixed Issues*

Bug ID	Description
110195	**Symptom:** Windows 8 and Windows 10 clients were unable to switch between guest network and corporate network. This issue is resolved by implementing internal code changes to address how the virtual AP authorizes clients switching from another virtual AP on the same radio. **Scenario:** This issue was observed in OAW-AP105 access points connected to OAW-4504 switches running AOS-W 6.3.1.10 in a master-standby topology. **Platform:** OAW-AP105. **Reported Version:** AOS-W 6.3.1.10.
111854	**Symptom:** An OAW-AP125 sent many Block Acknowledge Retry (BAR) requests to the client because it did not receive Block Acknowledge (BA) from the client. This issue is resolved by reducing the retry counts per BAR frames. **Scenario:** This issue was observed in clients when the **Allow the computer to turn off this device to save power** NIC power management option was enabled on the client device. This issue was observed in OAW-AP125 and OAW-AP105 access points connected to switches running AOS-W 6.3.1.9. **Platform:** OAW-AP125 and OAW-AP105. **Reported Version:** AOS-W 6.3.1.9.

Base OS Security

Table 36: *Base OS security Fixed Issues*

Bug ID	Description
107252	**Symptom:** A memory leak was observed in the **authentication** process of the switch. This issue is resolved by implementing internal code changes. **Scenario:** This issue was seen in the LDAP server keepalive/connection operation of the switch. This issue was observed in switches running AOS-W 6.3.1.5. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.5.
111030	**Symptom:** The switch classified a Lumia Windows 8.1 mobile phone as Android in the user table. This issue is resolved by implementing internal code changes to how user agent strings from the client are parsed by the switch. **Scenario:** This issue was observed in switches running AOS-W 6.3.x or 6.4.x. **Platform:** All platforms. **Reported Version:** AOS-W 6.4.2.2.

Configuration

Table 37: *Configuration Fixed Issues*

Bug ID	Description
106791	**Symptom:** A RADIUS key was not synchronized with the standby switch. This issue is resolved by making changes to the key values in the RADIUS profile to accept a string length of more than 256 characters. **Scenario:** This issue occurred when the clear text key length was 110 characters, whereas the encrypted length was more than 256 characters. This issue was observed in standby switches in a master-standby topology running AOS-W 6.3.1.8. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.8.

Switch-Datapath

Table 38: *Switch-Datapath Fixed Issues*

Bug ID	Description
100756 110071	**Symptom:** A switch stopped responding and rebooted. The log files listed the reason for the event as **datapath exception**. This issue is resolved by internal changes that updated the IP header length with the appropriate value. **Scenario**: This issue was observed when the **firewall deny-source-routing** table was enabled and the switch received an IP packet with invalid option header length. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.8.

Switch-Platform

Table 39: *Switch-Platform Fixed Issues*

Bug ID	Description
108536 108794 108797 109386 110061 110072 110723 111313 111452 111557 111981	**Symptom:** A OAW-4550/4650/4750 Series switch rebooted unexpectedly. The log files listed the reason for the crash as **Reboot Cause: kernel panic**. This issue is resolved by implementing internal code changes. **Scenario**: This issue occurred when captive portal was enabled on the switch. This issue was observed in OAW-4550/4650/4750 Series switches and is not specific to any AOS-W release version. **Platform:** OAW-4550/4650/4750 Series switches. **Reported Version:** AOS-W 6.3.1.8.
110482	**Symptom:** The link between a switch and an external switch using the SFP module did not come up. This issue is resolved by using an SFP module that is compatible with an external switch. **Scenario**: This issue was observed in OAW-4550 switches running AOS-W 6.3.1.10 in master-local topology. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.10.
111549	**Symptom:** A local switch crashed and rebooted. The log files listed the reason for the crash as **Hard Watchdog reset**. This issue is resolved by implementing internal code changes. **Scenario:** This issue was observed in XLP chipset with OAW-AP105, OAW-AP125, OAW-AP135, and OAW-AP115 access points connected to switches running AOS-W 6.4.2.3. **Platform:** All platforms. **Reported Version:** AOS-W 6.4.2.3.

IPSec

Table 40: *IPSec Fixed Issues*

Bug ID	Description
105112 109796	**Symptom:** The management protocol [IKE] in the VPN module crashed when revocation check of certificates was performed multiple times. This issue is resolved by ensuring that the **exchange** element in IKE is set to NULL for all the corresponding requests of that exchange, when exchange is freed. **Scenario:** This issue was observed when the **exchange** element was set to NULL for only one of the multiple requests, when exchange was freed. This issue was not limited to a specific switch model or release version. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.8.
111100	**Symptom**: AOS-W did not support uplink failover within a site-to-site tunnel prior to 6.3.1.15. This issue is resolved by changes that improve the way old IKEv2/IPSec security association (SA) states are deleted before a new SA is established. **Scenario**: This issue was observed in switches using IKEv2-PSK SA authentication methods for site-to-site VPNs. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.14.

IPv6

Table 41: *IPv6 Fixed Issues*

Bug ID	Description
112636	**Symptom:** The customer was unable to get an IP address using the IPv6 Neighbor Discovery (ND) protocol or Router Advertisement (RA) when the **Broadcast-filter ARP** parameter was enabled. To resolve this issue a check is introduced to observe if the MAC address obtained after unicast conversion is similar to the source MAC of the packet. If it is, then the packet is not sent to the tunnel or as multicast, depending on whether **Suppress ARP** parameter is enabled on the vlan. **Scenario:** This issue was observed when the OAW-S3 switch was upgraded from AOS-W 6.3.1.6 to 6.3.1.14. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.14.

Port-Channel

Table 42: *Port-Channel Fixed Issues*

Bug ID	Description
110563	**Symptom:** The Link Aggregation Control Protocol (LACP) timed out and did not send Link Aggregation Control Protocol Data Units (LACDUs). This issue is resolved by implementing internal code changes. **Scenario:** This issue was observed in OAW-S3 switches connected to routers that use LACP over 1 Gigabit Ethernet links. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.13.

Remote AP

Table 43: *Remote AP Fixed Issues*

Bug ID	Description
104073	**Symptom:** The user could not reconnect to the 3G up-link sites after upgrading from AOS-W 5.x to 6.x. The fix ensures that the Sierra driver on the OAW-IAP is updated to maintain compatibility. **Scenario:** This issue was observed in OAW-RAP5s connected to OAW-S3 switches running AOS-W 6.3.1.8. **Platform:** OAW-S3 switches. **Reported Version:** AOS-W 6.3.1.8.

VRRP

Table 44: *VRRP Fixed Issues*

Bug ID	Description
109845	**Symptom:** After upgrading to 6.4.2.2, the VRRP routed through a L2 GRE tunnel for non-routable VLAN was in backup state. The fix ensures that the status of the tunnel is retrieved before proceeding with lookup for master transition when the tunnel is UP. If operstate of the VRRP VLAN is UP and the tunnel state is DOWN, the VRRP routed through tunnel will fail-over to master in 120 seconds. **Scenario:** This issue was observed when VRRP instances in the tunneled VLANs was in backup state and was not being handled while receiving the link status of the VLAN. This issue was observed in OAW-4306G and OAW-4550 switches running AOS-W 6.4.2.2. **Platform:** OAW-4306G and OAW-4550 switches. **Reported Version:** AOS-W 6.4.2.2.

Resolved Issues in AOS-W 6.3.1.14

The following issues are resolved in AOS-W 6.3.1.14.

AirGroup

Table 45: *AirGroup Fixed Issues*

Bug ID	Description
102648	**Symptom:** The **mDNS** process crashed frequently. This issue is resolved by making code level changes to obtain the switch MAC address in a robust manner. **Scenario:** This issue was observed in OAW-4550/4650/4750 Series switches running AOS-W 6.4.0.3. **Platform:** OAW-4550/4650/4750 Series switches. **Reported Version:** AOS-W 6.4.0.3.
102706 108029	**Symptom:** Loss of wired connectivity was observed for a short duration, when the MAC address table was polluted on the L3 switch. This issue is resolved by ensuring that the source MAC address in the response packet and the MAC address of the switch that is sending the packet are identical. **Scenario:** This issue was observed in a switch–L3 switch–switch topology where both the switches were in the same AirGroup domain. This issue was observed on switches running AOS-W 6.3.1.7. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.7.

AP-Platform

Table 46: *AP-Platform Fixed Issues*

Bug ID	Description
105930	**Symptom:** When the **show ap debug client-stats** command was executed and there was no response from the AP, an internal process was blocked. This issue is resolved by modifying the implementation of the **show ap debug client-stats** command to avoid internal processes from being blocked. **Scenario:** This issue was observed when a message was sent to the AP after the command was executed and if the response was larger than the network MTU size then it was fragmented. If there was an issue with the network, the response did not reach the switch, so the switch waited until timeout limit was reached. During this time frame, no other AP messages were processed which caused other APs to reboot. This issue was observed in APs connected to switches running AOS-W 6.3 or later versions. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.9.
109925	**Symptom:** A mesh point failed to establish a link with the mesh portal. Adding the **wpa-supplement** process resolved this issue. **Scenario:** This issue was observed in 6.3.1.x FIPS version, as it did not include the **wpa-supplement** process for mesh. This issue was observed in OAW-AP85 connected to switches running AOS-W 6.3.1.1 - AOS-W 6.3.1.13. **Platform:** OAW-AP60/OAW-AP61/OAW-AP65/OAW-AP70/OAW-AP85 access points. **Reported Version:** AOS-W 6.3.1.12 FIPS version.
110095	**Symptom:** An AP did not renew its DHCP lease when the old DHCP server was out of service. This issue is resolved by updating the DHCP server IP in the DHCP acknowledgment packet. **Scenario:** This issue was observed when an AP sent a DHCP renewal message to the old DHCP server even when it was not present in the network. This issue was observed in APs connected to switches running AOS-W 6.3.1.x. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.x. **Workaround:** None.

AP-Wireless

Table 47: *AP-Wireless Fixed Issues*

Bug ID	Description
109972	**Symptom:** The value of Signal to Noise Ratio (SNR) was high for neighboring APs and monitored clients in AM (Air Monitor) tables. The issue is resolved by checking if SNR is within a valid range (0 to 100). If the Received Signal Strength Indicator (RSSI) value is zero, SNR is set to zero instead of RSSI – Noise. **Scenario:** This issue was observed when the hardware was unable to determine the RSSI, as a result it was set to zero and SNR became invalid. This issue was observed in OAW-AP200 Series access points connected to switches running AOS-W 6.4.3. **Platform:** OAW-AP200 Series access points. **Reported Version:** AOS-W 6.3.1.13.

Authentication

Table 48: *Authentication Fixed Issues*

Bug ID	Description
96286	**Symptom:** Username was missing in RADIUS accounting **start** packets. This issue is resolved by avoiding the usage of Pairwise Master Key (PMK) information saved in the user copy, in the absence of PMK cache. **Scenario:** This issue was observed when PMK information saved in the user copy was used to authenticate a client although the authentication server did not have the client credentials. This issue occurred on switches running AOS-W 6.3.1.2 or later versions. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.2.
107114	**Symptom:** 802.1X clients failed to authenticate. The fix ensures that 802.11r enabled tunnel-mode clients in the **ActivedotxStation** table are appropriately handled during fast-roaming. **Scenario:** This issue was observed when 802.11r enabled tunnel-mode clients roamed rapidly between access points. This issue was not specific to any switch model or AOS-W version. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.9.

Configuration

Table 49: *Configuration Fixed Issues*

Bug ID	Description
108271	**Symptom:** When a switch was out of memory and the **write memory** command was executed , Layer 2/Layer 3 configurations were not captured. This resulted in network outage of switches or APs. This issue is resolved by adding defense checks to prevent incomplete Layer 2/Layer 3 configurations, when the **write memory** command is executed and the switch is low on memory. **Scenario:** This issue was observed in switches running AOS-W 6.3.1.5 in a master local topology. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.5.

Control Plane Security Whitelist Management

Table 50: *Control Plane Security Whitelist Management Fixed Issues*

Bug ID	Description
107118	**Symptom:** The datapath route cache was corrupted because the IP address of a switch was assigned as the inner IP address of a RAP. This issue is resolved by implementing internal code changes. **Scenario:** This issue was observed when RAPs terminated on switches running AOS-W 6.3.1.8. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.8.

Switch-Datapath

Table 51: *Switch-Datapath Fixed Issues*

Bug ID	Description
106870 107973 107974 109521 109919	**Symptom:** A switch stopped responding and rebooted. The log files for the event listed the reason as **datapath exception**. Changes in the datapath module code fixed this issue. **Scenario:** This issue was observed in OAW-4704 switches running AOS-W 6.3.1.9. **Platform:** OAW-4704 switches. **Reported Version:** AOS-W 6.3.1.9.

Switch-Platform

Table 52: *Switch-Platform Fixed Issues*

Bug ID	Description
106253	**Symptom:** The **show cpu current** command displayed incorrect CPU utilization status. The value returned for the first iteration was incorrect whereas the values for the later iterations were correct. This issue is resolved by implementing internal code changes. **Scenario:** This issue occurred due to inconsistency in the value displayed. This issue was not limited to a specific switch model or AOS-W release version. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.5.
106254	**Symptom:** The system log recorded multiple instances of a particular port reaching the maximum bridge entry limit. The fix ensures that the log file is updated with the correct port information sent from the datapath to the control plane. **Scenario:** This issue was observed when STP was enabled in the network. This issue was observed in OAW-S3 and OAW-6000 Series switches running AOS-W 6.3.1.5. **Platform:** OAW-S3 and OAW-6000 Series switches. **Reported Version:** AOS-W 6.3.1.5.
106573 107888 108040 108320 108471 108986 109863 110411	**Symptom:** The **watchdog** process monitor on the switch continued to be in the **INITIALIZING** state. This issue is resolved by implementing internal code changes. **Scenario:** When the switch was rebooted, the **show process monitor statistics** command displayed the **DOGMA** process in the **INITIALIZING** state. This issue was observed in OAW-4550/4650/4750 Series switches running AOS-W 6.4.x. **Platform:** OAW-4550/4650/4750 Series switches. **Reported Version:** AOS-W 6.4.2.1.
108533	**Symptom:** After logs were introduced to track the crashes in the **firewall-visibility** process caused by DNS cache, there was an increase in the errors logged. This issue is resolved by introducing a delay logic to reduce the number of errors logged for firewall-visibility and by increasing the maximum number of mappings. **Scenario:** This issue was observed when the number of IP address mappings to DNS name increased beyond the permitted value. This issue was not limited to a specific switch model or AOS-W release version. **Platform:** All platforms. **Reported Version:** AOS-W 6.4.2.2.
109123 109414	**Symptom:** A switch became unresponsive. The log files listed the reason for the event as **Halt reboot (Intent:cause:register 13:86:0)**. **Scenario:** This issue was observed in OAW-4x04 Series switches running AOS-W 6.3.1.13. **Platform:** OAW-4x04 Series switches. **Reported Version:** AOS-W 6.3.1.13.

IPv6

Table 53: *IPv6 Fixed Issues*

Bug ID	Description
107993	**Symptom:** The switch flooded ICMPv6 Neighbor Solicitation (NS) packets to different VLANs. Duplicate Address Detection (DAD) message was sent as a multicast packet instead of a unicast packet. The fix ensures that the switch sends a DAD message as a unicast packet: • if **broadcast-filter arp** is enabled, DAD message is sent as a unicast packet to the station if the target address is already present in the user table. • if **suppress-arp** is also enabled, DAD message is not sent over the Wi-Fi tunnel if the address is not present in the user table. **Scenario:** This issue was observed when VLAN pooling was enabled for the VLAN and the DAD message was sent as a multicast packet over the Wi-Fi network. This issue was observed in switches running AOS-W 6.4.0.2. **Platform:** All platforms. **Reported Version:** AOS-W 6.4.0.2.

Remote AP

Table 54: *Remote AP Fixed Issues*

Bug ID	Description
107975	**Symptom:** OAW-RAP155 did not reboot after failing over from Ethernet to a cellular link connected to Huawei® K4505 modem. This issue is resolved by making code level changes to the usb initialization script. **Scenario:** This issue was observed in OAW-RAP155 when an usb-mode switch failed while disconnecting storage devices. This issue was observed in OAW-4550 switches running AOS-W 6.3.1.10. **Platform:** OAW-4550 switches. **Reported Version:** AOS-W 6.3.1.10.

VRRP

Table 55: *VRRP Fixed Issues*

Bug ID	Description
108693 110519	**Symptom:** After the switches were upgraded to AOS-W 6.3.1.13, the VRRP instances were still in the backup state. To resolve this issue, the VRRP state machine is restarted based on the link status instead of the STP state convergence, when the STP is globally enabled but not on the VRRP VLAN. **Scenario:** This issue was observed when STP was globally enabled but VRRP VLAN was not part of STP. This issue was observed in switches running AOS-W 6.3.1.13. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.13.

Resolved Issues in AOS-W 6.3.1.13

The following issues are resolved in AOS-W 6.3.1.13.

Air Management - IDS

Table 56: *Air Management - IDS Fixed Issues*

Bug ID	Description
101919	**Symptom:** The WLAN Management System (WMS) process was busy and showed high CPU usage. This issue is resolved by changing the way the WMS process queues are handled. **Scenario:** This issue was observed when the same MAC address was reused between clients and their hosted soft-APs. This issue was observed in OAW-4306 Series switches running AOS-W 6.2.1.0. **Platform:** OAW-4306 Series switches. **Reported Version:** AOS-W 6.2.1.0.
106128	**Symptom:** The switch displayed incorrect properties for a valid AP when a rogue AP was spoofing it. The fix ensures that the switch does not allow a spoofing AP to change the properties of a valid AP. **Scenario:** A rouge AP sent spoofed probe response frames from a Virtual AP to a client. The switch allowed these spoofed frames to change the SSID and encryption type of the Virtual AP. This issue was observed in a master-local topology and was not limited to any specific switch model or AOS-W release version. **Platform:** All platforms. **Reported Version:** AOS-W 6.1.x-FIPS.

AirGroup

Table 57: *AirGroup Fixed Issues*

Bug ID	Description
89088 106999	**Symptom:** When a wired AirGroup user disconnected from the network, the AirGroup user entry persisted for many hours. This issue is resolved by clearing all disconnected wired AirGroup users. **Scenario:** This issue was observed in switches running AOS-W 6.3.x.x with wired AirGroup users. This issue was not limited to a specific switch model. **Platform:** All platforms. **Reported Version:** AOS-W 6.4.0.0.
106505	**Symptom:** A Switch used to send multiple authentication requests for AirGroup users to CPPM server when it did not receive a response from the CPPM server. This issue is resolved with internal code changes. **Scenario:** This issue was not limited to a specific switch model or AOS-W release version. **Platform:** All platforms. **Reported Version:** AOS-W 6.4.2.0.

AP-Platform

Table 58: *AP-Platform Fixed Issues*

Bug ID	Description
104186	**Symptom:** On the switch WebUI, the **Rx Frames to Me** parameter value was zero. The fix ensures that the WebUI shows the correct non-zero value when the AP's radio has clients associated to it. **Scenario:** This issue was specific to OAW-AP125 on switches running AOS-W 6.3.1.8. **Platform:** OAW-AP125. **Reported Version:** AOS-W 6.3.1.8.
104786 108566	**Symptom:** AP kernel crashed on DFS channel. The log indicated the reboot reason as **Kernel unaligned instruction access**. This issue is resolved with internal code changes. **Scenario:** This issue was observed with DFS channel in OAW-AP65 and OAW-AP70 connected to switches running AOS-W 6.3.1.6. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.6.
104520 104726 105296 105627 106396 107104 108006 101510 114050	**Symptom:** The status of an AP was displayed as UP on the local switch, but as DOWN on the master switch. The fix ensures that when there is no change in the value of the master switch IP, an update from the IKE module is rejected. **Scenario:** This issue was observed in OAW-S3 and OAW-4704 switches running AOS-W 6.3.1.5 in a master-standby-local topology. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.5.

AP-Regulatory

Table 59: *AP-Regulatory Fixed Issues*

Bug ID	Description
106949	**Symptom:** Mexico had all 5 GHz band channels as DFS channels. This issue is resolved by removing DFS functionality on channels 36 through 48 and 149 through 165 according to new regulatory standards. **Scenario:** This issue was observed in OAW-AP105 connected to switches running AOS-W 6.3.1.9. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.9.

AP-Wireless

Table 60: *AP-Wireless Fixed Issues*

Bug ID	Description
98692	**Symptom:** OAW-AP220 Series access points stopped responding and rebooted. The log files for the event listed the reason for the crash as **kernel panic: Fatal exception**. This issue is resolved with internal code changes. **Scenario:** This issue was observed in OAW-AP220 Series access points connected to OAW-4550 switches running AOS-W 6.4.0.2 in a master-local topology where the APs terminate on both the switches in campus mode. **Platform:** OAW-AP220 Series. **Reported Version:** AOS-W 6.4.0.2.
105613	**Symptom:** Intermittent connectivity problem occurred between clients and OAW-AP225. This issue is resolved with internal code changes. **Scenario:** This issue was observed between clients like Vocera badge and OAW-AP225 using 2.4 GHz radio. **Platform:** OAW-AP225. **Reported Version:** AOS-W 6.3.1.6.
106540	**Symptom:** Driver log showed low tx power for OAW-AP105. This issue is resolved by correcting the algorithm to get the tx power after the first beacon. **Scenario:** This issue was observed in OAW-AP105 connected to switches running AOS-W 6.3.1.9. **Platform**: OAW-AP105. **Reported Version**: AOS-W 6.3.1.9.
106285	**Symptom:** Packets were sent at 40 MHz rate even though 40 MHz was disabled in SSID profile. This issue is resolved by initializing the rate based on BSS configuration instead of initializing the rate based on radio configuration. **Scenario:** This issue was observed when 40 MHz was disabled in SSID profile of OAW-AP225 devices connected to switches running AOS-W 6.3.1.9. **Platform**: All Broadcom based devices including OAW-AP225. **Reported Version**: AOS-W 6.3.1.9.

Base OS Security

Table 61: *Base OS Security Fixed Issues*

Bug ID	Description
100248 103007 107117	**Symptom:** The authentication module crashed in a OAW-4550 switch. This issue is resolved by denying access to a wired user with zero MAC address and by adding logs and error statistic counters to identify occurrences of such crashes. **Scenario:** This issue was observed in a network where the RAP and a wired user were on the same switch. This issue was observed in OAW-4550 switches running AOS-W 6.4.0.3. **Platform:** OAW-4550 switch. **Reported Version:** AOS-W 6.4.0.3.

Switch-Datapath

Table 62: *Switch-Datapath Fixed Issues*

Bug ID	Description
101587 104272 104273 104505	**Symptom:** A switch rebooted and crashed while reassembling the fragments received from a mesh AP. Changes to the recursive IP packet assembly resolved this issue. **Scenario:** This issue occurred due to a misconfiguration between a switch running AOS-W 6.3.1.5 and the mesh AP. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.5.

Switch-Platform

Table 63: *Switch-Platform Fixed Issues*

Bug ID	Description
95071 95444 97548 97835 98115 98262 104276 107166 107964	**Symptom:** When a show command was executed in a standby switch, **Module Configuration Manager is busy** error message was displayed. This issue is resolved by making code level changes to prevent deadlock scenarios between processes that access the database. **Scenario:** This issue was observed in a OAW-4704 switch running AOS-W 6.3.1.1 in a master-local topology. **Platform:** OAW-4704 switches. **Reported Version:** AOS-W 6.3.1.1.
104932 103416 106115 106630 106868 107052 107273 107283 107874 107996 108033 108224 108256 110067	**Symptom:** A switch stopped responding and there was no entry made in the log file. This issue is resolved by implementing internal code changes. **Scenario:** This issue was observed in OAW-4704 switches running AOS-W 6.3.1.9. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.9.
106426 106314 106771	**Symptom:** A master switch was slow and did not respond to some output commands. Processes such as CFGM, STM, and WMS stopped responding. This issue is caused by low memory on the switch and is fixed by restricting one of the WMS databases from exceeding the threshold. **Scenario:** This issue was observed in switches running AOS-W 6.3.x and 6.4.x. This issue was not limited to a specific switch model and was observed in a master-local topology. **Platform**: All platforms. **Reported Version**: AOS-W 6.3.1.8.

Remote AP

Table 64: *Remote AP Fixed Issues*

Bug ID	Description
103850	**Symptom:** A Huawei E160 USB modem was not functional because it lost synchronization with the RAP. This issue is resolved by making code level changes to delay the modem boot-up process. **Scenario:** This issue was observed in switches running AOS-W 6.4.1. This issue was not limited to a specific switch model and was observed in a master-local topology where OAW-RAP109 terminated on both the switches in RAP mode.
104045 105730	**Symptom:** When the link between the switch and the AP was disconnected, clients associated with back-up Virtual APs, but did not get an IP address through DHCP. This fix ensures that the clients can connect to the AP, get an IP address, and send traffic. **Scenario:** This issue was not limited to any specific switch, AP model, or AOS-W release version. **Platform:** All platforms. **Reported Version:** AOS-W 6.4.2.0.

Routing

Table 65: *Routing Fixed Issues*

Bug ID	Description
94746	**Symptom:** When the loopback IP address was used as the IP address of a switch, the switch was not reachable from a wired network after reboot. The switch was reachable only from the same subnet to which the uplink of the switch belonged to. This issue is resolved by implementing internal code changes. **Scenario:** This issue was observed when two threads in an internal process tried to modify the kernel default route information and lost the sequence of execution. This issue was seen in OAW-4550/4650/4750 Series switches running AOS-W 6.3.1.0. **Platform:** OAW-4550/4650/4750 Series switches. **Reported Version:** AOS-W 6.3.1.0.

WebUI

Table 66: *WebUI Fixed Issues*

Bug ID	Description
101933	**Symptom:** An error occurred when a user tried to open the WebUI with Fully Qualified Domain Name (FQDN) or IP address in the compatibility view of Internet Explorer 9 or higher version. This issue is resolved by overriding the compatibility mode. The page loads in the standard mode. **Scenario:** This issue was observed in switches running AOS-W 6.3.1.5 or higher version. This issue was not limited to any specific switch model. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.5.
101989	**Symptom:** The status of an AP was displayed as inactive when the user tried to view the client activity in the **Monitoring** tab of the switch WebUI. This issue is resolved by implementing internal code changes. **Scenario:** This issue was observed in OAW-4604 switches running AOS-W 6.2.1.x. and 6.3.1.x. **Platform:** OAW-4604 switches. **Reported Version:** AOS-W 6.3.1.6.
102077 106193	**Symptom:** The **Script error in browser** message was displayed in the **Configuration** > **Networks** > **Port** > **Port-channel** page of the switch WebUI when the switch did not have a PEF license. This issue is resolved by implementing internal code changes.

Table 66: *WebUI Fixed Issues*

Bug ID	Description
	Scenario: This issue was observed in OAW-4550/4650/4750 Series switches without PEF license running any version of AOS-W. **Platform:** OAW-4550/4650/4750 Series switches. **Reported Version:** AOS-W 6.4.3.0.

Resolved Issues in AOS-W 6.3.1.11

The following issues are resolved in AOS-W 6.3.1.11.

Activate

Table 67: *Activate Fixed Issues*

Bug ID	Description
105345	**Symptom:** When the active whitelist feature was enabled and the switch downloaded the whitelist from the Active Server, the customer's account credentials were logged in the active logs. These logs were enabled only when the logging level was set to debugging. The fix ensures that the logs retrieving the activate HTTP message content is removed. **Scenario:** This issue was observed in switches running AOS-W 6.3 and later versions. **Platform:** All platforms. **Reported Version:** AOS-W 6.4.1.0.

Air Management - IDS

Table 68: *Air Management - IDS Fixed Issues*

Bug ID	Description
89705	**Symptom:** Log messages on the switch displayed an incorrect warning message about a TKIP DoS attack from a valid client. This issue is resolved with internal code changes. **Scenario:** The current TKIP attack detection code incorrectly identified certain types of (normal) packet exchanges as a TKIP DoS attack. This issue was observed in a master-local topology and occurred on all switches running AOS-W 6.x. **Platform:** All platforms. **Reported Version:** AOS-W 6.1.3.8.
106242	**Symptom:** The initial RSSI (Received Signal Strength Indication) value was incorrect for some wireless client entries in the AP. While creating the client entry, the AP checks if the frame was sent by the client device. If not, the switch does not update the RSSI value, and it remains unset until a frame was seen from the client device. This check resolved the issue. **Scenario:** This issue occurred only when an AP2STA (AP to station) frame was used to create the client entry. Though this frame was not initiated from the wireless client, the AP incorrectly used the RSSI from this frame to set the RSSI value for the wireless client. This issue was not limited to any specific switch model or AOS-W release version. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.0.0.

AP-Platform

Table 69: *AP-Platform Fixed Issues*

Bug ID	Description
105120	**Symptom:** An AP provisioned with LMS and backup-LMS in an AP system profile initially terminated on primary LMS. When the switch was rebooted, the AP did not re-associate with the primary switch until the AP was manually rebooted. This issue is resolved by changing the processing configuration. **Scenario:** This issue was observed in a setup where: • Both LMS and backup-LMS existed in an AP system profile. • An AP received at least three different LMS IPs during reboot. In this case, the first IP was the master switch IP, the second IP was the server IP, and the third IP was the DNS resolution of Alcatel-Lucent-master switch. • CPSEC was enabled with RAP included. This issue was triggered when the number of LMS IPs were set incorrectly and more than two IPs were received. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.5.
105529	**Symptom:** When the AP restarted, the Enet1 port was used as the new active uplink so the AP did not reboot. This issue is fixed by ensuring that the Enet0 port is used as the primary active link. **Scenario:** This issue was observed in OAW-AP224/OAW-AP225 when the Enet1 port was connected to a laptop or a projector and the AP was using static IP address. **Platform:** OAW-AP224/OAW-AP225. **Reported Version:** AOS-W 6.3.1.9.

AP-Wireless

Table 70: *AP-Wireless Fixed Issues*

Bug ID	Description
97709 103855 106485 106681 107161	**Symptom:** Multiple APs rebooted unexpectedly on switches. Internal code changes in the wireless driver fixed this issue. **Scenario:** This issue was observed in switches running AOS-W 6.3.1.8. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.8.
104447	**Symptom:** In OAW-AP224/OAW-AP225, the transmit power was fluctuating in the 3 db range. This issue is resolved by using hardware saved power index instead of using pre-defined power index in the closed loop algorithm. **Scenario:** This issue was observed in OAW-AP224/OAW-AP225 when pre-defined power index was inconsistent with different units. **Platform:** OAW-AP224/OAW-AP225. **Reported Version:** AOS-W 6.3.1.8.
105528	**Symptom:** Dell laptop did not connect to OAW-AP225 and Extensible Authentication Protocol (EAP) exchange failed. This issue is resolved by fixing the capability in beacon when High Throughput (HT) is disabled. **Scenario:** This issue was observed in OAW-AP225 connected to switches running AOS-W 6.3.1.5. **Platform:** OAW-AP225. **Reported Version:** AOS-W 6.3.1.5.

Authentication

Table 71: *Authentication Fixed Issues*

Bug ID	Description
101664	**Symptom:** On reboot, management user account created for Cert-based GUI access was deleted. This issue is fixed by storing the username with quotes. **Scenario:** This issue was observed when the management user account created for cert based GUI access contained a space in the username. **Platform:** All platforms. **Reported Version:** AOS-W 6.1.4.7.

Base OS Security

Table 72: *Base OS Security Fixed Issues*

Bug ID	Description
96950	**Symptom:** The switch stopped sending authorization packets to the radius server due to sequence number leak. This issue is resolved by implementing internal code changes. **Scenario:** This issue was observed in OAW-4750 and OAW-40xx Series switches running AOS-W 6.3.1.5 or later versions, when the **accounting** parameter was enabled and client 802.1X authentication increased suddenly. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.5.
105418	**Symptom:** A flaw in the OpenSSL SSL/TLS server caused a forced downgrade to TLS 1.0 even if both the server and client supported a higher protocol version. This issue is resolved by implementing internal code changes. **Scenario:** This issue was observed in switches running AOS-W 6.4.0.0. **Platform:** All platforms. **Reported Version:** AOS-W 6.4.0.0.
105705	**Symptom:** Invalid station entries were created when **aaa user add** command was executed to change a user role on the switch. The fix reduces the number of invalid station entries on the switch. **Scenario:** This issue was observed in OAW-S3 switch running AOS-W 6.3.1.7, when the **show station-table** command was executed or the maximum user capacity was reached due to invalid station entries. **Platform:** OAW-S3 switches. **Reported Version:** AOS-W 6.3.1.7.
105873	**Symptom:** There was a memory leak in the Authentication module while sending out radius accounting start. This issue is resolved by freeing the memory in the authentication module. **Scenario:** This issue was observed in OAW-S3 switch running AOS-W 6.1.3.2. **Platform:** All platforms. **Reported Version:** AOS-W 6.1.3.2.
105952	**Symptom:** After the switch rebooted, the AAA user derivation rule name that was configured with spaces was missing from the current configuration. This issue is resolved by addressing the space in the profile name. **Scenario:** This issue was observed in AOS-W 6.3.1.5 and earlier versions. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.5.
106066 106572	**Symptom:** Authentication module crashed in OAW-4750 switch. This issue is resolved by implementing internal code changes. **Scenario:** This issue was observed in OAW-4750 switch running AOS-W 6.3.1.5. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.5.

Configuration

Table 73: *Configuration Fixed Issues*

Bug ID	Description
103740	**Symptom:** Executing the **show dot1x supplicant-info pmkid** command did not display the correct Pairwise Master Key Identifier (PMKID). Internal code changes ensure that the correct PMKID is displayed. **Scenario:** This issue occurred when the user performed a 802.1X authentication. This issue was observed in switches running AOS-W 6.4 and earlier versions. **Platform:** All platforms. **Reported Version:** AOS-W 6.2.1.3.

Switch-Platform

Table 74: *Switch-Platform Fixed Issues*

Bug ID	Description
102443 102930 103736 103798 103968 104828 105499 106615	**Symptom:** In a master-local topology, the kernel module crashed. This issue is resolved by fixing the watchdog respawn feature. **Scenario:** This issue was observed in OAW-4750 switches running AOS-W 6.4.0.2 when the watchdog process failed. **Platform:** All platforms. **Reported Version:** AOS-W 6.4.0.2.
102943 105329 105905 106616 111585	**Symptom:** A master switch rebooted and remained in cpboot state. The log files for the event listed the reason as **Hardwatchdog reset**. This issue is resolved by implementing internal code changes. **Scenario:** This issue was observed in OAW-4x04 Series and OAW-S3 switches running AOS-W 6.3.1.5 and later versions. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.5.

Remote AP

Table 75: *Remote AP Fixed Issues*

Bug ID	Description
105024	**Symptom:** When the RAPs uplink IP address was set in 192.168.11.x range and was not rebooted, the RAP disconnected from the network. This issue is resolved by implementing internal code changes. **Scenario:** This issue was observed when the RAP was upgraded to AOS-W 6.3.1.2. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.2.
105751	**Symptom:** On a cellular link with same parameters, the Huawei K4605 modem associated with OAW-RAP109 but did not associate with OAW-RAP155. This issue is resolved by modifying the **USB modeswitch** parameter. **Scenario:** This issue was observed in OAW-RAP155 but not limited to any AOS-W version. **Platform:** OAW-RAP155 **Reported Version:** AOS-W 6.3.1.9.

Role/VLAN Derivation

Table 76: *Role/VLAN Derivation Fixed Issues*

Bug ID	Description
81889 103231	**Symptom:** The switch displayed an error message **Incompatible with other settings** when mapping a Server Derived Role (with named VLAN) to a **dot1x-server-group** of a AAA profile. Removing the validation check for server group allows the mapping of a Server Derived Role (with named VLAN) to a **dot1x-server-group** of a AAA profile. **Scenario:** The server group validation checked if the named VLAN had an associated VLAN ID. In this case, the named VLAN did not have a valid VLAN ID. VLAN IDs are local to each switch whereas VLAN name is synchronized from master to local switch. Assignment of VLAN IDs to VLAN name happens locally at each switch. The switch did not allow to configure a **dot1x-server-group** in AAA profile if the server group contained VLAN derivation rules based on named VLAN which did not map to any VLAN ID. This issue was observed in switches running AOS-W 6.3.x in a master-local topology. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.

Station Management

Table 77: *Station Management Fixed Issues*

Bug ID	Description
104639	**Symptom:** Wireless clients unexpectedly failed to be in 802.11r enabled WLAN. The clients failed because the station management process crashed on the AP. Changes in the internal code of the station management module ensures clients work seamlessly in a 802.11r enabled WLAN. **Scenario:** This issue was observed when an 802.11r-capable wireless client roams from one AP to another with the same or different ESSID. In addition, this issue lasted until the client manually switched to another ESSID. This issue was observed in switches running AOS-W 6.3.1.8 or later versions. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.9.
106411	**Symptom:** The station management module on a local switch crashed and caused all APs to failover to the master switch. This issue is resolved by checking for the null pointer before accessing it. **Scenario:** This issue was observed when the null pointer was accessed in a master-local topology. This issue was not limited to any specific switch model or AOS-W release version. **Platform:** All RAPs and APs with multiple Ethernet ports. **Reported Version:** AOS-W 6.3.1.5.

VRRP

Table 78: *VRRP Fixed Issues*

Bug ID	Description
103093	**Symptom:** Though Virtual Router Redundancy Protocol (VRRP) preemption was disabled on the switches, the actual master switch did not remain as standby after it came up. The fix ensures that the actual master switch waits for the correct master rollover time calculation before assuming the role of the master switch again. **Scenario:** This issue was observed in OAW-4550 switches when a master switch rebooted and took the role of the master switch instead of remaining in the standby role. This issue occurred due to wrong timing calculation on **Higher priority Standby**. **Platform:** All platforms. **Reported Version:** AOS-W 6.4.0.2.

Resolved Issues in AOS-W 6.3.1.10

The following issues are resolved in AOS-W 6.3.1.10.

Air Management-IDS

Table 79: *Air Management-IDS Fixed Issues*

Bug ID	Description
102715	**Symptom:** Ekahau/RTLS server did not parse tag frames forwarded to the server from OAW-AP225. This issue is resolved by adding extra two bytes of padding in the forwarded frame, which the server expects. The padding is added by default, but it can be configured in AP system profile. **Scenario:** This issue can be observed when using tag forwarding to Ekahau/RTLS servers from OAW-AP225 connected to switches running AOS-W 6.3.0.0 or later. The issue does not affect Aeroscout tag forwarding. **Platform:** OAW-AP225. **Reported Version:** AOS-W 6.4.0.3.

AP-Platform

Table 80: *AP-Platform Fixed Issues*

Bug ID	Description
102260	**Symptom:** Although multiple Virtual Access Points (VAPs) were enabled, only one VAP could be configured. This issue is resolved by making code level changes to the VAP configuration. **Scenario:** This issue was observed when multiple VAPs were enabled on a single radio. This issue was observed when the `show ap debug received-config` command was executed. **Platform:** OAW-AP220 Series. **Reported Version:** AOS-W 6.3.1.7.
103362	**Symptom:** All active APs on a local switch displayed the status as down on master switch. Fixing the LMS list processing in the Station Management (STM) process for restart cases resolved this issue. **Scenario:** After an STM restart, the LMS list for the master switch was not updated in STM. This issue was observed in master-local topology. This issue was not limited to any specific switch model and was observed in switches running AOS-W 6.4.1.0 or 6.3.1.8. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.8.

AP-Wireless

Table 81: *AP-Wireless Fixed Issues*

Bug ID	Description
98613 104755	**Symptom:** OAW-AP225 beacons did not go out or went out intermittently in 5 GHz or 2.4 GHz radio. Hence, a client cannot connect to OAW-AP225 in RAP bridge mode and the association failed with error message **Associating to Unknown AP**. This issue is resolved by making internal code changes. **Scenario:** This issue was observed in OAW-AP225 connected to switches running AOS-W 6.3.1.6. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.6.
100251	**Symptom:** An AP rebooted with error **unhandled kernel unaligned access**. Internal code changes in the Linux kernel fixed this issue. **Scenario:** This issue was observed in OAW-AP125 connected to switch running AOS-W 6.3.1.5. **Platform:** OAW-AP125 **Reported Version:** AOS-W 6.3.1.5.

Base OS Security

Table 82: *Base OS Security Fixed Issues*

Bug ID	Description
102632	**Symptom:** EAP-TLS termination displayed error **certificate verification failed** when switch was upgraded from AOS-W 6.1 to AOS-W 6.3. Changes in the certificate verification to support partial chain fixed this issue. **Scenario:** This issue was observed when the CA-certificate that was used for verification did not have the full chain to the Root CA. This issue was observed when the switch was configured with EAP-TLS termination running AOS-W 6.2 or later. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.7.
103227 103355	**Symptom:** The **ssh mgmt-auth public-key** parameter was disabled on the master switch but was not synchronized on the local switch when the value in the **cfg sync-type** command was set as **complete**. This issue is resolved by including **no ssh mgmt-auth public-key** in the running-config when the **ssh mgmt-auth public-key** parameter is disabled. **Scenario:** This issue occurred in a master-local setup due to the absence of a trigger on the local switch to delete **ssh mgmt-auth public-key**. This issue was not limited to any specific switch or release version. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.7

Switch-Datapath

Table 83: *Local Database Fixed Issues*

Bug ID	Description
103223	**Symptom:** When **netservice** command with end port 65535 (0xffff) was executed followed by execution of **no netservice** command, infinite loop of deletion **netservice** command occurred and the switch rebooted. This issue is resolved with internal code changes. Do not use end port value 65535 (0xffff) for **netservice** command. **Scenario:** This issue was observed when **netservice** or **no netservice** commands were executed with end port value as 65535. This issue was observed in switches running AOS-W 6.3.x and later. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.6.

Switch-Platform

Table 84: *Switch-Platform Fixed Issues*

Bug ID	Description
95993 105502 106959	**Symptom:** Firewall visibility process crashed on a local switch. The process restarts and recovers on its own. **Scenario:** This issue was observed after a switch was running for a long duration, possibly due to overflow of an internal data structure. This issue was not limited to any specific switch model or release version. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.1.
101003	**Symptom:** Centralized image upgrade over TFTP did not work if the image file was in sub-directory. Centralized upgrade over TFTP worked if the image file was in root directory. Changes in the internal code fixed this issue. **NOTE:** The present implementation does not support absolute path. The TFTP server typically runs in sandbox. Only relative path is supported. **Scenario:** The download function ignored the file-path in case of download from a TFTP server. This issue was not limited to any specific switch model or AOS-W release version. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.0.2.
103937	**Symptom:** Establishing an SSH session to switch failed randomly with error message **ssh_exchange_identification: Connection closed by remote host**. SSH sessions were either stale or notty, where an SSH session did not exist but the underlying TCP connection existed. This issue is resolved by: • Performing graceful log out for all SSH sessions whose terminal was closed earlier without logging out. This clears notty sessions. • Setting the parameter **ClientAliveCountMax** to 7200 and parameter **ClientAliveInterval** to 0, which terminates SSH sessions that are idle for 7200 seconds (2 hours) on the switch without killing the respective process from the shell. Disable keep alive on the SSH client so that the channel remains idle during inactivity **Scenario:** This issue was observed because of stale SSH processes (with notty) which were unresponsive for a long duration. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.8.

HA-Lite

Table 85: *HA-Lite Fixed Issues*

Bug ID	Description
86715	**Symptom:** Users are unable to re-provision an AP through the master switch's CLI or UI. Internal code changes ensure that all provisioning and apboot requests are forwarded to the Local Management Switch (LMS) of the local switch. **Scenario:** This issue was observed when High Availability (HA) is enabled and the master switch is configured as the HA-standby. This issue was observed in switches running AOS-W 6.3.1.8. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.8.

Local Database

Table 86: *Local Database Fixed Issues*

Bug ID	Description
104157	**Symptom:** A switch crashed due to lack of flash space. This issue is resolved by setting size limit on log files stored in the flash memory of the switch. **Scenario:** This issue was observed when log files occupied most of the flash space due to multiple crashes in the database server. This issue was not limited to any specific switch model or release version. **Platform:** All platforms. **Reported Version:** AOS-W 6.4.0.3.

LLDP

Table 87: *LLDP Fixed Issues*

Bug ID	Description
103548	**Symptom:** LLDP packets were sent on boot and prior to configuration push. This issue is fixed by not sending LLDP TLVs when AP boots, sending three mandatory TLVs (chassis subtype, port subtype and TTL) and one AOS-W TLV on boot, and sending the configured TLVs after the AP receives the configuration from the switch. **Scenario:** This issue was observed in switches running AOS-W versions prior to 6.4.2.0. **Platform:** All platforms. **Reported Version:** AOS-W 6.4.2.0.

Mobility

Table 88: *Mobility Fixed Issues*

Bug ID	Description
101517	**Symptom:** Switch sets the L3 mobility roaming state incorrectly as Home Switch/Foreign VLAN instead of Home Switch/Home VLAN when the user roamed between two SSIDs. This issue is resolved by stopping the association timer on the L3 mobility client. **Scenario:** This issue was observed when L3 mobility was enabled with a single WAN switch having two SSIDs, one SSID with L3 mobility enabled and another with L3 mobility disabled. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.5.

Remote AP

Table 89: *Remote AP Fixed Issues*

Bug ID	Description
105187	**Symptom:** When OAW-RAP155 was provisioned with 4G LTE UML295 USB modem, the Remote AP (RAP) did not come up as a cellular RAP. Adding support for 4G LTE UML295 USB modem on OAW-RAP155 fixed this issue. **Scenario:** This issue was observed in OAW-RAP155 running AOS-W 6.3.1.9. **Platform:** OAW-RAP155 **Reported Version:** AOS-W 6.3.1.9

Station Management

Table 90: *Station Management Fixed Issues*

Bug ID	Description
102035	**Symptom:** STM crashed in local switch. This issue is resolved by adding sanity checks to STA number. **Scenario:** This issue was observed in OAW-4550 switch in the master-standby topology when a corrupt or malformed packet had wrong STA number and STM used the number directly without checking the upper boundary. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.1.
102223	**Symptom:** When the **show ap association** command was executed, the association table listed invalid entries. These entries were not displayed when the **show user ap-name** and **show ap debug client-table-ap-name** commands were executed. The fix ensures that the **send_ageout** parameter is called when the new node is not created and a counter is added to track the old sap entry. **Scenario:** This issue was observed when there were a large number of mobile users. This issue was observed in OAW-AP92, OAW-AP105, OAW-AP125, and OAW-AP225 connected to OAW-4550 switches running AOS-W 6.3.1.7. **Platform:** OAW-AP92, OAW-AP105, OAW-AP125, and OAW-AP225 connected to OAW-4550 switches. **Reported Version:** AOS-W 6.3.1.7.
102241	**Symptom:** The Station Management (STM) module crashed on the master switch when the **ap wipe out flash** command was executed. This issue is resolved by relaying the correct message to the local switch. **Scenario:** This issue was observed if an AP was present on the local switch when the **ap wipe out flash** command was executed on the master switch running FIPS AOS-W version. This issue was observed only on switches running any version of FIPS AOS-W image and was not limited to any release version. **Platform:** All platforms. **Reported Version:** 6.1.x-FIPS
103452	**Symptom:** When a client previously associated with OAW-AP225 left, its record showed up in **show ap remote debug association** table and **show ap association** table. The stale record was not removed. This issue is resolved by implementing internal code changes. **Scenario:** This issue was observed in busy OAW-AP225 where many clients were connected. This issue was observed in OAW-AP225 connected to switches running AOS-W 6.4.0.2. **Platform:** OAW-AP225. **Reported Version:** AOS-W 6.4.0.2.

WebUI

Table 91: *WebUI Fixed Issues*

Bug ID	Description
96082	**Symptom:** The Received Signal Strength Indicator (RSSI) value of a client was displayed incorrectly in the **Client Monitoring** page of the WebUI in Chrome browser. This issue is resolved by making code level changes to ensure that the correct value is displayed on all browsers. **Scenario:** This issue was observed only when the WebUI of the switches running AOS-W 6.4 was opened in Chrome browser. **Platform:** All platforms. **Reported Version:** AOS-W 6.4.0.0.
100284	**Symptom:** The user had to enter the complete MAC address when querying a whitelist-db entry. Code level changes in the search API fixed this issue and the user can now use a partial MAC address. **Scenario:** This issue is observed in switches running AOS-W 6.3.1.6. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.6.
103384	**Symptom:** The user was unable to add port Access Control Lists (ACLs) using the WebUI. This issue was fixed by making changes to the port values. **Scenario:** This issue occurred if the minimum port value was more than the maximum port value and this issue is observed in OAW-4704 switches running AOS-W 6.3.1.5. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.5.

Resolved Issues in AOS-W 6.3.1.9

The following issues are resolved in AOS-W 6.3.1.9.

802.1X

Table 92: *802.1X Fixed Issues*

Bug ID	Description
103635	**Symptom:** When an 11r client with tunnel-mode roamed from one AP to other AP, the data traffic from the client stopped sometimes. This issue is resolved by setting a key at the switch datapath for 11r tunnel-mode stations. **Scenario:** This issue was observed when 11r clients, with tunnel forwarding mode enabled, roamed between APs. This issue was observed in switches running AOS-W 6.3.1.6. This issue was not limited to any specific switch model. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.6.

AP-Datapath

Table 93: *AP-Datapath Fixed Issues*

Bug ID	Description
99655	**Symptom:** Gratuitous ARP (GARP) triggered responses which caused station buffer overflow. This issue is resolved by making code level changes to GARP packets to avoid devices in a network from replying to the same request. **Scenario:** This issue was observed when a Gratuitous ARP was sent from a RAP to update the uplink switch/router MAC table. This caused devices in the same network to send ARP responses which lead to buffer overflow for the client. This issue was observed in OAW-AP105 connected to switches running AOS-W 6.2.1.5. **Platform:** OAW-AP105. **Reported Version:** AOS-W 6.2.1.5.

AP-Platform

Table 94: *AP-Platform Fixed Issues*

Bug ID	Description
95298 103161	**Symptom:** When an AP was configured with bridge mode VAP, it rebootstrapped many times after boot up. The AP wrongly received ICMP UNREACH notification for the bridge mode VAP from the switch. This issue is resolved by setting the VLAN to 1 for bridge mode VAP. **Scenario:** This issue was observed in switches running AOS-W version lower than 6.4. This issue was not limited to any specific switch model. **Platform:** All platforms. **Reported Version:** AOS-W 6.1.3.7.
96944	**Symptom:** When an AP and standby switch were on the same subnet, the IPSEC tunnel setup failed. This issue is resolved by not adding the host route when a master or standby switch is with an AP on the same subnet. **Scenario:** This issue was observed when an AP and standby switch were on the same subnet. This issue was observed in switches running AOS-W version 6.4 or lower. This issue was not limited to any specific switch model. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.3.
99548	**Symptom:** OAW-AP104, OAW-AP105, and OAW-AP175 rebooted unexpectedly. The log files for the event listed the reason for the reboot as **Ethernet crash due to throughput error**. This issue is resolved by adding debug information for Ethernet Rx, which checks if the skb memory is changed. **Scenario:** This issue is observed in OAW-AP104, OAW-AP105, and OAW-AP175 connected to switches running AOS-W 6.3.1.5. **Platform:** OAW-AP104, OAW-AP105, and OAW-AP175. **Reported Version:** AOS-W 6.3.1.5.

AP-Wireless

Table 95: *AP-Wireless Fixed Issues*

Bug ID	Description
99061 103160	**Symptom**: OAW-AP225 unexpectedly rebooted when Multi-VAPs were enabled. This issue is fixed by adding a lock to prevent the **asap_bw_mgmt_timer** timer from getting added twice. **Scenario**: This issue was observed when the timer, **asap_bw_mgmt_timer**, was getting added twice causing kernel crash. This issue was observed in OAW-4750 switches and OAW-AP225 running AOS-W 6.4.1.0 **Platform:** All platforms. **Reported Version:** AOS-W 6.4.1.0.
102631	**Symptom**: When running a downlink test with best effort (BE) traffic to one client and voice traffic to another client, the voice traffic dropped to 10-12 %. This issue is fixed by setting the packet size for the UDP test to 1260 bytes or enabling MTU discovery, and not limiting the MTU to 1500 bytes. **Scenario:** This issue occurred when significant packets dropped before reaching the wireless driver. This issue was observed in a Server - Switch - AP - Client topology with OAW-AP225 devices. **Platform:** OAW-AP220 Series. **Reported Version:** AOS-W 6.3.1.6

Base OS Security

Table 96: *Base OS Security Fixed Issues*

Bug ID	Description
98966	**Symptom:** When the MAC Authentication failed, the user was not placed in the initial role after re-authentication. This issue is fixed by sending a station-deauth to ensure that the client is put back into the initial role if L2-fail-through is not enabled and 802.1X is not configured during MAC Authentication failure. **Scenario:** This issue was observed when the MAC Authentication was run along with 802.1X re-authentication. This issue was not specific to any switch model or AOS-W version. **Platform:** All platforms. **Reported Version:** AOS-W 6.4.
99882	**Symptom:** The downlink packets to wpa-tkip clients randomly stopped on OAW-4550/4650/4750 Series switches. The fix ensures that issues related to support single replay counter with TKIP, which is independent of the WMM priority of the packet is addressed. **Scenario:** The issue was observed when a client used TKIP with WMM enabled. This lead to the locking of WMM queues which resulted in the client losing network connectivity. **Platform:** OAW-40xx Series and OAW-4550/4650/4750 Series. **Reported Version:** AOS-W 6.3.x
101269	**Symptom:** The output of **show rights <role>** command displayed only partial list of session ACLs. This issue is resolved by correcting the scanning function that fetches the output in batches. **Scenario:** This issue was observed when a large number of ACLs with large number of policies were configured under a role. This issue was observed in switches running AOS-W 6.3.1.4 or later. This issue was not limited to any specific switch model. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.5.

Table 96: *Base OS Security Fixed Issues*

Bug ID	Description
101594	**Symptom:** When **snmpwalk** is used to query the **nUser6Name** Object Identifier(OID), some addresses were not retrieved. Internal code changes ensures that the subsequent IPv6 address for the same station MAC on the switch is retrieved. **Scenario:** This issue was observed when there were consecutive IPv6 addresses for the same station MAC on the switch and subsequent IPv6 address was not retrieved. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.2.
102480	**Symptom:** When a wired user moved to a new port and VLAN, the port switched to the initial role and did not repeat L2 authentication. The fix ensures that the old user entries including the ipuser entries are deleted. **Scenario:** This issue was observed when a wireless user moved from one switch to another and the DMZ switch observed the user traffic from the second GRE tunnel. L2 authentication was not initiated because the VLAN was different. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.5.

Switch-Datapath

Table 97: *Switch-Datapath Fixed Issues*

Bug ID	Description
100922	**Symptom:** Accessing Microsoft® SharePoint using Microsoft Internet Explorer timed out. Correcting the TCP Maximum Segment Size (MSS) on the switch fixed the issue. **Scenario:** This issue was observed in switches running AOS-W 6.2 or later. This issue was not limited to any specific switch model. **Platform:** All platforms. **Reported Version:** AOS-W 6.2.1.5.
101392	**Symptom:** In a switch, user did not appear immediately in the user-table when connected. Traffic passed through only after the user appeared in the user-table. This issue is resolved by deleting the oldest 5% of total entries during devid_cache table full condition instead of deleting only one entry so that table-full condition is not reached for consecutive new users. **Scenario:** This issue was observed in OAW-4550/4650/4750 Series switches running AOS-W 6.3.1.3. This issue might be observed in earlier AOS-W releases too when the devid_cache table is full and new users (who are not present in the devid-cache) come in at approximately 10 users per second. This issue was not limited to any specific switch model, but the scenario is likely on OAW-4550/4650/4750 Series switches where the max-users is higher. Maximum devid_cache is twice the max-users and SQL sorting operations take longer along with the number of entries present. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.3

Switch-Platform

Table 98: *Switch-Platform Fixed Issues*

Bug ID	Description
102647 85289	**Symptom:** A switch rebooted unexpectedly. The log file for the event listed the reason as **Reboot Cause: kernel panic**. The fix ensures that the httpd process resumes immediately after crashing. **Scenario:** This issue was observed in OAW-4550/4650/4750 Series switch having a high density of IPv4 captive-portal users configured. This resulted in a high number of httpd processes running on the switch. This issue was observed in switches running AOS-W 6.2 or later versions. **Platform:** All platforms. **Reported Version:** AOS-W 6.2 and later versions.
102725 103483 103558	**Symptom:** The Fpapps module crashed and the switch rebooted. This issue is resolved by deleting a section of debug code that was not required. **Scenario:** This issue was caused due to the debug code added to fix bug 95129 and was observed on switches running AOS-W 6.3.1.7, 6.1.3.13, and 6.4.1.0. **Platform:** All platforms **Reported Version:** AOS-W 6.3.1.7 and later versions.

GRE

Table 99: *GRE Fixed Issues*

Bug ID	Description
103336	**Symptom:** Tunnel went down due to keep-alive failure. This issue is resolved by modifying the keep-alive process to avoid packet loss. **Scenario:** This issue was observed when the tunnel endpoints were not in the same VLAN as the uplink VLAN through which switches were connected. This issue was observed in switches running AOS-W 6.3.1.8 and was not limited to any specific switch model. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.8.

Licensing

Table 100: *Licensing Fixed Issues*

Bug ID	Description
101443 103325	**Symptom:** RAPs did not come up after upgrading from AOS-W 6.3.1.1 (or prior) to AOS-W 6.3.1.2 (or later). This issue is resolved by enabling the RAP feature if AP licenses exist. **Scenario:** This issue was observed when centralized licensing was enabled with RAPs and switches were upgraded from AOS-W 6.3.1.1 (or prior) to AOS-W 6.3.1.2 (or later). The RAP feature bit was enabled in the cached bitmap on switches running AOS-W 6.3.1.2 which caused the upgrade issue. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.2.

LLDP

Table 101: *LLDP Fixed Issues*

Bug ID	Description
102431	**Symptom:** When OAW-AP225 was connected to a switch with a long (more than 50 m) Ethernet cable, it always worked in restricted mode even though the switch secured 19 W power by LLDP. This issue is resolved by enforcing OAW-AP225 to work in unrestricted mode if switch can secure 19 W power by LLDP. **Scenario:** This issue was not limited to any specific switch model or release version. **Platform:** OAW-AP225 and OAW-AP224. **Reported Version:** AOS-W 6.3.1.4.

QoS

Table 102: *QoS Fixed Issues*

Bug ID	Description
103363	**Symptom:** When the DSCP value on outer GRE IP was not set, voice quality issue was observed with Vocera badges. This issue is resolved by copying the inner DSCP value to the outer DSCP field when packet is GRE encapsulated. **Scenario:** This issue was observed only when WEP was enabled and not for other encryption modes. This issue was not limited to any specific switch model. **Platform:** OAW-4550/4650/4750 Series switches. **Reported Version:** AOS-W 6.3.1.3.

Remote AP

Table 103: *Remote AP Fixed Issues*

Bug ID	Description
99635	**Symptom:** A Huawei E160 USB modem was not functional because it lost synchronization with the RAP. This issue is resolved by making code level changes to delay the modem boot-up process for E160. **Scenario:** This issue was observed when the RAP connected to the USB modem was hard rebooted. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.3.
101767	**Symptom:** The Huawei EC177 modem was not functional as it incorrectly executed script of another modem. This issue is resolved by scanning the modem twice to get the updated product ID (modem mode ID). **Scenario:** This issue was observed when the AP did not wait until the completion of mode-switch process for EC177. This resulted in the same product ID for both Huawei E392 and EC177. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.2.
102267	**Symptom: IAPMGR** process crashed. This issue is resolved by removing the assert statement in an erroneous condition. **Scenario:** This issue was observed on Switches running AOS-W 6.4 with OAW-IAPs in VPN configuration. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.5.

Role/VLAN Derivation

Table 104: *Role/VLAN Derivation Fixed Issues*

Bug ID	Description
103090	**Symptom:** In a network that has internal and DMZ switches and the internal switch tunnels packets from the clients through the L2 GRE tunnel to the DMZ switch, UDR rules were not applied when a user moved as a wired user over GRE tunnel from the internal switch to the DMZ switch. This issue is resolved with internal code changes. **Scenario:** This issue was observed when using L2 GRE tunnel to send the client traffic from internal switch to DMZ switch. This issue was observed on OAW-4704 Series switch running AOS-W 6.3.1.8. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.8.

TACACS

Table 105: *TACACS Fixed Issues*

Bug ID	Description
100762	**Symptom:** The customer was unable to delete a TACACS server group that was referenced but was taken out of the **AAA** profile. The fix ensures that the reference to the old server group is decremented. **Scenario:** This issue was observed in OAW-S3 switches running AOS-W 6.1.3.9. **Platform:** All platforms. **Reported Version:** AOS-W 6.1.3.9.

WebUI

Table 106: *WebUI Fixed Issues*

Bug ID	Description
96567	**Symptom:** Some UI links like Spectrum analysis were available only when a certain license was activated. However, the UI automatically checks for activated license when the switch boots up. So, if a license was activated when a switch was up, the UI would not get updated if a new license was already activated, and hence those UI links would not show until the switch rebooted. This issue is resolved by ensuring that the UI checks for activated license even without rebooting the switch, and accordingly update the UI links. **Scenario:** This issue was triggered by activation of license by central licensing without rebooting the local switch. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.0.
103187	**Symptom:** User was unable to create a guest user through GPP login by using capital letters in E-mail ID. This issue is resolved by allowing capital letters in E-mail address. **Scenario:** This issue was observed in switches running AOS-W 6.2.1.4. This issue was not limited to any specific switch model. **Platform:** All platforms. **Reported Version:** AOS-W 6.2.1.4.

Resolved Issues in AOS-W 6.3.1.8

The following issues are resolved in AOS-W 6.3.1.8.

AirGroup

Table 107: *AirGroup Fixed Issues*

Bug ID	Description
102063 102258 102877 104130	**Symptom:** The multicast **Domain Name System (mDNS)** process of AirGroup crashed and restarted in OAW-S3 switch. The logs for the event listed the reason for the crash as **Nanny rebooted machine - low on free memory**. Internal code changes are implemented to ensure the memory leak was removed. **Scenario:** A memory leak occurred every time the user sent a query and switch responded with the relevant mDNS records. This issue was observed in OAW-S3 switch running AOS-W 6.3.1.7. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.7.

Air Management-IDS

Table 108: *Air Management -IDS Fixed Issues*

Bug ID	Description
90630	**Symptom:** Log messages incorrectly warn of a Block ACK (BA) DoS attack from a valid client. Changes in the internal code has fixed this issue. **Scenario:** This issue was identified in a OAW-6000 switch running AOS-W 6.2.0.2 in a master-local topology. **Platform:** All platforms. **Reported Version:** AOS-W 6.2.0.2.

AP-Platform

Table 109: *AP-Platform Fixed Issues*

Bug ID	Description
98995	**Symptom:** OAW-AP70 crashed when scanning an unsupported channel. This issue is resolved by changing the channel in SG country code and not allowing OAW-AP70 to scan an unsupported channel. **Scenario:** This issue was observed in OAW-AP70 Series devices connected to a switch running AOS-W 6.2.1.3. **Platform:** All platforms. **Reported Version:** AOS-W 6.2.1.3.
99577	**Symptom:** OAW-AP125 unexpectedly crashed and rebooted. Log files for the event listed the reason for the crash as **kernel page fault at virtual address 0000000000000000**. This issue is resolved by making improvements to the wireless drivers. **Scenario:** This issue was observed in OAW-AP125 Series devices connected to a switch running AOS-W 6.3.1.5. **Platform:** OAW-AP125. **Reported Version:** AOS-W 6.3.1.5.

AP-Wireless

Table 110: *AP-Wireless Fixed Issues*

Bug ID	Description
102301	**Symptom**: OAW-AP225 rebooted unexpectedly. The log files listed the reason for the reboot as **Out of Memory error**. The fix ensures that the accounting error that causes AP reboot is addressed. **Scenario**: This issue was observed when UDP bidirectional traffic was sent using the **iperf** command, which resulted in an increase in traffic and RX queue. This issue was observed in OAW-AP225 connected to switches running AOS-W 6.3.1.7. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.7.

Base OS Security

Table 111: *Base OS Security Fixed Issues*

Bug ID	Description
87405	**Symptom:** Firewall policies were not enforced on certain client traffic when the clients were connected to a RAP in wired mode and configured with a static IP. This issue is resolved by ensuring that the sessions established with untrusted users are deleted and recreated to apply the firewall policies correctly. **Scenario:** This issue was observed when the traffic was initiated by a device or server connected to the switch with an idle client. This issue was not limited to any specific switch model or release version. **Platform:** All platforms. **Reported Version:** AOS-W 6.1.3.5.
93066	**Symptom:** The MAPC module on the crashed unexpectedly. The log files for the event listed the reason for the crash as **mapc segmentation fault**. Internal code changes in the MAPC module of the fixed this issue. **Scenario:** This issue is observed when IF-MAP is configured to communicate with ClearPass Policy Manager (CPPM). This issue is observed on switches running AOS-W 6.3 or later versions. **Platform:** OAW-4550 switches. **Reported Version:** AOS-W 6.3.1.0.
99123	**Symptom: Authentication** process crashed when authenticating a Captive portal user from an external XML-API server. The crash occurred when trying to access a NULL pointer. This issue is resolved by addressing a race condition and returning an error message if IP user entry is not found. **Scenario:** This issue was observed when users tried to connect to a RAP in split tunnel mode. This issue was not limited to any specific switch model or release version. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.4.
102259	**Symptom:** AOS-W was vulnerable to SSL/TLS Man-In-The-Middle (MITM) attack. This issue is resolved by implementing internal code changes **Scenario:** An attacker, using a carefully crafted handshake, forced the use of weak keying material in OpenSSL SSL/TLS clients and servers. This was exploited by a MITM attack where the attacker decrypted and modified traffic from the attacked client and server. The attack was performed only between a vulnerable client and server. All versions of OpenSSL clients are vulnerable. OpenSSL servers are only known to be vulnerable in OpenSSL version 1.0.1 and 1.0.2-beta1. **Platform:** All platforms. **Reported Version:** AOS-W 6.4.1.0.

Switch-Datapath

Table 112: *Switch-Datapath Fixed Issues*

Bug ID	Description
97223	**Symptom:** The L3 GRE tunnel between Alcatel-Lucent switch and a Cisco device was not restored when there was a keep-alive failure. The fix ensures that Alcatel-Lucent and Cisco uses the same protocol number in the GRE keep-alive packets. **Scenario:** This issue was observed when Alcatel-Lucent and Cisco used different protocol numbers in GRE keep-alive packets, and both the devices dropped the keepalive packets sent by the other as the protocol number was unknown. This issue was not limited to any specific switch model and was observed in AOS-W 6.3.1.2. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.2.

Switch-Platform

Table 113: *Switch-Platform Fixed Issues*

Bug ID	Description
95835 98034 98202 99342	**Symptom:** A switch stopped responding and rebooted. The log files for the event listed the reason as **softwatchdog reset**. This issue is resolved by removing the race conditions in the panic dump path and reimplementing the watchdog framework. **Scenario:** This issue was seen during datapath core dump. This issue was observed on OAW-40xx Series and OAW-4550/4650/4750 Series switches running AOS-W 6.3.1.2. **Platform:** OAW-40xx Series and OAW-4550/4650/4750 Series. **Reported Version:** AOS-W 6.3.1.2.
97816 98418 98419 98686 98688	**Symptom:** Local handling **Station Management (STM)** and **WLAN Management System (WMS)** processes crashed, with **0x01 exit status**. The fix ensures that during a specific table backup, the database does not get corrupted. **Scenario:** This issue occurred due to database table corruption. This issue was observed in switches running AOS-W 6.3 and 6.4. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.2.
99208 99210 99211 99212 99213	**Symptom:** A switch crashed due to memory leak in PIM after a long uptime (for example, 90 days). The fix ensures that there are no memory leaks in PIM module. **Scenario:** This issue was observed when IGMP snooping or proxy was enabled and users performed multicast streaming. This issue occurred when the user's DHCP pool range is too vast (more than 2 million addresses). This issue was not limited to any specific switch model or AOS-W version. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.2.
100679	**Symptom:** A OAW-4604 switch crashed and rebooted with hardware watchdog reset. This issue is resolved by serialization in die path for watchdog and panic and removal of cerr printk from path in panic. **Scenario:** This issue was observed in OAW-4504, OAW-4604, OAW-4704, OAW-4306, OAW-4306G, and OAW-S3 switches, but is not limited to any specific AOS-W version. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.6.

IPSec

Table 114: *IPSec Fixed Issues*

Bug ID	Description
102039	**Symptom:** During an Internet Key Exchange (IKE) negotiation, if an IPsec client proposed IPv4 and IPv6 traffic selector in the same message, the switch responded by sending an incorrect IPv4 traffic selector of 0.0.0.0 - 0.0.0.0. Internal code changes are implemented to ensure the correct IPv4 traffic selector is returned. **Scenario:** This issue was observed when an IPsec client proposed IPv6 traffic selectors along with IPv4 traffic selectors. This issue was not limited to any specific switch model or release version. **Platform:** All platforms. **Reported Version:** AOS-W 6.4.1.0.

LLDP

Table 115: *LLDP Fixed Issues*

Bug ID	Description
100439	**Symptom:** Clients were unable to disable the 802.3 TLV power in the AP LLDP configuration. This results in PoE allocation issue on the switches. The fix allows the customer to enable/disable the 802.3 power Type Length Value (TLV). **Scenario:** This issue was observed in OAW-4550 switches running AOS-W 6.2.1.5. **Platform:** All platforms. **Reported Version:** AOS-W 6.2.1.5.

Master-Local

Table 116: *Master -Local Fixed Issues*

Bug ID	Description
100526	**Symptom:** When the **aaa user fast-age** feature was enabled, all the existing ip-users were removed from the table. The fix ensures that existing ip users are not removed when **aaa user fast-age** is configured. **Scenario:** This issue was observed when **aaa user fast-age** feature was configured. This issue was not limited to any specific switch model and was observed in AOS-W 6.2 and above. **Platform:** All platforms. **Reported Version:** AOS-W 6.2.

Remote AP

Table 117: *Remote AP Fixed Issues*

Bug ID	Description
101526	**Symptom:** The Remote AP Authorization Profile feature was not functional when the RAP was upgraded from AOS-W 6.2.1.0 to AOS-W 6.3.1.6. This issue is resolved by changing the code to perform AP authorization against RAP whitelist instead of local-userdb-ap. **Scenario:** This issue was observed when the flag status of the RAPs did not change to Rc2 even after they were authorized by the Captive Portal user. As a result, the configuration download was incomplete. This issue was observed in AOS-W 6.3 and above. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.6.

Resolved Issues in AOS-W 6.3.1.7

The following issues are resolved in AOS-W 6.3.1.7.

Air Group

Table 118: *Air Group Fixed Issues*

Bug ID	Description
102063 102258	**Symptom:** The **multicast Domain Name System (mDNS)** process of AirGroup crashed and restarted in OAW-S3 switch. The logs for the event listed the reason for the crash as **Nanny rebooted machine - low on free memory**. Internal code changes are implemented to ensure the memory leak was removed. **Scenario:** A memory leak occurred every time the user sent a query and switch responded with the relevant mDNS records. This issue was observed in OAW-S3 switch running AOS-W 6.3.1.7. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.7.

Air Management-IDS

Table 119: *Air Management-IDS Fixed Issues*

Bug ID	Description
96206	**Symptom:** The WMS module periodically failed to respond when it removed monitored devices that were not in use. This issue is resolved by optimizing the WMS station check and AP removal process. **Scenario:** This issue occurred in large networks with many monitored devices, when the table size became large in the WMS module, and the WMS module failed to respond to the SNMP poll requests. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.2.

AP-Platform

Table 120: *AP-Platform Fixed Issues*

Bug ID	Description
95482	**Symptom:** BSS Tx/Rx Rate for a BSSID showed 1 Mbps for 802.11g radio even after disabling the 1 Mbps option in SSID profile. This issue was due to the incorrect display of the **show ap active ap-name** command. Issuing the same command now displays **N/A** for BSS Tx/Rx Rate parameters. **Scenario:** Issuing the **show ap active ap-name** command displayed BSS Tx/Rx Rate as 1 Mbps for 802.11g radio even after disabling the 1 Mbps option in SSID profile. This issue was not limited to any specific switch version or AOS-W release version. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.1.

AP-Regulatory

Table 121: *AP-Regulatory Fixed Issues*

Bug ID	Description
98628	**Symptom:** MaxEIRP for OAW-RAP3WN/ OAW-RAP3WNP was inconsistent due to wrong maximum tx-power setting. The fix ensures that the regulatory and hardware limits are correctly set and the MaxEIRP value is always greater than tx-power. **Scenario:** This issue was observed when the value of configured tx-power was larger than the MaxEIRP. **Platform:** OAW-RAP3WN and OAW-RAP3WNP. **Reported Version:** AOS-W 6.3.1.3.

AP-Wireless

Table 122: *AP-Wireless Fixed Issues*

Bug ID	Description
88940	**Symptom:** A crash was observed on APs when the status of the channel was set inappropriately by the process handling the AP management. This issue is resolved by selecting the first channel of the current 802.11 band, using the auto-channel option. **Scenario:** This issue was observed when a standard RAP or CAP was configured at the Dynamic Frequency Selection (DFS) channel. This issue is observed in OAW-AP70 connected to switches running AOS-W 6.3.1.2. **Platform:** All platforms. **Reported Version:** AOS-W 6.4.0.0.
94482 96677	**Symptom:** An AP crashed due to an internal Watchdog timeout. This issue is resolved by reducing the wait time, and rebooting the AP to recover from that state. **Scenario:** This issue occurred within one of the reset functions in the Ethernet driver where there was a long wait, which exceeded the watchdog timeout, causing AP failure. **Platform:** OAW-AP220 Series **Reported Version:** AOS-W 6.4.0.0.
99833 100559 100652	**Symptom:** When more than 120 customers were connected in the bridge mode, broadcast packets were dropped and customers lost connectivity. This fix ensures that the broadcast packet handling is modified to resolve the issue. **Scenario:** This issue was observed when the frequency of customers trying to connect to the APs was high. This issue was observed in OAW-AP225 connected to switches running AOS-W 6.3.1.2. **Platform:** OAW-AP225. **Reported Version:** AOS-W 6.3.1.2
99922	**Symptom:** OAW-AP220 Series access points displayed more than actual number of associated stations. When reclaiming the client data structures, there was inconsistency between driver and AP processes which is now resolved. **Scenario:** This issue was observed when the value of the parameter **max-clients** was set to 255 and the count of the associated and non-associated stations exceeded the maximum value. This issue was observed in OAW-AP220 Series access points connected to switches running AOS-W 6.3.x. **Platform:** OAW-AP220 Series. **Reported Version:** AOS-W 6.3.x

Table 122: *AP-Wireless Fixed Issues*

Bug ID	Description
85522 100352	**Symptom:** OAW-AP93/OAW-AP93H/OAW-AP92 crashed multiple times. The log files for the event listed the reason for the reboot as **Kernel unaligned instruction access**. To resolve this issue, changes are made to the radio reset routines. **Scenario:** The issue occurred due to memory corruption. This issue was observed in OAW-AP93/OAW-AP93H/OAW-AP92 connected to switches running AOS-W 6.3 and above. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.5.
100652 100731	**Symptom:** Some access points were not transmitting multicast streams. This issue is resolved by fixing the accounting problem. **Scenario:** This issue was observed when the counter used to track the buffered multicast frames was not decremented when invalid frames in the buffers were discarded. When the counter reached the maximum outstanding multicast frames, no more multicast frames were allowed for transmission. **Platform:** OAW-AP220 Series. **Reported Version:** AOS-W 6.3.1.5
101216	**Symptom**: Clients associated to encrypted SSID in d-tunnel mode but did not get IP address and AP did not respond to any command or apply configuration change. This issue is resolved by not displaying any output for command **show ap debug bandwidth-management**. **Scenario**: This issue was observed on an encrypted SSID in d-tunnel mode when command **show ap debug bandwidth-management** was executed or command **show ap tech-support** was executed which ran the bandwidth-management command. **Platform:** OAW-AP220 Series. **Reported Version:** AOS-W 6.3.1.5.

Base OS Security

Table 123: *Base OS Security Fixed Issues*

Bug ID	Description
98492	**Symptom:** When the customer moved from demilitarized zone (DMZ) to an internal switch, the display showed wireless instead of wired. This issue is resolved by checking the tunnel through which the user is connected and changing the user to wired. **Scenario:** This issue was observed when the customer routed traffic from an internal switch to DMZ using the L2 GRE Tunnel. This issue was observed in OAW-4704 switches running AOS-W 6.2.1.3. **Platform:** All platforms. **Reported Version:** AOS-W 6.2.1.3.
96980	**Symptom:** Customer faced connectivity issues with Pre-Shared Key (PSK), Mac Authentication, and VLAN Derivation as key1 packet was sent out twice. This issue is resolved by introducing serialized Mac Authentication and PSK. **Scenario:** This issue occurred when PSK and Mac Authentication were parallel processed, but PSK was initiated before MAC Authentication VLAN update. This issue was observed in AOS-W 6.3.1.1. **Platform:** OAW-AP105. **Reported Version:** AOS-W 6.3.1.1.

Configuration

Table 124: *Configuration Fixed Issues*

Bug ID	Description
95535 95582	**Symptom**: The ACL configuration on the local switch went out of sync intermittently with the master switch. The fix ensures that when centralized licensing is enabled and if PEFNG license is installed, the ACL configuration associated with the license is not be changed even if the PEFNG license is not available temporarily. **Scenario**: This issue occurred when there was a change in licenses. This issue was observed in switches running AOS-W 6.3 in a master-local topology. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.2.

Switch-Datapath

Table 125: *Switch-Datapath Fixed Issues*

Bug ID	Description
96349	**Symptom:** The DNS request for switch's domain name returned 0.0.0.0. This issue is resolved by fixing the race condition which populated the wrong IP in DNS response. **Scenario:** This issue was observed when the wrong IP was populated in DNS response, due to a race condition. This issue was observed in switches running AOS-W 6.3.1.2, and was not limited to any specific switch model. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.2.
96227	**Symptom:** APs dropped heartbeat messages to the switch, and the APs rebooted. This issue is resolved by introducing the **arp** and **grat-arp** parameters to drop or blacklist the clients that are including unnecessary ARP traffic. For more information on these parameters, see Commands Modified in AOS-W 6.3.1.7 on page 32. **Scenario:** This issue occurred due to large number of unnecessary ARP traffic and was observed on OAW-4550/4650/4750 Series switches running AOS-W 6.3.1.2 or later. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.2.
97434	**Symptom:** High volume of Address Resolution Protocol (ARPs) requests triggered an increase in datapath utilization, which resulted in service impact. This issue is resolved by introducing the **arp** and **grat-arp** parameters to drop or blacklist the clients that are sending excessive ARPs. For more information on these parameters, see Commands Modified in AOS-W 6.3.1.7 on page 32 **Scenario:** This issue was observed when a client excessively scanned and dropped the Internet Control Message Protocol (ICMP) packets. This issue was observed in a local OAW-S3 switch running AOS-W 6.3.1.3, in a master-local topology. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.3.
98499 100392 100393	**Symptom**: Switches crashed multiple times. The log files for the event listed the reason for the reboot as datapath exception. **Scenario**: When a wireless user generated encrypted wifi fragments, these were sent to the security engine for decryption, which returned results that were out-of-order and some of them had decryption errors. The fix ensures that the wifi fragments out-of-order decryption errors are handled correctly. **Platform**: OAW-4650 Series switches. **Reported Version**: AOS-W 6.3.1.3.
98500	**Symptom:** A legacy platform switch crashed when it received more than three Aggregated Mac Service Data Unit (A-MSDU) fragments. To resolve this issue, a check is introduced in the switch to drop the packets when more than three A-MSDU fragments were received.

Table 125: *Switch-Datapath Fixed Issues*

Bug ID	Description
	Scenario: This issue was observed when a wireless client sent aggregated A-MSDU packets to the AP which was further fragmented to more than three packets and sent to the switch. This issue was specific to legacy platform switches (OAW-6000 Series switches platforms with XLR/XLS processors and OAW-4306G switches) running AOS-W 6.3 and 6.4. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.3.
99483 106224	**Symptom:** When AMSDU-TX was enabled, one of the packets were incorrectly freed and another packets failed, which lead to double incarnation of the same buffer and the system crashed. The fix ensures that the buffers are freed correctly. **Scenario:** This issue was observed in switches running AOS-W 6.3 or later, and was not limited to any specific switch model. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.3.
100084	**Symptom:** Unknown ARP (ARP without user entry in datapath) requests were flooded in RAP wired tunnels. This issue is resolved by changing the behavior of the unknown ARPs from flooding in RAP wired tunnels. **Scenario:** This issue was observed in all switches running AOS-W 6.3.1.6 or later. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.6
101010	**Symptom:** When both DMO and broadcast-filter-all were enabled and port-channel was used for uplink port, incoming known multicast traffic from uplink got dropped in the switch. This issue is resolved by changing the multicast forwarding logic. **Scenario:** This issue was observed in switches running AOS-W 6.3.x.0 and 6.4.x.0. **Platform:** All platforms. **Reported Version:** AOS-W 6.4.0.2.

Switch-Platform

Table 126: *Switch-Platform Fixed Issues*

Bug ID	Description
76059 85289 92255 93467 93827 95431 96293 96791 96827 98196 99287 99360 99362 99472 99568 100857 100858	**Symptom:** A switch rebooted unexpectedly. The log files for the event listed the reason as **Reboot Cause: kernel panic**. The fix ensures that the **httpd** process resumes immediately after crashing. **Scenario:** This issue was seen in OAW-4550/4650/4750 Series switch having a high density of IPv4 captive-portal users configured. This resulted in a high number of **httpd** processes running on the switch. This issue was observed in AOS-W 6.2 or later versions. **Platform:** OAW-4550/4650/4750 Series. **Reported Version:** AOS-W 6.2.
94427 96347 97456 97468 97938 98425 98656 99448 99814	**Symptom:** OAW-S3 switch rebooted unexpectedly. The log files for the event listed the reason for the reboot as **User pushed reset** error. The issue is resolved by removing the lock contention. **Scenario:** This issue was observed due to panic dump or SOS crash, which was a result of jumbo packet or packet corruption. This issue was observed in OAW-S3, OAW-4504, OAW-4604, and OAW-4704 switches, but was not limited to any specific AOS-W release version. **Platform:** All platforms. **Reported Version:** AOS-W 6.1.3.5.
96819	**Symptom:** Unable to transfer files using SCP to or from a switch on MAC devices. The fix ensures that the SCP copy operation is successful. **Scenario:** This issue is not limited to any specific switch model or AOS-W version. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.2.
98873 100421	**Symptom:** A OAW-4306G switch crashed during reboot. The log files for the event listed the reason as **address error on CPU4**. This issue is resolved by reverting the sos_download sequence in rcS script. **Scenario:** This issue was observed on OAW-4306G switches running AOS-W 6.2.1.5. **Platform:** All platforms. **Reported Version:** AOS-W 6.2.1.5.
99106	**Symptom:** A large number of **Only Bottom slots can arbitrate** debug messages were generated and as a result the switch console was flooded with these redundant messages. The issue is fixed by disabling these redundant messages in the arbitration algorithm. **Scenario:** This issue was observed in OAW-S3 switches and is not limited to any AOS-W version. **Platform:** All platforms. **Reported Version:** AOS-W 6.1.3.4.

DHCP

Table 127: *DHCP Fixed Issues*

Bug ID	Description
92438 100213	**Symptom:** Dynamic Host Configuration Protocol (DHCP) logs were displayed even when the DHCP debug logs were not configured. The fix ensures that the DHCP logs are printed only when the debug log is configured. This issue is resolved by changing the DHCP debug log configuration. **Scenario:** This issue was observed on switches running AOS-W 6.2 or later. **Platform:** All platforms. **Reported Version:** AOS-W 6.2.1.3.

IPSec

Table 128: *IPSec Fixed Issues*

Bug ID	Description
97775 100139	**Symptom:** If a user entered a wrong password, the VIA application did not prompt thrice for a password retry. This issue is resolved by sending the **XAUTH STATUS FAIL** message to the VIA client before deleting the IKE/IPSec session of the VIA client. **Scenario:** This issue was observed in switches running AOS-W 6.2, 6.3, or 6.4. The issue was caused when the switch did not send **XAUTH STATUS FAIL** to the VIA client. **Platform:** All platforms. **Reported Version:** AOS-W 6.1.3.2.
99675	**Symptom: ISAKMPD** process crashed on master switch when maximum number of RAP limit was reached and a new user had to be added. This issue is resolved by reworking the debug infra code to remove the tight loop. **Scenario:** This issue was observed when more than 2 supported RAPS terminated on a switch. This resulted in **ISAKMPD** process sitting in a tight loop. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.4.
102039	**Symptom:** During an Internet Key Exchange (IKE) negotiation, if an IPsec client proposed IPv4 and IPv6 traffic selector in the same message, the switch responded by sending an incorrect IPv4 traffic selector of 0.0.0.0 - 0.0.0.0. Internal code changes are implemented to ensure the correct IPv4 traffic selector is returned. **Scenario:** This issue was observed when an IPsec client proposed IPv6 traffic selectors along with IPv4 traffic selectors. This issue was not limited to any specific switch model or release version. **Platform:** All platforms. **Reported Version:** AOS-W 6.4.1.0.

Master-Redundancy

Table 129: *Master-Redundancy Fixed Issues*

Bug ID	Description
98663	**Symptom:** Error messages were displayed when database synchronization was taking place in OAW-4306 Series switches. This issue is resolved by removing support for **iapmgr**. **Scenario:** This issue was observed in OAW-4306 Series switches. The issues is caused when the user upgrades to AOS-W 6.3 and executes the **write erase all** command. **Platform:** All platforms. **Reported Version:** AOS-W 6.1.3.3.

Port-Channel

Table 130: *Port-Channel Fixed Issues*

Bug ID	Description
95129	**Symptom:** The line protocol status of a port in the Link Aggregation Control Protocol (LACP) configuration went down after enabling port monitor feature on the LACP port member. The fix ensures that the LACP port member does not go down. **Scenario:** Enabling port monitor, some flags did not set correctly in the switch. Due to this the switch mirrored the received frames back to the source port. This caused the line protocol status to go down. **Platform:** All platforms. **Reported Version:** AOS-W 6.1.3.10.

Remote AP

Table 131: *Remote AP Fixed Issues*

Bug ID	Description
95572 96920	**Symptom:** All clients, wired and wireless, connected to Remote AP (RAP), were unable to pass traffic locally with source NAT in split-tunnel forwarding mode. The fix ensures that the entries in the route cache table are aged out correctly. **Scenario:** This issue was observed when the route-cache table reached the max size as the aging was not working. This issue was observed when the OAW-4504XM switch was upgraded from AOS-W 6.1.3.6 to AOS-W 6.3.1.2. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.1.

Role/VLAN Derivation

Table 132: *Role/VLAN Derivation Fixed Issues*

Bug ID	Description
89236 94936 96005 99978	**Symptom:** Incorrect VLAN derived for mac-auth derived role-based VLAN. This issue is resolved by deriving the mac-auth derived role-based VLAN from the L2 user-role. **Scenario:** This issue was observed when a user entry existed, user entry was assigned to mac-auth derived role-based VLAN, and the client re-associated. A user was assigned to the default VLAN instead of the mac-auth derived role-based VLAN because mac-auth was skipped for the existing mac authenticated user-entry. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.x.
99745 100008 100198 100435	**Symptom:** Role/VLAN derived from SDR and UDR were incorrect since they matched only the first rule. This issue is resolved by correcting the logical error in code to make sure role/VLAN derivation for SDR and UDR works correctly. **Scenario:** This issue occurred only when SDR and UDR was configured with multiple rules. **Platform:** All platforms. **Reported Version:** AOS-W 6.4.1.0.

VRRP

Table 133: *VRRP Fixed Issues*

Bug ID	Description
87398	**Symptom:** VRRP took 120 seconds to transition from backup to master after switch was reloaded. This issue is resolved by transitioning the VRRP from backup to master when at least one port in the VLAN is in forwarding state. If the forwarding state is not determined till the end of 120 seconds or until 120 seconds of lack of advertisements from the peer switch, the state is eventually transitioned to master state. **Scenario:** This issue was observed after reloading a switch running AOS-W 6.3.0.0. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.3.

WebUI

Table 134: *WebUI Fixed Issues*

Bug ID	Description
94669	**Symptom:** When a channel was not specified during packet capture, error **can't support channel** was displayed. This issue is resolved by using the current working channel. **Scenario:** This issue was observed in switch running AOS-W 6.3.x. **Platform:** All platforms. **Reported version:** 6.3.x.
98939	**Symptom:** The user was unable to access the **Monitoring> Summary** page on a switch GUI using Internet Explorer 9 (IE 9). This issue is resolved by implementing internal code changes that ensures the Web UI loads correctly. **Scenario:** This issue was observed when the switch was upgraded to 6.3.1.4-FIPS. This issue was caused by a missing **DOCTYPE** HTML code in the **Monitoring > Summary** page. Alternatively, the user can access the **Monitoring > Summary** page using Google Chrome or Mozilla Firefox. This issue is not limited to any specific switch model or AOS-W version. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.0.0-FIPS.
99961	**Symptom:** Remote AP settings were missing in the switch WebUI under the **Configuration->Wireless->AP Installation > Provision** page. The remote AP license check is removed to fix this issue. **Scenario:** This issue was observed in switches running AOS-W 6.3.1.6. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.6
100051	**Symptom:** Banner text on login page of the switch's WebUI was incorrectly aligned. The fix ensures that the banner text is aligned correctly. **Scenario:** This issue was observed when a switch was upgraded to AOS-W 6.3.x. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.3.
98951	**Symptom:** Unable to view the configured firewall policies on user role page of web user interface. This issue is resolved by changing the XML data rendering logic to retrieve the data from the attributes instead of nodeValue. **Scenario:** This issue was observed on browsers Internet Explorer 10 and Internet Explorer 11. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.7.

XML API

Table 135: *XML API Fixed Issues*

Bug ID	Description
97102 99101	**Symptom:** Radius accounting START was not triggered for clients when a user was added using XML-API. To resolve this issue, the **check-for-accounting** parameter has been introduced in the Captive Portal configuration. This parameter helps in bypassing the check for Captive Portal profile role, by toggling between older versions and AOS-W 6.3. For more information on this parameter, see Commands Modified in AOS-W 6.3.1.7 on page 32. **Scenario:** This issue was observed only when a user was added before the authentication was complete. This issue was not limited to any specific switch model or release version. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.3.

Resolved Issues in AOS-W 6.3.1.6

The following issues were resolved in AOS-W 6.3.1.6.

AirGroup

Table 136: *AirGroup Fixed Issues*

Bug ID	Description
96236	**Symptom:** An Apple TV got dropped off from the AirGroup server list as the device got deleted from the switch cache table due to expiry of mDNS address record (A or AAAA). The fix ensures that the device is deleted from the switch cache table only if the IP address of the device matches with the expired mDNS address records (A and AAAA). **Scenario:** When an Apple TV acted as a sleep proxy server for other mDNS devices connected in the network, it advertised the address records and services of these mDNS devices. When the advertised address records of the sleeping device expired , the apple TV that acted as the sleep proxy server got deleted incorrectly. This issue is not limited to any specific switch model or AOS-W version.
97685	**Symptom:** AirGroup did not adhere to the global RADIUS settings when the **ip radius source-interface [loopback | vlan]** command was issued. The fix ensures that the global RADIUS configuration overrides the IP address used for sending AirGroup RADIUS requests. **Scenario:** This issue is not limited to any specific switch model or AOS-W version.

ARM

Table 137: *ARM Fixed Issues*

Bug ID	Description
93312	**Symptom:** Analytics and Location Engine (ALE) did not receive the location feed even though the APs were set in AM mode. The fix ensures that the AM configuration for the AP is applied when a switch is rebooted. **Scenario:** This issue was observed when a switch configured with ALE management server was rebooted. This issue was not limited to any specific switch model or release version.
95944	**Symptom:** APs were not allowed to switch channels due to lack of adequate scanning information on the other channels. The fix ensures that APs are allowed to switch channels even if adequate channel information is unavailable when scanning is disabled. **Scenario:** This issue was observed when both scanning and 80 MHz support in the ARM profile were disabled on OAW-AP225 access points running AOS-W 6.3.1.2.
97585	**Symptom:** The **show ap arm client-match history** command displayed that a client was steered to a radio with less than -70 dBm. This was a display error. ARM log does not record the correct signal strength. The fix ensures that the ARM log always notes the signal strength that is used to make client match decision. **Scenario:** This issue was observed in switches running AOS-W 6.3.1.2 or later versions.

AP-Regulatory

Table 138: *AP-Regulatory Fixed Issues*

Bug ID	Description
98303	**Symptom**: Incorrect max EIRP value was displayed for OAW-AP104. This issue is resolved by correcting the regulatory limit. **Scenario**: This issue was observed in OAW-AP104 access points running AOS-W 6.3.1.x due to incorrect value defined for the regulatory limit.

AP-Wireless

Table 139: *AP-Wireless Fixed Issues*

Bug ID	Description
97428	**Symptom**: Users were unable to access the network as the old DHCP route-cache entry was not modified by the new DHCP cache route on Alcatel-Lucent Remote APs (RAP). The fix ensures that the old route cache entry is replaced by the new route cache. **Scenario**: This issue was observed when IPs were assigned to clients through DHCP on RAP. This issue was observed in RAPs running AOS-W 6.3 and 6.4.

Authentication

Table 140: *Authentication Fixed Issues*

Bug ID	Description
96492	**Symptom**: When 802.1X authentication was in progress, two key1 packets were sent out during key exchange. This issue is resolved by making code level changes to ensure that only one key1 packet is sent out during key exchange. **Scenario**: This issue was observed when machine authentication was enabled and when user authentication was processed. During this time if the machine-authentication details were found in the cache, key1 was sent out again for the second time. This issue is not limited to any specific switch model or AOS-W version.

Base OS Security

Table 141: *Base OS Security Fixed Issues*

Bug ID	Description
89169	**Symptom:** The output of the **show aaa authentication-server radius statistics** command displayed a negative value for average response time (AvgRspTm). The fix ensures that the final value is not negative. **Scenario:** This issue was observed in switches running AOS-W 6.4 or earlier.

Captive Portal

Table 142: *Captive Portal Fixed Issues*

Bug ID	Description
93927	**Symptom:** On OAW-4x50 Series switches the output of **show datapath user** displayed a user entry but the user entry was not present in the control plane. This issue was resolved by internal code changes. **Scenario:** This issue occurred when WLAN was configured in the tunnel mode and was observed in AOS-W versions 6.2 or later.
98992	**Symptom:** After upgrading from 6.1.3.9 to 6.3.1.4, Captive Portal (CP) redirect was not sent, so CP Authentication could not be completed. This issue is resolved by introducing forward lookup mechanism to check if CP Authentication has been configured multiple times for the same client. If multiple CP Authentications are detected, they are redirected until the CP configuration is complete. **Scenario:** This issue was observed only when multiple CP Authentication configurations were created. This issue was observed in AOS-W 6.4 and 6.3.1.3 or later versions.

Switch-Datapath

Table 143: *Switch-Datapath Fixed Issues*

Bug ID	Description
84585 92227 92228 92283 94200 96860 98380	**Symptom:** Traffic failed to pass a network with heavy traffic (such as high levels of packet replication), when AES-CCM or another encryption/decryption modes were enabled. This issue is resolved by increasing the estimated time for packet processing, in the datapath. **Scenario:** This issue was identified on a OAW-4x50 Series switch connected to 2000 APs when Gratuitous ARP messages were replicated and sent to clients.

Switch-Platform

Table 144: *Switch-Platform Fixed Issues*

Bug ID	Description
91097	**Symptom:** A local switch rebooted unexpectedly. The log files for the event listed the reason for the reboot as **Mobility Processor update**. The fix ensures that the switch does not reboot unexpectedly by making code level changes to the primary and secondary nor flash boot partition. **Scenario:** This issue was observed in switches running AOS-W 6.1.3.9.
96712	**Symptom:** A local switch rebooted unexpectedly during terminal/ssh related operation. The log files for the event listed the reason for the reboot as **Kernel panic**. **Scenario:** This issue was observed in OAW-4750 switches running AOS-W 6.2.1.4.
97658 97388 98373	**Symptom:** Some access points went down when the switch to which they were connected rebooted. This issue is resolved by ensuring that the boot partition information is updated in the secondary bank of the switch. **Scenario:** This issue occurred when the switch rebooted due to a watchdog reset. This issue was not limited to any specific switch model or release version.

DHCP

Table 145: *DHCP Fixed Issues*

Bug ID	Description
96117 96433	**Symptom:** Some wireless clients experienced delay in obtaining an IP address. This issue is fixed by disabling the DDNS (Dynamic Domain Name system) update logic within Dynamic Host Configuration Protocol (DHCP). **Scenario:** This issue occurred when the DHCP pool was configured with the domain name and the Domain Name System (DNS) server was configured on the switch, using **ip name-server** command. This resulted in DDNS update of the host and delayed the response for the DHCP request. This issue was not limited to any specific switch model or AOS-W version.

IPsec

Table 146: *IPsec Fixed Issues*

Bug ID	Description
98901	**Symptom:** An internal process (**ISAKMPD**) crashed on the switch. This issue is fixed by properly allocating the Process Application Programming Interface (PAPI) message that is sent from **ISAKMPD** process to the Instant Access Point (OAW-IAP) manager. **Scenario:** This issue occurred when the OAW-IAPs terminated on the switch and established IKE/IPsec connections with the switch. This issue was more likely to happen on OAW-S3, OAW-4704, and OAW-4504 switch models than on OAW-4550/4650/4750 Series switch models, and occurred on AOS-W running 6.3 or later.

Master-Redundancy

Table 147: *Master -Redundancy Fixed Issues*

Bug ID	Description
98005	**Symptom:** After centralized licensing was enabled, the standby master displayed **UPDATE REQUIRED** message. This issue is resolved by ignoring the RAP bit when checking if a new license type has been added. **Scenario:** This issue was observed when the centralized licensing was enabled and the master switch had embedded AP licenses. This issue was not limited to a specific switch model but is observed in AOS-W 6.3.1.3, when the master switch has embedded AP licenses.

RADIUS

Table 148: *RADIUS Fixed Issues*

Bug ID	Description
93578	**Symptom:** In the **show auth-trace buff** command output, the number of RADIUS request packets jumped from 127 to 65408. This issue is fixed by changing the data type of the variable used in the command output. **Scenario:** This issue occurred due to an incorrect value that was displayed in the command output. This issue was not limited to any specific switch model or AOS-W version.
97931	**Symptom:** Radius accounting packets displayed an incorrect AVP value when the accounting octet counter value exceeded 2^32. This issue is resolved by updating the 64 bit counter in the switch. **Scenario:** This issue was observed when the data upload/download exceeded 4 GB. This issue was not limited to any specific switch model or release version.

Remote AP

Table 149: *Remote AP Fixed Issues*

Bug ID	Description
99136 98432	**Symptom:** A RAP displayed **Regulatory domain miss-match** error and got converted to AirMonitor mode even though it was set in AP specific mode. This issue is resolved by making code level changes to the AP regulatory domain. **Scenario:** This issue occurred when both ap-name and ap-group were configured for the RAP and if the AP regulatory was configured only for the ap-group. This issue was observed in a RAP that terminated on a switch running AOS-W 6.3.1.4.

Station Management

Table 150: *Station Management Fixed Issues*

Bug ID	Description:
96910	**Symptom:** The SNMP query on the objects, **wlanAPRxDataBytes64** and **wlanAPTxDataBytes64** returned incorrect values for OAW-AP225. This issue is resolved by making code level changes to the read function in the Broadcom driver. **Scenario:** This issue was observed when the statistics in the Broadcom driver was parsed incorrectly. This issue was observed in OAW-AP225 access points running AOS-W 6.3.x and later versions.

Voice

Table 151: *Voice Fixed Issues*

Bug ID	Description
94342	**Symptom:** The **Station Management (STM)** process crashed in a New Office Environment (NOE) deployment. This issue is resolved by making code level changes to avoid a STM crash. **Scenario:** This issue was observed when an NOE user tried to call an extension, but disconnected the call before it was complete, as a result the CDR changed to **CONNECTING** state. This issue was observed in AOS-W 6.1.3.10.
95566	**Symptom:** When two parties made a VoIP call using Microsoft® Lync 2013, media classification running on the switch prioritized the media session with wrong DSCP values. The fix ensures that the wmm value is read from the TUNNEL Entry rather than the Bridge Entry, so that the value is correct. **Scenario:** The DSCP values configured under the ssid-profile did not take effect. This issue occurred when the initial VLAN and the assigned VLAN were different. This issue was observed on OAW-S3 switches running AOS-W 6.1.3.10.

VLAN

Table 152: *VLAN Fixed Issues*

Bug ID	Description
94423	**Symptom:** There was a mismatch between the device id stored in the user table and the AP cache. The fix ensures that the information retrieved from **show user** command and device id cache display the information received in the first packet. **Scenario:** This issue was observed when the device id cache was not updated by the AP, but when the **show user** command was executed, the updated device id cache was displayed. This issue was not limited to any specific switch model or release version.
97117	**Symptom:** When the RADIUS server returned multiple Vendor Specific Attributes (VSAs), AOS-W did not check these attributes or set user roles. This issue is fixed by verifying the list of attributes before matching them with the rules. **Scenario:** This issue was observed when a user tried to set a role using the VSA attributes that were returned from the RADIUS server. This issue was observed in OAW-4604 Series switches running AOS-W 6.2.1.4.

WebUI

Table 153: *WebUI Fixed Issues*

Bug ID	Description
95185	**Symptom:** Collecting the **logs.tar** with **tech-support** logs from the switch's WebUI failed with **Error running report... Error: receiving data from CLI, interrupted system call** error message. The fix ensures that the session is kept active till the logs are ready to be downloaded. **Scenario:** This issue was not seen under the following cases: • Downloading the **logs.tar** without **tech-support** log from the WebUI. • Downloading the **logs.tar** with **tech-support** logs from the CLI. This issue was observed in OAW-4650 switch running AOS-W 6.3.1.2.

Resolved Issues in AOS-W 6.3.1.5

The following issue was resolved in AOS-W 6.3.1.5.

Base OS Security

Table 154: *Base OS Security Fixed Issues*

Bug ID	Description
99070	**Symptom:** An Alcatel-Lucent switch's WebUI and captive-portal were vulnerable to an OpenSSL TLS heartbeat read overrun attack. For more information on this vulnerability, read the OpenSSL Security Advisory. The TLS heartbeat in the current OpenSSL version 1.0.1c is disabled so that any heartbeat request will be ignored by the switch. This fixed the issue. **Scenario:** This issue was observed in switches running AOS-W 6.3 or later versions.

Resolved Issues in AOS-W 6.3.1.4

The following issues were resolved in AOS-W 6.3.1.4.

AirGroup

Table 155: *Air Group Fixed Issues*

Bug ID	Description
96675	**Symptom:** Local switches handling **multicast Domain Name System (mDNS)** process crashed. To resolve this issue, the cache entries and memory used for the device that sends an mDNS response packet with a time-to-live (TTL) value as zero are cleared. **Scenario:** This issue was observed when the switch received mDNS response packets, and the value of TTL was set to zero. This issue was observed in AOS-W 6.3, but is not specific to any switch model.

AMON

Table 156: *AMON Fixed Issues*

Bug ID	Description
94570	**Symptom:** Incorrect roles were displayed in the WebUI Dashboard for the clients connected to RAPs in split-tunnel mode. This issue was resolved by resetting the flag that populates the client role value, in the Dashboard. **Scenario:** This issue was not limited to any specific switch model or release version.

AP-Platform

Table 157: *AP-Platform Fixed Issues*

Bug ID	Description
94716	**Symptom:** When client traffic was moving through an L3 GRE tunnel between a data switch and a switch, the switch did not provide the captive portal page to the client. **Scenario:** This issue was observed after the OAW-S3 was upgraded to AOS-W 6.1.3.10. This issue was caused because the switch was unable to find the correct role for the client traffic and, therefore, did to provide the captive portal page.
95893	**Symptom:** When an AP sent a DHCP request, it received an IP address 0.0.0.0 from the Preboot Execution Environment (PXE) server. Though the AP accepted this IP address, the AP could not communicate further and rebooted. The fix ensures that the PXE acknowledgment is ignored and the AP receives a valid IP address. **Scenario:** This issue was observed in deployment scenarios that have a DHCP server and multiple PXE servers. This issue was observed in APs running AOS-W 6.3 or earlier.
96051 96754 98008	**Symptom:** OAW-AP115 access points rebooted unexpectedly. This issue is resolved by adding a device queue status check before sending data to an ethernet driver. **Scenario:** A crash occurred when the throughput was high on ethernet connected to a 100/10M switch. This issue was observed in OAW-AP114 and OAW-AP115 access points running AOS-W 6.3.x and later versions.
96239 95472	**Symptom:** When an AP was configured with a static IP address, the Link Aggregation Control Protocol (LACP) on OAW-AP220 Series access points was not functional. This issue is resolved by initiating a LACP negotiation when an AP with a static IP is identified. **Scenario:** This issue was observed in OAW-AP220 Series access points running AOS-W 6.3.1.3 and 6.4.0.1 when configured with a static IP.
96913	**Symptom:** When a switch was upgraded from AOS-W 5.x or AOS-W 6.0.x to AOS-W 6.3.1.3, APs failed to upgrade to AOS-W 6.3.1.3. A defensive check is made in affected API so that PAPI messages which are smaller than PAPI header size are handled properly in 6.0.x compared to 5.x. **Scenario:** This issue was observed in APs running AOS-W 5.x or AOS-W 6.0.x. APs running AOS-W 6.1 and later versions were not impacted.
97544	**Symptom:** OAW-RAP109 could not be used on un-restricted switches that do not have Japan country code. This issue is resolved by using the country code in AP regulatory domain profile for AP regulatory domain enforcement. **Scenario:** This issue was observed when OAW-IAP109 with Japan SKU was converted to OAW-RAP109 which was running AOS-W 6.3.1.3.

AP-Regulatory

Table 158: *AP-Regulatory Fixed Issues*

Bug ID	Description
94264 96731	**Symptom:** The equivalent isotropically radiated power (EIRP) displayed an incorrect value when CSA was enabled. This issue is resolved by updating the EIRP statistics when transmit power changes from open loop to close loop with CSA enabled. **Scenario:** This issue was observed on OAW-AP225 devices running AOS-W 6.3.1.4 and earlier.

AP-Wireless

Table 159: *AP-Wireless Fixed Issues*

Bug ID	Description
86184	**Symptom:** Wireless clients were unable to associate to an access point on the 5 GHz radio. This issue is resolved by making code level changes to ensure that an APs channel is changed after radar detection. **Scenario:** This issue was observed when a channel change in an access point failed after a Dynamic Frequency Selection (DFS) radar signature detection. This issue was observed in OAW-AP125 running AOS-W 6.1.x, 6.2.x, 6.3.x.
96751	**Symptom:** An AP continuously crashed and rebooted due to out of memory. Disabling wireless and rogue AP containment features in the **Intrusion Detection System (IDS**) profile resolved this issue. **Scenario:** This issue occurred when wireless and rogue AP containment features were enabled on the IDS profile. This issue was observed only on the OAW-AP225 Series running AOS-W 6.3.1.2 version.
97818	**Symptom:** Zebra® QL 420 Plus did not associate with OAW-AP220 Series access points. Improvements in the wireless driver of the AP in AOS-W 6.4.0.2 resolved the issue. **Scenario:** This issue was observed in OAW-AP220 Series access points running AOS-W 6.3.1.2 or later versions.

Authentication

Table 160: *Authentication Fixed Issues*

Bug ID	Description
96285	**Symptom:** The user was not assigned with the correct role when the XML API changed the user role. This issue is resolved by sending a notification to the Campus AP (CAP) in the bridge mode during External Captive Portal (ECP) event of role change. **Scenario:** This issue was observed when the client was connected to the CAP in the bridge mode. This issue was not limited to any specific switch model and occurred on AOS-W running 6.3.1.2.

Base OS Security

Table 161: *Base OS Security Fixed Issues*

Bug ID	Description
88271 96676	**Symptom:** It was not possible to configure a **deny any any protocol** access control list (ACL) that overrode a statically configured **permit any any protocol** ACL. This issue is resolved by improvements that allow a user-defined ACL to take precedence over a static ACL entry. **Scenario:** This issue was observed on a switch running AOS-W 6.3.0.1.
95367	**Symptom:** Issuing **show rules <role-name>** command from the command-line interface of a switch resulted in an internal module (Authentication) crash. Ensuring that Access Control Lists (ACLs) are not configured with spaces in the code resolved the issue. **Scenario:** This issue was observed when a large number of ACLs were configured with spaces in their names. This was not limited to any specific switch model or AOS-W version.
96458	**Symptom:** A switch rebooted with the reboot cause **Nanny rebooted machine - low on free memory**. This issue is resolved by freeing the memory that was leaking in the authentication module. **Scenario:** This issue was observed for VPN users when the **cert-cn-lookup** parameter was disabled under **aaa authentication vpn** profile. This issue was not limited to a specific switch model or release version.

Table 161: *Base OS Security Fixed Issues*

Bug ID	Description
96755	**Symptom:** Wired 802.1X authentication with protocol EAP-MD5 was not working. This issue is resolved by the modifying the authentication code to allow the wired-clients that perform authentication with protocol EAP-MD5. **Scenario:** This Issue was observed when wired clients connected directly either to the switch or to the Ethernet port of a CAP or Remote AP. This issue was not limited to a specific switch model or release version.

Captive Portal

Table 162: *Captive Portal Fixed Issues*

Bug ID	Description
92927 94414 97765	**Symptom:** When iOS 7 clients tried to connect through the Captive Portal profile, the users were not redirected to the next page even after a successful authentication. A change in the redirect URL has fixed this issue. **Scenario:** This issue was observed only in clients using Apple iOS 7 devices.

Switch-Datapath

Table 163: *Switch-Datapath Fixed Issues*

Bug ID	Description
93582	**Symptom:** A OAW-4550 switch crashed. The logs for the event listed the reason for the crash as **datapath timeout**. Ensuring that the destination UDP port of the packet is PAPI port while processing Application Level Gateway (ALG) module resolved this issue. **Scenario:** This issue was observed in OAW-4550 switches running AOS-W 6.3.1.0.
93874 96093 96886	**Symptom:** When connected to WPA2 SSID some clients did not receive any successful acknowledgment from the server. The OAW-4550/4650/4750 Series switches now correctly handles the replay counter capabilities. **Scenario:** This issue was observed when multiple Wi-Fi Multimedia Traffic IDs (WMM TIDs) were sent to the clients that did not support multiple replay counters and the TIDs did not function properly. This issue occurred on OAW-4550/4650/4750 Series switches running AOS-W prior to 6.3.1.3.
95939 96156	**Symptom**: The local switch crashed as buffer allocation requests were queued to a single processor that resulted in high CPU utilization. This issue is resolved by distributing allocation requests to different CPUs to balance the load across all processors. **Scenario**: This issue was observed in OAW-4550/4650/4750 Series switches running AOS-W 6.3.

Switch-Platform

Table 164: *Switch-Platform Fixed Issues*

Bug ID	Description
95929	**Symptom:** The switch rebooted with incorrect partition. The fix ensures that when you issue the **halt** command and reboot the switch manually, the switch reboots with the correct partition. **Scenario:** This issue was seen when you issue the **halt** command and reboot the switch manually. This issue was observed in OAW-S3 switches running AOS-W 6.3.1.1.
96420 88234 91172 93465 93913 94754 95664 97384	**Symptom:** A local switch rebooted unexpectedly. The log files for the event listed the reason for the reboot as **Kernel Panic**. This issue is resolved by making code level changes to handle chained buffer punts to the CPU. **Scenario:** This issue was observed when the local switch received an Aggregate MAC Service Data Unit (AMSDU) packet sent by the clients as fragmented multiple packets which triggered internal conditions. This issue was observed in OAW-4704 switches running AOS-W 6.3.1.2.
97237	**Symptom:** A switch rebooted because of memory leak in the module that handles address, route, and interface related configurations and notifications on the system. This issue is resolved by fixing the memory leak in the flow. **Scenario:** Memory leak occurred when an interface or STP states changed frequently with PAPI error. This issue was observed on OAW-4306G switch running AOS-W 6.2.1.6 or later.

DHCP

Table 165: *DHCP Fixed Issues*

Bug ID	Description
94512	**Symptom:** The **Not enough memory** error occurred on the DHCP Server page when many DHCP pools (60+) were configured. This issue was resolved by modifying the backend information-fetch logic. **Scenario:** This issue was triggered when executing the **show ip dhcp database** command in the CLI or when navigating to **Configuration** > **Network** > **IP** > **DHCP Server** in the WebUI. This issue was observed on switches running AOS-W 6.3.0.0

Hotspot 802.11u

Table 166: *Hotspot 802.11u Fixed Issues*

Bug ID	Description
79063	**Symptom:** Radius accounting packets displayed an incorrect AVP value when the accounting octet counter value exceeded 2^32. This issue is resolved by updating the 64 bit counter in the switch. **Scenario:** This issue was observed when the data upload/download exceeded 4 GB. This issue was not limited to any specific switch model or release version.

IPSec

Table 167: *IPSec Fixed Issues*

Bug ID	Description
95634	**Symptom:** Site-to-Site IPsec VPN tunnels randomly lost connectivity on a OAW-4550 switch. This issue is resolved by making code level changes to ensure that the key length matches. **Scenario:** This issue was observed when there were 500 or more remote sites terminating IPsec VPN tunnels on a OAW-4550 switch running AOS-W 6.3.1.2.

LDAP

Table 168: *LDAP Fixed Issues*

Bug ID	Description
90859	**Symptom**: A switch intermittently disconnected from the LDAP server because the LDAP server reset its TCP connection. After establishing a TCP connection for each user and binding it using admin-dn and password fixed this issue. Once the user is authenticated, the connection binds the actual user. **Scenario**: This issue was triggered by null binds created when the switch established TCP/SSK connections in advance, so that they can be used whenever a user joined the network. This issue occurred in a OAW-4x04 Series switch running AOS-W 6.1.3.10.

Mobility

Table 169: *Mobility Fixed Issues*

Bug ID	Description
96207 96214 96222 96555	**Symptom:** The client did not receive an IP address through DHCP, and could not pass traffic when L3 mobility was enabled on the switch. This issue is resolved by clearing the state machine of the affected client. **Scenario:** This issue was observed when the client roamed from a Virtual AP (VAP) in which the **mobile-ip** parameter was enabled to a VAP in which the **mobile-ip** parameter was disabled. This issue was observed in AOS-W 6.3 and later versions, but was not limited to a specific switch model.

Radius

Table 170: *Radius Fixed Issues*

Bug ID	Description
96038	**Symptom:** Sometimes, the user name was missing in the RADIUS accounting stop messages sent from the switch. The fix ensures that a check is added for user entries with multiple IP addresses before deauthenticating. **Scenario:** This issue was observed when user entries with multiple IP addresses was deauthenticated as it had more than one IP address. This issue was not limited to any specific switch model or release version.

Remote AP

Table 171: *Remote AP Fixed Issues*

Bug ID	Description
93707	**Symptom:** A Remote AP (RAP) re-bootstrapped every six minutes if the RAP's local gateway IP was 192.168.11.1. Changing the DHCP pool of the RAP to 172.16.11.* by the AP resolved this issue. **Scenario:** This issue occurred on switches running AOS-W 6.2.1.4 and 6.3.1.1. It was caused by the DHCP server net assignment conflicting with the RAP's local networks.
97009	**Symptom:** A RAP failed to establish a PPPoE connection when the RAP's uplink port was VLAN tagged. The fix ensures that the RAP can establish a PPPoE connection with VLAN tag. **Scenario:** This issue was observed in RAPs running AOS-W 6.3.1.3.

Station Management

Table 172: *Station Management Fixed Issues*

Bug ID	Description
86620 88646	**Symptom**: The **show ap association client-mac** command showed client MAC addresses for clients that aged out beyond the idle timeout value. This issue is resolved by making code level changes to station table in the STM module. **Scenario**: This issue was not limited to a specific switch or AOS-W release version.

Voice

Table 173: *Voice Fixed Issues*

Bug ID	Description
91910	**Symptom:** The output of the **show voice call-cdrs** command displayed multiple CDR with **INITIATED** state for calls between ASCOM® phones. The fix ensures to handle the state transitions for New Office Environment (NOE) application layer gateway. **Scenario:** This issue occurred during a consulted call scenario. This issue is observed in an NOE deployed voice environment with switches running AOS-W 6.1 or later versions.
94038 94600	**Symptom:** The **show voice call-cdrs** and **show voice client-status** commands displayed incorrect state transitions for consulted, transfer, and speaker announced call scenarios. The fix ensures the state transitions for New Office Environment (NOE) application layer gateway. **Scenario:** This issue was observed in an NOE deployed voice environment with switches running AOS-W 6.1 or later versions.
94546 94641	**Symptom:** The CDR for NOE phones was in an **ALERTING** state when a call was disconnected by the caller before it was accepted. The fix ensures that the CDR is terminated when the **RING_OFF** event is triggered in for New Office Environment (NOE) Application Layer gateway (ALG). **Scenario:** This issue occurred when an NOE call was received by a wireless client connected to the switch from a wired client outside the switch. This issue was observed in switches running AOS-W 6.1 or later versions.

WebUI

Table 174: *WebUI Fixed Issues*

Bug ID	Description
68464 94529 94961	**Symptom:** The user was forced out of a WebUI session with the **Session is invalid** message. This issue is resolved by fixing the timing issue for the exact session ID from cookies in the https request. **Scenario:** This issue was observed when a web page of the parent domain name was accessed previously from the same browser. This issue was not limited to any specific switch model or release version.
94818	**Symptom: AP Group** name did not support special characters. With this fix, you can create an **AP Group** name with the following special characters: **" / > < : } { + _) (* & ^ % $ # @ ! [ ] ; , . /**. **Scenario:** This issue was seen when you create an **AP Group** from the **Configuration > WIRELESS > AP Configuration** page of the switch's WebUI. This issue was not limited to any specific switch or release version.
96465	**Symptom:** Some cipher suites were not working when the operations were offloaded to hardware. This issue was resolved by disabling the cipher suites which were not working with the hardware engine. **Symptom:** This issue was observed during any crypto operation that uses DH key exchange**.**

Resolved Issues in AOS-W 6.3.1.3

The following issues were resolved in AOS-W 6.3.1.3:

Air Management-IDS

Table 175: *Air Management-IDS Fixed Issues*

Bug ID	Description
92070	**Symptom:** The age field in the RTLS station report sent by an AP was sometimes reset, although the station was no longer associated to an AP. **Scenario:** This issue occurred when the AP could not detect frames from the station. This issue occurred when the detecting AP can no longer hear frames from the station, but it can still hear frames sent by other APs to the station. This issue was observed on a switch running AOS-W 6.1 or later.
93912	**Symptom:** The **show wms client probe** command did not display any output, instead displayed a **wms module busy** message. To resolve this issue, execute the command with the MAC address. **Scenario:** This issue was observed when there was a large number of entries in the WLAN Management System (WMS) table. This issue was not limited to any specific switch model or release version.

AP-Platform

Table 176: *AP-Platform Fixed Issues*

Bug ID	Description
87857	**Symptom**: Fragmented configuration packets sent from a switch to an AP caused the AP to come up with the "D:" (dirty) flag. Improvements to how AOS-W handles out-of-order packets resolved this issue. **Scenario**: This issue was triggered by network congestion or breaks in the connection between the switch and AP.
88504	**Symptom:** No output was displayed when the **show ap config ap-group <ap-group>** command was executed. To resolve this issue, the buffer size of SAPM (an AP management module in STM) was increased. **Scenario:** This issue was observed on switches running AOS-W 6.3.0.x.
88813 89594	**Symptom:** The **show ap allowed-max-EIRP** command displayed incorrect information for OAW-AP220 Series access points. This issue is resolved by increasing the buffer size that stores Effective Isotropic Radiated Power (EIRP) information. **Scenario:** This issue was observed in OAW-4504 switches and OAW-4604 switches running AOS-W 6.3.x.
92348	**Symptom:** Upstream traffic flow was interrupted and caused IP connectivity issues on MAC OS clients. This issue is fixed by setting the maximum number of MAC service data units (MSDUs) in one aggregate-MSDU (A-MSDU) to 2 and disabling the de-aggregation of AMSDU for tunnel mode VAP. **Scenario:** This issue occurred when the maximum number of MSDUs in one A-MSDU was set to 3, which was not supported in Broadcom driver. This issue was observed in MacBook Air clients associated with OAW-AP225 access points running AOS-W 6.3.1.0.
93012	**Symptom:** Sometimes, a low voice call quality was observed on the clients. This issue is resolved by suspending any off-channel AP operation and ensuring that the voice calls are given higher priority. **Scenario:** This issue was observed in OAW-AP225 connected to switches running AOS-W 6.3.1.0 and earlier versions.
93715 95259 93380 93744 95619	**Symptom:** An unexpected reboot of a OAW-AP220 Series occurred due to a kernel panic. To resolve this issue, internal software changes were made.

Table 176: *AP-Platform Fixed Issues*

Bug ID	Description
	Scenario: This reboot was triggered by VAP deletion and occurred upon mode change when all VAPs were deleted. The crash was caused because AOS-W accessed the PCI device when it was inactive and all the VAPs were deleted. This issue was observed in OAW-AP220 Series and was not limited to any specific AOS-W release version.
94279	**Symptom:** A mismatch was observed on switches in the non-US regulatory domain, after OAW-IAP was converted to a switch-based AP. This issue is resolved by adding a new rule to verify the Rest of the World (RW) domain and accept RW APs on non-US switches. **Scenario:** This issue was observed in OAW -IAP224, OAW -IAP225-RW, OAW -IAP114, and OAW -IAP114-RW.
94456	**Symptom:** Users observed AP reboot issues with two source MAC addresses from the same port. This issue is fixed by not allowing ICMPv6 packets (even when it is UP) before Ethernet 1 is bonded. **Scenario:** This issue occurred when Ethernet 1 acted as uplink on an AP and the first ICMPv6 packet was sent with source MAC address of Ethernet 1. However, the successive ICMPv6 packets were sent with the source MAC of Ethernet 0 and caused AP reboot. This issue was not limited to any AP, switch models, or release version.

AP-Regulatory

Table 177: *AP-Regulatory Fixed Issues*

Bug ID	Description
92775 96408	**Symptom:** Wireless clients received Automatic Private IP Address (APIPA) when associated to OAW-AP225. Improvements in the wireless driver of the AP fixed the issue. **Scenario:** This issue was observed when wireless clients associated to encryption-enabled tunnel-mode Virtual AP (VAP) on the OAW-AP225 and there was one or more bridge or decrypt-tunnel VAPs configured with encryption mode set to **static-wep**.
95759	**Symptom:** RADAR detection and channel change events were observed in APs on Russia country code. The issue is fixed by correcting the country domain code for Russia. **Scenario:** This issue was not limited to any specific AP model or AOS-W release version.

AP-Wireless

Table 178: *AP-Wireless Fixed Issues*

Bug ID	Description
86584	**Symptom:** The OAW-AP225 did not support prioritization for multicast traffic. **Scenario:** This issue was observed on the OAW-AP220 Series running AOS-W 6.3.x.
88827 93771	Symptom: An AP stopped responding and rebooted. Log files listed the reason for the event as **ath_bstuck_tasklet: Radio 1 stuck beacon; resetting**. To resolve this issue, changes were made to the radio channel assignments and reset routines. **Scenario**: This issue occurred in OAW-AP125 running AOS-W 6.2.1.3, and was not associated with any switch model.
93113	**Symptom:** Windows 7 clients using Intel 4965 NIC intermittently stopped passing traffic when connected to OAW-AP225. Changes in the internal code resolved this issue. **Scenario:** This issue occurred on OAW-AP225 running AOS-W 6.3.1.1.

Table 178: *AP-Wireless Fixed Issues*

Bug ID	Description
93288	**Symptom:** Some clients with low signal strength had trouble sending packets to an AP. Implementing the Cell-Size-Reduction feature on OAW-AP220 Series along with deauthorizing clients when they roam out of the desired cell range resolved this issue. **Scenario:** This issue was observed in OAW-AP220 Series connected to switches running AOS-W 6.3.1.1 or earlier.
93996	**Symptom:** A OAW-AP120 Series access point rebooted unexpectedly. **Scenario:** This issue occurred on OAW-AP120 Series devices connected to switches running AOS-W 6.3.1.0.
94117	**Symptom**: Clients are unable to connect to an SSID when the **Local Probe Request Threshold** setting in the SSID profile was set to a value of 25 dB. This issue is resolved by introducing changes that allow the AP to respond to probe requests with the same dB value as the local probe request threshold. **Scenario**: This issue was triggered in AOS-W 6.3.1.x, when the Local Probe Request Threshold was set to 25 dB, and the AP did not respond to probe requests with an SNR higher than 35 dB. As a result, APs did not respond to authentication requests from the clients, preventing them from associating to the AP.
94164	**Symptom:** In a WPA-AES network, wireless clients were unable to connect to OAW-AP225 when high throughput (HT) and very high throughput (VHT) were disabled in HT-SSID profile , but enabled in the radio profile. This issue is fixed by ensuring that the WMM configuration is consistent across virtual APs. **Scenario:** This issue was occurred due to inconsistencies in the WMM configuration when HT-SSID profile configuration was changed. This issue was observed in OAW-AP225 running AOS-W 6.3.1.1.
94198	**Symptom:** An AP rebooted unexpectedly with the log error message out of memory. **Scenario:** This issue was observed in OAW-AP120 Series switches running AOS-W 6.3.1.0.
95006	**Symptom:** IOS devices could not connect to APs after upgrading from 6.1.3.8 to 6.3.1.2.This issue is resolved by revising the received signal strength indication (RSSI) threshold value that triggers the hand-off assist. **Scenario:** This issue was observed in switches running AOS-W 6.2 and 6.3 when the RSSI dropped below the defined threshold value.

Authentication

Table 179: *Authentication Fixed Issues*

Bug ID	Description
88385 94033	**Symptom**: Bridge mode users (802.1X and PSK) were unable to associate to a remote access point (RAP). Adding reference count for messages between authentication and Station management processes to avoid incorrect order of messages resolved this issue. **Scenario**: This issue occurred because of the incorrect order of messages between authentication and station management processes. This issue is observed in switches running AOS-W 6.3.0.1 or later.
94629	**Symptom:** The clients connected to RAPs lost connectivity when the process handling the AP management and user association crashed. This fix ensures that the AP management and user association process does not crash. **Scenario:** This issue was observed in switches running AOS-W 6.3 and 6.4.

Base OS Security

Table 180: *Base OS Security Fixed Issues*

Bug ID	Description
90904 92079	**Symptom:** In the AOS-W Dashboard, under **Clients > IP address**, the IP addresses, Role Names, and names of clients connected to a RAP in split tunnel mode were not displayed. **Scenario:** This issue occurred when the complete client information was sent to the switch and therefore was not displayed in the dashboard.
93130	**Symptom:** A switch reboots unexpectedly. The log files for the event listed the reason for the reboot as **datapath exception**. This issue is resolved by adding SSL implementation to validate a packet before processing it. **Scenario**: This issue was observed when VIA was used to establish a tunnel with the switch, using SSL fallback. This issue was not limited to any specific switch model or release version.
93237	**Symptom:** An internal module (Authentication) crashed on the switch. This issue is resolved by ignoring the usage of the **equivalentToMe** attribute that was not used by the master switch. **Scenario**: This issue was observed when the Novell Directory System (NDS) pushed the bulk of user data as the value for the attribute to the master switch. This issue was not limited to any specific switch model or release version.
93537	**Symptom:** Wireless clients did not get a Dynamic Host Configuration (DHCP) IP. This issue is resolved by enabling both IP Mobility and MAC authentication, so that user gets an IP address even if the MAC authentication fails due to configuration error or connectivity issues. **Scenario**: This issue was observed when L3 mobility was configured on the switch and MAC authentication failed for the client, which caused mobile IP to drop packets from the client. This issue was not limited to any specific switch model or release version.

Captive Portal

Table 181: *Captive Portal Fixed Issues*

Bug ID	Description
88405	**Symptom**: After successfully authenticating a client using Captive Portal, the browser did not automatically redirect the client to the original URL. **Scenario**: This issue was observed in the OAW-4550/4650/4750 Series switch running AOS-W 6.3.0.0.
92170	**Symptom:** In Captive Portal, a custom welcome page did not redirect to the original Web page after successful client authentication. Changes in the Captive Portal code to send "url" cookie to the Web browser fixed this issue. **Scenario:** This issue was not limited to a specific switch model and was observed in AOS-W 6.3.0.0 and later versions.
93674	**Symptom**: Clients are unable to access an external Captive Portal page after the switch resets. Changes in how AOS-W manages captive portal authentication profiles resolved this issue. **Scenario**: This issue occurred in AOS-W 6.1.3.x when the switch failed to use the correct ACL entry for a pre-authentication captive portal role.

Configuration

Table 182: *Configuration Fixed Issues*

Bug ID	Description
88120	**Symptom**: The **Configuration > Wireless > AP Installation > AP provisioning > Status** tab of the switch WebUI and the output of the commands **show ap database long status up start 0 sort-by status sort-direction ascending** and **show ap database long status up start 0 sort-by status sort-direction descending** did not sort the AP entries in ascending or descending order of up time. Improvements to how the switch sorts APs by status and up time resolve this issue. **Scenario**: This issue was observed in switches running AOS-W 6.2.1.2.
94559	**Symptom**: An ACL configured by the user could not be edited or deleted. This issue is resolved by ensuring that the flag is reset when the ACLs generated for the whitelist configuration were re-used after removing the white-list. **Scenario**: This issue was observed in AOS-W 6.2 or later, when a user configuration had white-listing in Captive Portal profiles.

Switch-Datapath

Table 183: *Switch-Datapath Fixed Issues*

Bug ID	Description
82770	**Symptom:** Using ADP, access points did not discover the master switch after enabling Broadcast/Multicast (BC/MC) rate optimization. With this new fix, enabling BC/MC rate optimization does not block ADP packets. **Scenario:** When BC/MC rate optimization was enabled on the VLAN, the switch dropped ADP packets from access points. This issue was not limited to a specific switch model or release version.
87417 87846 87949 88039 88226 88445 89433 89539 89641 90024 90458 90469 90746 90896 91853 92284 92464 92466 92827 92828 92829 92830 92832 94007	**Symptom:** A master switch rebooted unexpectedly. The log files for the event listed the reason for the reboot as **datapath exception**. Enhancements to the chipset driver of the switch fixed this issue. **Scenario:** This issue was observed in OAW-4750 switch running AOS-W 6.3.1.1 in a master-local topology.
92657	**Symptom:** Although the **prohibit-arp-spoofing** parameter was disabled in Firewall, clients were getting blacklisted with reason: ARP spoofing. Controlling the action on ARP-spoofing only by the prohibit-arp-spoof parameter and on ip-spoofing only by the **firewall prohibit-ip-spoof** parameter fixed the issue. **Scenario:** This issue was not limited to a specific switch model or release version.

Table 183: *Switch-Datapath Fixed Issues*

Bug ID	Description
93466	**Symptom**: The OAW-4x50 Series switches rebooted and the log files for the event displayed the reason for the reboot as **datapath timeout.** The fix ensures that packets to monitor the port are not sent if the port is down. **Scenario**: This issue was observed when the port monitor was enabled on the switch and then a Small Form-factor Pluggable (SFP) was plugged in the monitor port. This issue was observed in OAW-4x50 Series switches and was not limited to a specific release version.
93874	**Symptom:** With Multiple TID Traffic to Temptrak device with AES Encryption, the device drops packets from AP. **Scenario:** This issue was observed on AOS-W 6.3.1.1 and is specific to OAW-4550/4650/4750 Series switches. This issue occurred, because the OAW-4x50 Series switch was using multiple replay counters, which the device did not support.
94965	**Symptom:** A OAW-4550 switch crashed. The logs for this error listed the reason for the crash as **datapath timeout**. This issue is resolved by adding a length check to ensure that the Wi-Fi fragments have at least 8 bytes of payload, else the Wifi packed is dropped. **Scenario:** The issue was observed in OAW-4550 switches running AOS-W 6.3.1.1 in a master-local topology.
95588	**Symptom:** GRE tunnel group sessions initiated by remote clients failed. This issue is resolved by redirecting the traffic initiated only by local clients. **Scenario:** This issue was observed when traffic from remote clients was redirected. This issue was observed in switches running AOS-W 6.3 or later.
95927	**Symptom:** Winphone devices were unable to pass traffic as the ARP requests from the devices were considered as ARP spoofs . This issue is resolved by using DHCP binding to verify if the IP address acquired by the device was already used by an old user in the switch and avoid incorrect determination of a valid ARP request as spoof. **Scenario:** This issue was observed when the devices acquired an IP address that was used by an old user earlier on the switch. This issue is not limited to any specific switch model or release version.

Switch-Platform

Table 184: *Switch-Platform Fixed Issues*

Bug ID	Description
82402 84212 86636 87552 89437 90466 91280 93591 94271 94727 95074 95624 95643 95644	**Symptom:** A switch unexpectedly stopped responding and rebooted. The log files for the event listed the reason for the crash as **httpd_wrap process died**. This issue is resolved by introducing a check to verify the validity of the PAPI messages before accepting packets from external PAPIs. **Scenario:** This issue occurred in OAW-4604 switches running AOS-W 6.2.1.0 and later, and triggered by limit set on the size of the data packets used by the internal switch library that managed communication between the switch processes.
91541 94045 95079	**Symptom:** A switch rebooted due to low memory. Changes to the switch software fixed this issue. **Scenario:** This issue occurred when there was a continuous traffic inflow terminating on the control plane. This resulted in an internal component of the AOS-W software to take up high memory. This issue was observed in OAW-4306 Series, OAW-4x04 Series, and OAW-S3 switches running AOS-W 6.1 or later versions.
85685 92814	**Symptom:** OAW-S3 switch stopped responding and rebooted due to an internal memory leak. Internal code changes fixed the memory leak. **Scenario:** This issue occurred after the **show running-config** or **write memory** command was executed on a switch with no static or default routes configured. This issue was observed in OAW-S3 switches running AOS-W 6.2.1.3 or later versions.
93743	**Symptom:** Console access to the switch was lost when the **ping** command was executed in non-privilege mode. The fix ensures that the CLI argument (IP address in this case) passed in the non-privilege mode is not treated as NULL to avoid CLI process crash. **Scenario:** This issue occurred in AOS-W running 6.3 or later.
95044	**Symptom:** All access points went down when the switch to which they were connected rebooted and an error was displayed - **Ancillary image stored on flash is not for this release**. This issue is resolved by writing the boot partition information to the secondary bank of the NVRAM. **Scenario:** This issue occurred when the switch rebooted due to a watchdog reset. This issue is observed only in OAW-4x50 Series switches.

IGMP Snooping

Table 185: *IGMP Snooping Fixed Issues*

Bug ID	Description
93737	**Symptom:** The **ERROR: IGMP configuration failed** error message was displayed when the **IGMP** proxy was configured using the WebUI. This issue is resolved by ensuring that only one of the following radio buttons –**Enable IGMP**, **Snooping**, or **Proxy** under the **Configuration** > **Network** > **IP** > **IP Interface** > **Edit VLAN** page of the WebUI is enabled. **Scenario:** This issue was not limited to any specific switch model or release version.

Licensing

Table 186: *Licensing Fixed Issues*

Bug ID	Description
87424	**Symptom:** The licenses on a standby master switch causing the configuration on the local switch to be lost. Caching the master switch's license limits on the standby switch for a maximum of 30 days resolved this issue. **Scenario:** This issue occurred when the standby comes up before the master after a reboot. This may also occur in an all master-local topology when running AOS-W 6.3 or later.

PPPoE

Table 187: *PPPoE Fixed Issues*

Bug ID	Description
94356	**Symptom:** PPPoE connection with IP NAT inside configuration failed. Changes to the logic that prevented NAT to occur in datapath fixed this issue. **Scenario:** This issue was observed on switches with uplink as a PPPoE interface, and the client VLAN with IP NAT inside.

RADIUS

Table 188: *RADIUS Fixed Issues*

Bug ID	Description
93689	**Symptom:** When clients run a script on their windows phone for 802.1X authentication, the switch sent an **EAP Failure** message. This issue is resolved by removing the EAP-Failure messages when the client timed out during 802.1X authentication. **Scenario:** This issue was not limited to any specific switch model or release version.

Remote AP

Table 189: *Remote AP Fixed Issues*

Bug ID	Description
82015	**Symptom:** An AP associated with a switch did not age out as expected when the heartbeat threshold and interval parameters were modified. Changes in the internal code resolved this issue. **Scenario:** This issue occurred when the heartbeat threshold and interval parameters in the AP's system profile were changed while the AP status was indicated as UP in the switch. This issue was not limited to any specific switch, AP model, or AOS-W release version.
86934	**Symptom:** An AP failed during boot up when the Huawei® modem E1371 was used. This issue was caused by an internal code error when using this modem. The fix ensures that the Remote AP (RAP) does not fail during reboot when using this modem. **Scenario:** This issue was observed in OAW-RAP108 and OAW-RAP109 running AOS-W 6.3.
90355	**Symptom:** OAW-AP70 and OAW-RAP108 access points connecting to the network using a cellular uplink were not able to achieve a 3G connection. This issue is resolved by improvements to the AP boot process, and changes that allow cellular modems to support multiple ports on the AP. **Scenario:** This issue was observed in AOS-W 6.3.0.x and 6.2.0.x, when OAW-AP70 and OAW-RAP108 access points connected to a Huawei® E220 Modem.

Table 189: *Remote AP Fixed Issues*

Bug ID	Description
91292	**Symptom:** A Remote AP (RAP) failed over from backup LMS to primary and did not shutdown wired port. This issue is fixed by ensuring that the wired port is shut down initially when a failover occurs from backup LMS to primary LMS and then reconnects to primary LMS. This ensures that the wired port is enabled and the **DHCP** process is initiated. **Scenario:** This issue occurred when wired clients retained the old IP address retrieved from backup LMS and connected to primary LMS with LMS preemption enabled. This issue was observed in RAPs running AOS-W 6.3.1.0.
94140	**Symptom:** The OAW-IAP whitelist database on the switch did not allow multiple APs in the same branch to share a common remote IP. **Scenario:** This issue was caused by a typecasting error that prevented smaller IP addresses from being allowed.
94703	**Symptom:** The OAW-IAP-VPN connection disconnected intermittently. This issue is resolved by preventing the OAW-IAP database from storing more than six subnets per branch. **Scenario:** This issue was observed when OAW-IAP database had more than six subnets per branch, although a maximum of only six was allowed. OAW-IAP-VPN branch with six subnets exceeded the idle timeout, and when it was up, it had different DHCP profiles which led to more than six subnet entries for the branch in the OAW-IAP database.

SNMP

Table 190: *SNMP Fixed Issues*

Bug ID	Description
94205	**Symptom:** The **sysExtFanSTatus** MIB could not be queried**.** This issue is resolved by initializing the value of the fanCount. **Scenario:** This issue was triggered when the **hwMon** process did not return the proper value for fanStatus SNMP queries. This issue occurred in OAW-4x50 Series switches running AOS-W 6.3.1.1.

Station Management

Table 191: *Station Management Fixed Issues*

Bug ID	Description
85662 84880 88009 88319 89321 91963 92164 93243 93388 93389 93984	**Symptom:** The state of APs were displayed as **down** on the master switch although they were connected and UP. Internal code changes resolved this issue. **Scenario**: This issue was observed when AP's system profile had a local switch as the primary Primary-LMS and master switch was configured as a backup Backup-LMS. This issue was not limited to any specific switch model and occurred in AOS-W running 6.3 or later.

VLAN

Table 192: *VLAN Fixed Issues*

Bug ID	Description
95622	**Symptom:** The even VLAN distribution did not work correctly as the VLAN assignment number and the AP VLAN usage number did not match. The fix ensures that the VLAN assignment and AP VLAN usage numbers match. **Scenario**: This issue was observed in clients that were frequently roaming when even VLAN distribution was enabled. This issue was observed in switches running AOS-W 6.3.1.2.

WebUI

Table 193: *WebUI Fixed Issues*

Bug ID	Description
76439	**Symptom:** When the Spectrum monitor saved in the preference file was not available on the switch, a pop-up was displayed intermittently with the message, **reconnecting**. This pop-up is eliminated by making code level changes. **Scenario**: This issue occurred in AOS-W 6.2.0.0, when OAW-AP105 access point in hybrid AP mode failed to appear as a connected spectrum monitor in the switch WebUI.
90264	**Symptom:** Layer 2 Tunneling Protocol (L2TP) pool was not displayed when the user-role was configured in the WebUI of a switch without an AP license. This issue is fixed by removing the WLAN_REMOTE_AP license validation while configuring L2TP pool. **Scenario:** This issue was triggered by Policy Enforcement Firewall (PEF) license with WLAN_REMOTE_AP validation while configuring L2TP pool on a switch. This issue was not limited to any specific switch model or release version.

Resolved Issues in AOS-W 6.3.1.2

The following issues were resolved in AOS-W 6.3.1.2:

802.1X

Table 194: *802.1X Fixed Issues*

Bug ID	Description
89106	**Symptom**: When previously idle clients reconnected to the network, a configured CLASS attribute was missing from the accounting messages sent from the RADIUS server. This issue is resolved with the introduction of the **delete-keycache** parameter in the 802.1X authentication profile. When this parameter is enabled, it deletes the user keycache when the client's user entries get deleted. This forces the client to complete a full **802.1X authentication** process when the client reconnects after an idle timeout, so the CLASS attributes will again be sent by the RADIUS servers. **Scenario**: This issue occurred in a deployment using RADIUS accounting, where the RADIUS server pushed CLASS attributes in the access-accept messages for 802.1X authentication. When an idle user timed out from the network, AOS-W deleted the CLASS attribute for the user along with rest of the user data.
92564	**Symptom**: Clients experienced authentication failure when they used 802.1 x authentication. This issue is resolved by increasing the stack size. **Scenario**: The issue occurred due to stack overflow which caused memory corruption. This issue was observed in OAW-4306 Series switches and OAW-4x04 Series switches running AOS-W 6.1 and 6.2.

AirGroup

Table 195: *AirGroup Fixed Issues*

Bug ID	Description
88522 92368	**Symptom:** The **multicast Domain Name System (mDNS)** process of AirGroup crashed and restarted in a switch. This issue is resolved by blocking the memory leak to ensure that the switch is not crashing when the maximum number of servers and users supported on each platform is exceeded. **Scenario:** This issue was triggered when the number of AirGroup users exceeded the limit set for the platform. This issue was observed in switches running AOS-W 6.3 or earlier versions.

Air Management-IDS

Table 196: *Air Management-IDS Fixed Issues*

Bug ID	Description
90330	**Symptom**: An adhoc AP marked to be manually contained would not be contained unless the protect from adhoc feature was enabled. This issue is resolved by allowing traditional adhoc containment whenever enhanced adhoc protection is enabled, even if the protect from adhoc feature is not enabled. **Scenario:** This issue was observed in switches running AOS-W 6.2.x.

AP-Datapath

Table 197: *AP-Datapath Fixed Issues*

Bug ID	Description
90645	**Symptom:** The **show datapath session ap-name** command output did not display **ap-name** option. The command output is now displayed correctly even if the **ap-name** parameter is used. **Scenario:** This issue was observed in switches running AOS-W 6.2.1.3 and was not limited to any specific switch model.
94067	**Symptom:** OAW-AP93H access points dropped packets from wired bridge clients whose MTU was below 1498 bytes. **Scenario:** The VLAN in the wired AP is different from the AP's native VLAN. This issue occurred on the OAW-AP93H device connected to switches running any AOS-W version. This issue occurred because the wired driver did not support the extra two bytes used by the internal switch chip.

AP-Platform

Table 198: *AP–Platform Fixed Issues*

Bug ID	Description
86096	**Symptom:** When multiple DNS servers were configured in a local RAP DHCP pool, only the first server in the DNS server list was available to the DHCP client. **Scenario:** This issue was observed in RAPs that were configured to use a local DHCP server and were running AOS-W 6.2 or 6.3. This issue occurred due to incorrect handling of the DNS servers configured by SAPD.
88389 89882 90175 90332	**Symptom:** 802.11n-capable access points unexpectedly rebooted. The log files for the event listed the reason for the reboot as **kernel page fault**. Improvements in the wireless driver of the AP resolved this issue. **Scenario:** This issue was observed when an 802.11n-capable campus AP was in bridge forwarding mode and there was a connectivity issue between the AP and the switch. This issue was observed in 802.11n-capable access points running any version of AOS-W.
89041	**Symptom:** A 802.11n-capable access point unexpectedly rebooted or failed to respond. This issue was resolved by improvements to the wireless drivers in AOS-W 6.3.1.1. **Scenario**: This issue was observed when a client disconnected from the network. The issue occurred on 802.11n access points running AOS-W 6.3.0.1.
89016	**Symptom**: The SNMP OID **wlanStaAccessPointESSID** had no value when a client roamed from a down AP to an active AP. Improvements to internal processes that managed Layer-2 roaming resolved this issue. **Scenario**: This issue was observed in switches running AOS-W 6.2, when clients roamed between APs.
89691 94047	**Symptom**: APs stopped responding and rebooted. The log files for the event listed the reason for the crash as **kernel page fault**. A change in the route cache has fixed this issue. **Scenario**: This issue occurred when the deletion of the route cache was interrupted. This issue was not limited to any specific switch model or release version.
91803	**Symptom**: The OAW-AP120 failed due to insufficient memory caused by heavy traffic. Improvements to the wireless drivers resolved this issue. **Scenario**: This issue was observed in OAW-AP120 connected to switches running AOS-W 6.3.1.0
91820	**Symptom:** An AP crashed and rebooted frequently and the log file for the event listed the reason for the reboot as **Kernel Panic**. Updates to the wireless driver fixed this issue. **Scenario:** This issue occurred while receiving and freeing the buffer memory. This issue was observed in OAW-AP135 access points running AOS-W 6.3.1.0.
91937	**Symptom:** OAW-AP92 and OAW-AP93 access points were unable to come up with AOS-W 6.3.x.x-FIPS. AOS-W 6.3.x.x-FIPS now supports OAW-AP92 and OAW-AP93 access points. **Scenario:** When upgrading to AOS-W 6.3.x.x.-FIPS, the image size was too big to fit into OAW-AP92's or OAW-AP93's 8 MB flash, and hence was rejecting these access points to come up although these access points required to be supported with 16 MB flash. **NOTE:** Due to the infrastructure limitation, to support 16 MB flash, the code block for 8 MB flash had to be removed as well. So, OAW-AP92 and OAW-AP93 access points with 8 MB flash will also come up with AOS-W 6.3.x.x-FIPS but it is not supported. Only OAW-AP92 and OAW-AP93 access points with 16 MB flash is supported with AOS-W 6.3.x.x-FIPS.
91963	**Symptom:** An AP rebootstrapped with the **Wrong cookie in request** error after a failover from one switch to other. This issue is fixed by enhancements to drop the error message if an AP detected a cookie mismatch when the error message came from a different switch than the current LMS. **Scenario:** This issue occurred after a failover of an AP from one switch to other and when the AP received the messages from old switch and incorrectly identified as a cookie mismatch. This issue was observed in switches in a master-local topology with a primary and backup LMS configured.

Table 198: *AP–Platform Fixed Issues*

Bug ID	Description
89514 92163 93504	**Symptom:** OAW-AP220 Series access point rebooted repeatedly when connected to a Power over Ethernet (PoE) switch, without storing a reboot reason code in the flash memory of the AP. Design changes to the OAW-AP220 Series code fixed this issue. **Scenario:** This issue was observed in OAW-AP220 Series running AOS-W 6.3.x and later versions.
92245	**Symptom:** An AP does not respond and displays an error message - **aruba_valid_rx_sig: Freed packet on list at ath_rx_tasklet+0x138/0x2880.....** A manual power cycle was required to restore the AP to the normal status. This issue is resolved by adding an assertion. **Scenario:** This issue was observed in OAW-AP125 access points connected to switches running AOS-W 6.3.1.
92572	**Symptom:** APs stopped responding and crashed due to a higher utilization of memory caused by the client traffic. A change in the AP memory management has resolved this issue. **Scenario:** This issue was observed in AOS-W 6.2 and later versions, but was not limited to any specific switch model.
93067	**Symptom:** The authorization for users was unexpectedly revoked and the **show ap client trail-info** CLI command displayed the reason as **Ptk Challenge Failed**. Sending the Extensible Authentication Protocol over LAN (EAPoL) packets as best effort traffic instead of voice traffic resolved this issue. **Scenario:** This issue was observed in OAW-AP220 Series access points running AOS-W 6.3.1.1 when the virtual AP is configured with WPA-802.1X-AES encryption.

AP-Regulatory

Table 199: *AP-Regulatory Fixed Issues*

Bug ID	Description
86764	**Symptom**: The output of the **show ap allowed channels** command incorrectly indicated that OAW-AP68 and OAW-AP68P supported 5 GHZ channels. This issue is resolved by modifying the output displayed for the allowed channel list for OAW-AP68 and OAW-AP68P APs. **Scenario:** This issue was observed in OAW-AP68 and OAW-AP68P running AOS-W 6.1.x.x and 6.2.x.x.

AP-Wireless

Table 200: *AP-Wireless Fixed Issues*

Bug ID	Description
67847 69062 69346	**Symptom:** APs unexpectedly rebooted and the log files listed the reason for reboot as **Data BUS error**. A change in the exception handling module has fixed this issue. **Scenario:** This issue was observed in the OAW-AP120 Series and OAW-AP68P connected to switches running AOS-W 6.3.1.2. **Duplicate Bugs:** 71530, 74352, 74687, 74792, 75212, 75792, 75944, 76142, 76217, 76715, 77273, 77275, 78118, 80735, 83242, 83243, 83244, 83624, 83833, 84170, 84339, 84511, 85015, 85054, 85086, 85367, 85959, 88515, 89136, 89253, 89256, 89816, 90603, 91084, 92871, 9287, 92878, 92879, 93923.
69424 75874 78978 78981 79891 80054 87250 88619 88620 88989 89537 91689 93455 93811	**Symptom:** When upgraded to AOS-W 6.2, OAW-AP125 crashed and rebooted. Reallocating the AOS-W loading address in memory fixed the issue. **Scenario:** This issue was observed when switches were upgraded to AOS-W 6.2 from AOS-W 6.1.3.2 and later in any deployment with OAW-AP125.
88741	**Symptom:** The degradation in performance occurred due to settings made in the preferred-access. **Scenario:** This issue was caused by an internal AOS-W malfunction and was observed only in OAW-AP225.
88328 89623	**Symptom:** Wireless clients experienced packet loss when connected to remote APs in bridge mode. The fix ensures that some buffer is reserved for transmitting unicast traffic. **Scenario:** This issue was observed in OAW-AP105 access points connected to switches running AOS-W 6.1.3.8 when there was a heavy multicast or broadcast traffic in the network.
89442	**Symptom:** The OAW-AP220 Series devices crashed frequently. **Scenario:** This issue occurred when the radio mode was altered between Monitor and Infrastructure. This issue was observed only in OAW-AP220 Series devices running AOS-W 6.3.1.2.
89460	**Symptom:** When APs used adjacent DFS channels, the OAW-AP135 falsely detected RADAR and exhausted all DFS channels. If no non-DFS were enabled, the AP stopped responding to clients. **Scenario:** This issue was observed in OAW-AP135 running AOS-W 6.3.x and 6.2.x. It was caused when APs used adjacent DFS channels.
89735 89970 90572 91140 91560 91620 92017 92428 93373	**Symptom:** The Ethernet interface of an 802.11ac capable AP restarted frequently. Changes in the internal code fixed this issue. **Scenario:** This issue was observed in OAW-AP220 Series connected to switches running AOS-W 6.3.1.0 and later version.
90065	**Symptom:** OAW-AP125 rebooted unexpectedly. Improvements to the wireless driver has resolved this issue. **Scenario:** This issue was observed in OAW-AP125 access points connected to switches running AOS-W 6.1.3.9.

Table 200: *AP-Wireless Fixed Issues*

Bug ID	Description
90960	**Symptom**: Microsoft® Surface Pro and Surface RT clients were unable to acquire an IP address or correctly populate the ARP table with a MAC address when connecting to an AP using 20 MHz channels on 2.4 GHz or 5 GHz radios. This issue is resolved by channel scanning improvements to APs in 20 MHz mode. **Scenario**: This issue was triggered when Microsoft Surface clients running Windows 8 or Windows 8.1 connected to 20 MHz APs running AOS-W 6.1.3.8.
91379	**Symptom:** OAW-AP220 Series access points unexpectedly crashed. Using the correct structure to fill the information in the outgoing response frame resolved this issue. **Scenario:** The 802.11k enabled client that sent a Neighbor Report Request frame caused the OAW-AP220 Series to crash when the packet was freed. This issue was observed in OAW-AP220 Series running AOS-W 6.3.x.
91856	**Symptom:** Certain 802.11b clients did not communicate with 802.11n-capable access points. Improvements to the wireless driver of 802.11n-capable access points resolved the issue. **Scenario:** This issue was observed when Denso® 802.11b handy terminals communicated with 802.11n-capable access points on channel 7. This issue was not limited to a specific switch model or release version.
91946 92052 92550 92552 92554 92555 92557 92559 92561 92562 92788 92976 92977	**Symptom:** OAW-AP135 stopped responding and rebooted. Improvements to the wireless driver in AOS-W 6.1.3.2 resolved the issue. **Scenario:** This issue occurred when the buffer was corrupted in the wireless driver. This issue was observed in OAW-AP135 access points connected to switches running AOS-W 6.3.1.0.
92346	**Symptom:** When the 80 MHz option in the rf arm-profile was enabled or disabled, HT Capabilities in the beacon showed only 20 MHz support. This issue was resolved by ensuring that the profile enable and disable function operates properly **Scenario:** This issue was observed in OAW-AP225 access points connected to switches running AOS-W 6.3.1.0.
92626	**Symptom:** An AP crashed and the log files for the event listed the reason for the crash as **kernel panic**. This issue was fixed by referencing the valid memory. **Scenario:** This issue occurred when an invalid memory was referenced. This issue occurred in OAW-AP220 Series access points running AOS-W 6.3.1.1.

Table 200: *AP-Wireless Fixed Issues*

Bug ID	Description
93710	**Symptom:** Vocera clients associated to an AP were unable to communicate with the Vocera server. This issue was resolved by limiting the multicast transmission rate so that the unicast transmission is not affected. **Scenario:** This issue occurred when multicast traffic blocked hardware and software queues resulting in unicast packets being dropped. This issue is observed in OAW-AP225 connected to switches running AOS-W 6.3.1.1.
94059 94520 95057 95106 95107	**Symptom:** An AP rebooted due to unhandled kernel unaligned access. **Scenario:** This issue was observed in OAW-AP120 Series access points when the switches were upgraded from AOS-W 6.1.3.7 to 6.1.3.9, but is not limited to any specific switch model.
94155	**Symptom:** OAW-AP225 device rebooted unexpectedly when connected to a PoE. This issue was resolved by making code level changes in the index table. **Scenario:** This issue occurred due to the drastic peak in power when OAW-AP225 is connected to 3af PoE (Power over Ethernet) and operates in low-power mode. This issue was observed in OAW-AP225 connected to switches running AOS-W.

Base OS Security

Table 201: *Base OS Security Fixed Issues*

Bug ID	Description
86141 93351 93726	**Symptom:** Issuing the **show global-user-table list** command displayed duplicate client information. Ignoring the master switch IP query in LMS list fixed the issue. **Scenario:** This issue was observed in a VRRP or master-local deployment whereby the master switch queried itself and the LMS list resulting in duplicate client information. This issue was observed in switches running AOS-W 6.3.X.0.
89453	**Symptom**: The show rights command did not display all the user roles configured in the switch. This issue is resolved by a change that ensures that the output of this command displays all the user roles configured on the switch. **Scenario**: This issue was observed when more than 50 user roles were configured in a switch running AOS-W 6.2.1.3.
89676	**Symptom:** Users could not authenticate to the TACACS server as TCP handshake failed and the aaa-test-server with TACAS displayed two different messages - **auth module busy** and **authentication is successful** for the same switch running a similar image version. **Scenario**: This issue was observed in switches running AOS-W 6.1.3.7 or 6.4, but is not limited to a specific hardware model.
90180	**Symptom:** Re-authentication of the management users was not triggered upon password change. The users are now getting **Password changed, please re-authenticate** message on the console, forcing the user to login again with the new password. **Scenario**: The issue was observed when users were already connected, and password for these users was changed. The re-authentication message for these users was not shown. This issue was not limited to any specific switch model or AOS-W version.
90209	**Symptom:** A switch rebooted unexpectedly due to an internal process (datapath) timeout. **Scenario:** The timeout occurred due to a VIA client sending an SSL fallback packet, where the third SSL record encapsulating the IPSec packet had an invalid IP header. was limited to a specific switch model and was observed in AOS-W 6.2.1.2.

Table 201: *Base OS Security Fixed Issues*

Bug ID	Description
90233	**Symptom:** Clients with a logon user role did not age out from the user-table after the logon-lifetime AAA timer expired. This issue was resolved by changing the aged out users to logon users if User Derivation Rule (UDR) is configured in the AAA profile. **Scenario:** This issue was observed when UDR was configured in the AAA profile with logon defined as the default user role. This issue was observed in switches running AOS-W 6.2.1.x.
90454	**Symptom**: A remote AP unexpectedly rebooted, because it failed to receive heartbeat responses from the switch. Changes to the order in which new IPsec Security Associations (SAs) are added and older IPsec SAs are removed resolved this issue. **Scenario**: This issue occurred after a random IPsec rekey was triggered and when the outbound IPsec SA was deleted before the inbound IPsec SA was added. This removed the route cache for the inner IP, causing the session entry to incorrectly point to the default gateway, and prevent heartbeat responses from reaching the AP.
92674	**Symptom:** The CLASS attribute was missing in Accounting STOP packet. This issue is resolved by not resetting the counters when an IPv6 user entry is deleted. **Scenario:** This issue occurred when the counters were reset during an IPv6 user entry aged out. This issue was not limited to a specific switch or AOS-W version.
92817	**Symptom:** Wireless clients were blacklisted even when the rate of the IP Session did not exceed the threshold value set. This issue is resolved by increasing the storage of the threshold to16 bits. **Scenario:** This issue was observed when the threshold of the IP Session rate was set to a value greater than 255. This issue was observed in switches running AOS-W 6.x.

Captive Portal

Table 202: *Captive Portal Fixed Issues*

Bug ID	Description
87294 87589 92575	**Symptom:** Captive Portal (CP) whitelist that was mapped to the user-role was not synchronized with the standby switch. Checks in the CP whitelist database fixed this issue. **Scenario:** This issue was observed when a net-destination was created and added to the CP profile whitelist that mapped to the user-role in the master switch. This issue was observed in AOS-W 6.2.1.2 and not limited to a specific switch model.
91442	**Symptom:** In the **Login** page using the master switch's command line interface, the question mark symbol was neither getting pushed nor getting added to the local switch. This issue is resolved by ensuring the question mark symbol is accepted by the command line interface of the master switch. **Scenario:** This issue was observed while synchronizing the configuration from the master switch to the local switch.

Switch-Datapath

Table 203: *Switch-Datapath Fixed Issues*

Bug ID	Description
88469	**Symptom:** A switch denied any FTP download that used Extended Passive mode over IPv4. Modifying the FTP ALG to handle Extended Passive mode correctly resolved this issue. **Scenario:** This issue was observed when an IPv4 FTP client used Extended Passive mode. In such a case, the FTP ALG on the switch detected it as a Bounce Attack and denied the session. This issue was not limited to a specific switch model or release version.
93423	**Symptom:** A switch unexpectedly rebooted and the log file listed the reason for the reboot as **Datapath timeout**. This issue is fixed by increasing the stack memory size in the data plane. **Scenario:** This issue was observed when clients using SSL VPN connected to RAP and the switch tried to decompress these packets. This issue was not limited to a specific switch model or a release version.

Switch-Platform

Table 204: *Switch-Platform Fixed Issues*

Bug ID	Description
82736 82875 83329	**Symptom:** A switch rebooted unexpectedly. Changes in the watchdog implementation on the switch resolved the issue. **Scenario:** Log files for the event indicated the reasons for the reboot as **soft watchdog reset** or **user pushed reset**. This issue was identified in AOS-W 6.1.3.x, and is not limited to a specific switch model. **Duplicate Bugs:** 83502, 83762, 84022, 85355, 85370, 85628, 86005, 86029, 86031, 86572, 87410, 87505, 87587, 88005, 88332, 88351, 88434, 88921, 89636, 89818, 90909, 91269, 91308, 91370, 91517, 92823, 93294, 93770
86216 85566 87090	**Symptom:** During a kernel panic or crash, the panic dump generated by the switch was empty. New infrastructure has been added to improve the collection of crash dumps. **Scenario:** This issue impacts OAW-4x04 Series, OAW-4306 Series, and OAW-S3 switches and was observed on AOS-W 6.1.3.7. **Duplicate Bugs:** 87635, 88321, 88387, 88699, 89436, 89727, 89839, 89911, 90162, 90338, 90481, 91193, 91387, 91941, 92139, 92187, 92516, 92808, 93630, 93693, 93931, 94308.
89155	**Symptom**: OAW-4306 Series switches experienced high level of CPU usage during bootup, which triggered a warning message - **Resource Controlpath CPU has exceeded 30% threshold.** This issue is resolved by changes to the internal CPU threshold that reflects the expected CPU usage levels. **Scenario**: This issue was observed in switches running AOS-W 6.1.2.3.
90619 92250	**Symptom:** The switch WebUI stopped responding indefinitely. The fix ensures that the OmniVista query fails if there is no firewall visibility. **Scenario:** This issue occurred when OmniVista queried for firewall visibility details from a switch on which the firewall visibility feature was disabled. This issue was observed in switches running AOS-W 6.2 or later.
91383	**Symptom**: Executing a **show** command causes the switch command-line interface to display an error: **Module Configuration Manager is busy. Please try later**. Improvements to how the switch manages HTTP session keys resolved this issue. **Scenario**: This issue occurred when issuing **show** commands from the command-line interface of a OAW-4x04 Series standby switch, and is triggered when the database synchronization process attempts to simultaneously replace and add an HTTP session key in the user database.

DHCP

Table 205: *DHCP Fixed Issues*

Bug ID	Description
90611	**Symptom:** The Dynamic Host Configuration Protocol (DHCP) module crashed on a switch and users were not able to perform a new DHCP configuration. The updates to the DHCP wrapper fixed this issue in AOS-W 6.3.1.2. **Scenario:** This issue was triggered by a race condition that caused the DHCP wrapper process to crash with continuous restarts. This issue was not specific to a switch model or release version.

GRE

Table 206: *GRE Fixed Issues*

Bug ID	Description
89832	**Symptom:** Layer 2 Generic Routing Encapsulation (L2 GRE) tunnel between L2 connected switches dropped because of keepalive failures. This issue is fixed by bridging the packets before routing to the forwarding pipeline. **Scenario:** This issue occurred when the GRE tunnel keepalives were enabled and the **Configuration > Network > IP > IP Interface > Edit VLAN (1) > Enable Inter-VLAN Routing** option was disabled. This issue was observed in switches running AOS-W 6.3 configured with L2 GRE tunnel between L2 connected switches.

GSM

Table 207: *GSM Fixed Issues*

Bug ID	Description
91870	**Symptom:** The output of the **show ap database** command indicated that a OAW-RAP5 was inactive and that the OAW-RAP5 would not come up. This issue is resolved by increasing the allocation for AP wired ports to 16x. **Scenario:** This issue was observed with OAW-RAP5 APs when all four wired AP ports were enabled in AOS-W 6.3. AOS-W 6.3 introduced GSM where space was pre-allocated for the AP wired ports based on the maximum number of APs times the maximum number of wired ports, because OAW-RAP5 has four wired ports and the switch allowed four times the campus APs. As a result, the number of GSM slots was insufficient.

Hardware-Management

Table 208: *Hardware-Management Fixed Issues*

Bug ID	Description
87481	**Symptom:** The OAW-4550/4650/4750 Series switches failed to generate the switch's internal temperature. Setting the SNMP attribute for temperature in OAW-4550/4650/4750 Series switches fixed this issue. **Scenario:** This issue was observed when an SNMP walk was performed using the OID.1.3.6.1.4.1.14823.2.2.1.2.1.10. This issue was observed in OAW-4550/4650/4750 Series switches running AOS-W 6.3 or later.

IPv6

Table 209: *IPv6 Fixed Issues*

Bug ID	Description
88814	**Symptom:** When clients connected to a switch, they received IPV6 router advertisements from VLANs that they were not associated with. This issue is resolved by updating the datapath with router advertisements conversion flag, so that datapath converts multicast router advertisements to unicast. **Scenario:** This issue was observed in IPv6 networks with derived VLANs and was not limited to a specific switch model or release version.

Licensing

Table 210: *Licensing Fixed Issues*

Bug ID	Description
89294	**Symptom:** RAPs were unable to come up on a standby switch if the AP licenses were installed only on the master switch. **Scenario:** This issue occurred when centralized licensing was enabled and all AP licenses were installed on the master switch and the RAP feature was disabled on the standby switch. This issue was observed in switches running AOS-W 6.3.

Local Database

Table 211: *Local Database Fixed Issues*

Bug ID	Description
88019	**Symptom:** A warning message **WARNING: This switch has RAP whitelist data stored in pre-6.3 format, which is consuming .....running the command local-userdb-ap del all** appeared, when a user logged in to the switch. This issue is fixed by deleting the warning file, when all the old entries are deleted. **Scenario:** This issue occurred when a switch was upgraded from a previous version of AOS-W to 6.3 or later versions. This issue was not specific to a switch model or release version.

Master-Redundancy

Table 212: *Master-Redundancy Fixed Issues*

Bug ID	Description
80041	**Symptom:** Master-Backup database fails to synchronize with the reason **Last failure cause: Standby switch did not respond to the start request or is not ready**. This issue was resolved by ignoring any aborted database synchronization sequence number on the master switch, so that the subsequent database synchronization can proceed without waiting for a response from the standby switch for the previous aborted database sync. **Scenario:** The standby switch database was out-of-sync with the master switch and any switchover during out-of-sync state caused the switch to be in an inconsistent state. This issue was observed in switches in a master-standby configuration and was not specific to a release version.

Mesh

Table 213: *Mesh Fixed Issues*

Bug ID	Description
92614	**Symptom:** A Mesh Point rebooted frequently as it could not connect to a Mesh Portal. This issue was resolved by allowing Mesh Point to use the configured power for transmitting probe requests instead of reduced power. **Scenario:** This issue occurred when the transmission power on the Mesh Point was very low compared to the configured power. This issue was observed in OAW-AP105 and OAW-AP175 connected to switches running AOS-W 6.1.x or later versions.

Mobility

Table 214: *Mobility Fixed Issues*

Bug ID	Description
88281	**Symptom:** IP mobility entries were not cleared even when the client leaves the switch and user entries aged out. Additionally, the command **clear ip mobile host <mac-address>** did not clear the stale entry. **Scenario:** This issue was caused by a message loss between the switch's Mobile IP and authentication internal processes. Due to the message loss, the affected clients were blocked. This issue was observed in switches running AOS-W 6.3.x, 6.2.x, and 6.1.x.

Remote AP

Table 215: *Remote AP Fixed Issues*

Bug ID	Description
86650	**Symptom:** A switch sent continuous RADIUS requests for the clients connected behind wired port of a remote AP (RAP). This issue is resolved by enhancing the code for memory corruption. **Scenario:** This issue was observed when the RAP used PPPoE uplink and wired AP was operating in split-tunnel or bridge mode. This issue occurred in switches running AOS-W 6.1.3.6 or later and was not limited to a specific switch model.
91106	**Symptom:** When a Remote Access Point (RAP) was rebooted from the switch using the **apboot** command, the system did not generate a log message. Changes to the internal code for handling log messages fixed this issue. **Scenario:** This issue was observed in RAPs running AOS-W 6.1 and later versions.

SNMP

Table 216: *SNMP Fixed Issues*

Bug ID	Description
83948	**Symptom:** The Simple Network Management Protocol (SNMP) module crashed when the management interface was deactivated while an SNMP query was running. A build option was modified to avoid generating code that may access invalid memory. **Scenario:** This issue was observed when SNMP was enabled and was used to monitor OAW-4306 and OAW-4704 switches running AOS-W 6.3.0.0.

Station Management

Table 217: *Station Management Fixed Issues*

Bug ID	Description
86357	**Symptom:** Station Down messages were not logged in the syslog. Changes to the syslog messaging resolved this issue. **Scenario:** This issue was observed in switches running AOS-W 6.3.x.
66261	**Symptom**: A client moving from one virtual AP (VAP) to another could not connect to the new virtual AP. Changes to how AOS-W allocates VLANs resolve this issue. **Scenario**: This issue occurred when the **even VLAN** and **preserve VLAN** features were enabled in both VAPs, and if the client VLAN defined in the previous VAP did not exist in the new VAP. This issue was first observed in AOS-W 6.1.3.x, and was not limited to any specific switch model.

Voice

Table 218: *Voice Fixed Issues*

Bug ID	Description
77716 88996 90000	**Symptom:** Incompatibility issues were observed between OAW-4704 switch and a Cisco CUCM using SCCP version 20. Users were able to make and receive calls using a Cisco phone but there was no audio. This issue is resolved by changes that allow the switch to handle Open Receive Channel Acknowledge (ORCA) messages for SCCP Version 20. **Scenario:** The Cisco CUCM was compatible with the Skinny Client Control Protocol (SCCP) version 20, while the OAW-4704 switch supported only up to version 17 of the SCCP. This incompatibility issue resulted in media traffic not passing through the OAW-4704 switch as the switch was not able to parse the SCCP signaling packets. This issue was observed in a OAW-4704 switch running AOS-W 6.0 or later.
86135 87296 88314 88891 89170 89893 90613 91073 91625 92159	**Symptom:** The Station Management (STM) module on a OAW-4750 local switch configured with voice ALGs stopped responding and restarted after idle voice clients aged out. This caused network disruption. This issue is resolved by making code level changes to avoid creation of voice clients with invalid MAC addresses. **Scenario:** This issue occurred in switches running AOS-W 6.3.1.0 where AP entries were created as voice clients with invalid MAC address.
86683	**Symptom:** The **show voice call-cdrs** and **show voice client-status** command outputs did not display the call details for Lync wired clients with media classification configured on session ACL. This issue is resolved by handling the message appropriately for wired clients. **Scenario**: This issue was observed when Lync clients were identified as voice clients using media classification. This issue occurred in AOS-W 6.2 and 6.3 versions, and was not limited to any specific switch version.
88998 90912	**Symptom:**Switches stopped responding and rebooted due to lack of memory resulting in network disruptions. Enhancements to memory allocation resolved this issue. **Scenario:** The issue occurred when an internal module (STM) crashed due to memory corruption. This issue was observed in switches running AOS-W 6.1 and later.
93517	**Symptom:** Access points rebooted unexpectedly resulting in wireless clients to lose network connectivity. Releasing CDR events for AP statistics and AP event in the CDR buffer resolved the issue. **Scenario:** This issue was observed in a VoIP deployment when the **Station Management (STM)** process that handles AP management and user association crashed on the switch. This issue was observed in switches running AOS-W 6.1 and later versions.

WebUI

Table 219: *WebUI Fixed Issues*

Bug ID	Description
88398	**Symptom:** Network administrators were unable to manually contain or reclassify a group of detected rogue APs in the **Dashboard** > **Security** page of the WebUI. This issue is fixed by adding support to classify multiple rouge APs. **Scenario:** This issue occurred when multiple rogue APs were selected in the **Dashboard** > **Security** page. This issue was observed in switches running AOS-W 6.2.1.3.
88802 91141	**Symptom:** When the client tried to access the **Air Group** option from the Web UI, the system did not respond. To resolve this issue, the **Air Group** option is now removed from the WebUI for OAW-4306 Series switches. **Scenario:** This issue was observed in OAW-4306 Series switches running AOS-W 6.3.x.
89225	**Symptom:** Configuration of a mgmt-server (ALE or OmniVista) using the WebUI was not supported. This issue is resolved by using the CLI to configure mgmt-servers. **Scenario:** This issue was observed in AOS-W 6.3.1.0 but not limited to a specific switch model.
90110	**Symptom:** The AOS-W Campus WLAN Wizard was not accessible. This issue is resolved by changing the LDAP server filter to include an ampersand. **Scenario:** The Campus WLAN wizard was not accessible due to the presence of an ampersand (&) in the LDAP server filter. This issue was observed in a OAW-4306G switch running AOS-W 6.2.1.3, but could impact any switch model.
92340 92649	**Symptom:** WebUI of the switch failed to load in Microsoft® Internet Explorer 11 with the error message **can't create XMLHttpRequest object: Object doesn't support property or method creatXMLHttpRequest**. The AOS-W WebUI is updated to be compatible with Microsoft® Internet Explorer 11. **Scenario:** This issue was not limited to a specific switch model or AOS-W release version.
93606 93718	**Symptom:** Clients were not displayed in the **Monitoring** > **Switch** > **Clients** page of the WebUI when filtered with AP Name. This issue is fixed by changing the **show user-table location <ap-name>** command to **show user-table ap-name <ap-name>**. **Scenario:** This issue was triggered by changes to CLI commands. This issue was observed in switches running AOS-W 6.2 and 6.3.

Resolved Issues in AOS-W 6.3.1.1

The following issues were resolved in AOS-W 6.3.1.1:

AP-Platform

Table 220: *AP–Platform Fixed Issues*

Bug ID	Description
89041	**Symptom:** 802.11n capable access points unexpectedly rebooted or failed to respond. This issue was resolved by improvements to the wireless drivers in AOS-W 6.3.1.1. **Scenario:** This issue was observed when a client disconnected from the network. The issue occurred on 802.11n access points running AOS-W 6.3.0.1.
89042	**Symptom**: An access point crashed and rebooted frequently, and the log files for the event listed the reason for the crash as **kernel panic**. This issue was resolved by improvements to the wireless drivers in AOS-W 6.3.1.1. **Scenario:** This issue was observed in 802.11n access points running AOS-W 6.3.0.1.
89043 89054 89045	**Symptom:** 802.11n capable access points unexpectedly rebooted or failed to respond. This issue was resolved by making improvements to the wireless drivers in AOS-W 6.3.1.1. **Scenario:** This issue was observed on 802.11n-capable access points running AOS-W 6.3.0.1.
89717	**Symptom:** The 802.11 APs had been malfunctioning. **Scenario:** This issue was observed on 802.11n APs and AOS-W 6.3.0.1. This issue no longer occurs as the wireless driver has been upgraded.
89898	**Symptom:** The OAW-AP120 Series APs malfunctioned due to low memory. **Scenario:** This issue was observed on OAW-AP120 Series APs. This issue no longer occurs as the wireless driver has been upgraded.
90934 89137 90021 90495 90604 91016 91392 91393	**Symptom**: Access points unexpectedly stopped responding and rebooted. Log files for the event listed the reason for the crash as **kernel panic** or **kernel page fault**. This issue was resolved by improvements to the wireless drivers in AOS-W 6.3.1.1. **Scenario**: This issue was observed in 802.11n access points such as OAW-AP125, OAW-AP134, and OAW-AP105 running AOS-W 6.3.0.1.

AP-Wireless

Table 221: *AP-Wireless Fixed Issues*

Bug ID	Description
88631 88044 88569 88843 89044 89046 89053 89058 89325 89326 89811 89901 90890	**Symptom:** An access point continuously stopped responding and rebooted. This issue was resolved by making improvements to the wireless drivers in AOS-W 6.3.1.1. **Scenario:** This issue was observed in OAW-AP220 Series running AOS-W 6.3.0.1 when the clients disconnected from the network.
88771 88772 91086	**Symptom:** 802.11n capable access points stopped responding and rebooted. The log files for the event listed the reason for the crash as **kernel page fault**. This issue was resolved by improvements to the wireless drivers in AOS-W 6.3.1.1. **Scenario**: This issue was observed only in 802.11n capable access points running AOS-W 6.3.0.1.
91163 91315 91380 91468 91492 91516 91557	**Symptom:** An access point continuously rebooted. This issue was resolved by improvements to the wireless drivers in AOS-W 6.3.1.1. **Scenario:** This issue occurred when the clients disconnected from the network. This issue was observed in OAW-AP220 Series access points running AOS-W 6.3.1.0.
91373	**Symptom**: MacBook clients were unable to pass traffic on the network. This issue was resolved by changes to AOS-W that require APs to send data frames to all connected clients. **Scenario**: This issue was observed in OAW-AP220 Series access points that were upgraded to AOS-W 6.3.1.0, and was triggered by virtual APs being enabled or disabled, either manually (by network administrators) or automatically, as a part of the regular AP startup process.
91374	**Symptom:** Wireless clients observed high latency when associated to 802.11ac capable access points. Enhancements to the Broadcom driver of the access point fixed this issue. **Scenario:** This issue was observed in OAW-AP225 running AOS-W 6.3.0.1. This issue occurred when the wireless client went into power-save mode.

Switch-Platform

Table 222: *Switch–Platform Fixed Issues*

Bug ID	Description
90751 90633 90863 91154 91138 91474 91656	**Symptom:** Switches continuously stopped responding and rebooted. Enhancements to memory allocation resolved this issue. **Scenario:** The issue occurred when an internal module (FPCLI) crashed due to memory corruption. This issue was observed in OAW-S3 switches and is not limited to a specific AOS-W version.

Resolved Issues in AOS-W 6.3.1.0

The following issues were resolved in AOS-W 6.3.1.0:

802.1X

Table 223: *802.1X Fixed Issues*

Bug ID	Description
86162	**Symptom**: Users experienced authentication failures with WPA2-PEAP. **Scenario**: This issue was triggered by some 2k server certificates. This issue was observed on OAW-6000 Series switches platforms with XLR/XLS processors, OAW-4x04 Series, and OAW-4306 Series switches running AOS-W 6.x.

AirGroup

Table 224: *AirGroup Fixed Issues*

Bug ID	Description
88239	**Symptom:** The command-line interface and the WebUI was not accessible on a switch when a large number of users supported multicast Domain Name System (mDNS) on the network and advertised different mDNS service IDs. This issue has not affected the client connectivity. This issue is fixed by upgrading to AOS-W 6.3.1.0. **Scenario:** This issue occurred only when the **AirGroup Status** parameter was enabled in the **Configuration > Advanced Services > AirGroup > AirGroup Settings** tab of the WebUI with a large number (above 400) of AirGroup service IDs listed under **allowall** service. This issue was observed in switches running AOS-W 6.3.

Air Management - IDS

Table 225: *Air Management-IDS Fixed Issues*

Bug ID	Description
75039 77380	**Symptom**: OAW-AP224 and OAW-AP225 access points generated frequent false Intrusion Detection System (IDS) alarm **Beacon Frame With Incorrect Channel**. Changes to the internal code of OAW-AP224 and OAW-AP225 access points fixed the issue. **Scenario**: Due to the way OAW-AP224 and OAW-AP225 access points scan a channel, it received frames from an alternate channel in the 80 MHz channel set. This triggered a false IDS alarm. This issue was observed in OAW-AP224 and OAW-AP225 access points running AOS-W 6.3.

AP-Datapath

Table 226: *AP-Datapath Fixed Issues*

Bug ID	Description
85279	**Symptom:** In a Master-local setup, all the users connected in bridge or split tunnel mode experienced a low throughput when no bandwidth contracts were configured. **Scenario:** This issue occurred on switches running AOS-W 6.2 or later due to incorrect mapping of the role to bandwidth contract when the ACL IDs in the master and local switches were different for the same role. It was also observed during an authentication process restart.

AP-Platform

Table 227: *AP-Platform Fixed Issues*

Bug ID	Description
78289	**Symptom:** Crashes observed in the kernel in the node leave path, when the STA is disconnected. This issue is fixed by using appropriate reference counter protection. **Scenario:** This issue was triggered by aggressive STATION roams and power saves. This issue is not specific to any AP model and release version.
87359	**Symptom:** Users were unable to connect to the OAW-AP225 every few hours. **Scenario:** Enabling the 802.11k feature caused this issue. The action frame was not freed up in the driver sent by the AP. This caused outstanding data frames in the driver to be dropped if the count exceeded a threshold. This issue was observed on the OAW-AP225 and release version AOS-W 6.3.

AP-Wireless

Table 228: *AP-Wireless Fixed Issues*

Bug ID	Description
88227 88286 88449 88509 88510 88561 88765 88767 88768 88770 88773 89133	**Symptom:** OAW-AP125 stopped responding and rebooted due to lack of memory when the traffic was heavy. This issue is resolved by removing lldp support on OAW-AP125, thereby reducing the memory consumed. **Scenario:** This issue was observed only on OAW-AP125.
88282	**Symptom:** OAW-AP225 running AOS-W 6.3.0.1 stopped responding and rebooted. The log files for the event listed the reason for the crash as **kernel panic: Fatal exception**. Changes to the internal code fixed this issue. **Scenario:** This issue occurred in a master-local OAW-4550/4650/4750 Series switch topology where the OAW-AP225 terminated on both the switches in a campus mode.
86063	**Symptom:** The Max Tx Fail feature was not supported on the OAW-AP220 Series in AOS-W 6.3. **Scenario:** When a user attempted to enable Max Tx Fail, the feature did not work on the OAW-AP220 Series in AOS-W 6.3. This feature has now been implemented.
87890	**Symptom:** The Service Set Identifier (SSID) was not hidden even after the **Hide-SSID** and the **deny-bcast** parameters were enabled. This issue is fixed by limiting the broadcast probe response if the **Hide-SSID** parameter is enabled. **Scenario:** This issue was observed in OAW-AP225 associated with OAW-4550/4650/4750 Series switches.

Bug ID	Description
88288	**Symptom:** OAW-AP134 crashed with a **Fatal exception in interrupt** error. **Scenario:** This issue was observed on 11n APs running AOS-W 6.3 upon client disassociation.
88512	**Symptom**: OAW-AP225 access point transmitting A-MPDU aggregate traffic can perform excessive retries. **Scenario**: This issue occurred on OAW-AP225 in a network environment with a busy channel and a large number of intel clients.
80426 77834 81672 85186 85381 85396 85400 85658 85713 80426 85186 80426 86821	**Symptom:** An AP crashed and rebooted frequently and the log files for the event listed the reason for the crash as kernel panic. **Scenario:** This issue occurred in remote APs (RAPs) or campus APs (CAPs) with CPSec enabled, when the VPN tunnel terminated and re-established with traffic on the tunnel. This issue was observed in OAW-AP134, OAW-AP135, and OAW-RAP155 models.

ARM

Table 229: *ARM Fixed Issues*

Bug ID	Description
86084	**Symptom:** A wireless client remained associated to OAW-AP220 Series even though the signal strength was weak. **Scenario:** This issue occurred on OAW-AP220 Series running AOS-W 6.3. When the hand off assist feature was enabled on OAW-AP220 Series, packets were not sent over the air to the client.

Authentication

Table 230: *Authentication Fixed Issues*

Bug ID	Description
81035	**Symptom:** When roaming, the offered PMKID from the client is ignored and full authentication occurred. If no user credentials are stored on the machine (or saved), the PMKID is ignored. The username and password need to be provided at each roam. **Scenario:** This issue occurred on no specific switch and was caused by a Wi-Fi client. In this case, the client was Ahteros-based NICs. This issue is not caused by an AOS-W switch or AP. A client driver upgrade resolved the issue.

Base OS Security

Table 231: *Base OS Security Fixed Issues*

Bug ID	Description
83776	**Symptom:** Atheros based client devices were unable to connect to WPA-TKIP networks after AOS-W 6.1.3.7. This issue is fixed by disabling use of multiple Traffic Identifier (TID) for WPA-TKIP. **Scenario:** This issue was observed when Wireless Multimedia Extensions (WMM) was enabled and the Atheros clients did not support multiple relay counters.
84456	**Symptom:** Remote APs (RAPs) kept rebooting and did not come up on the switch. **Scenario:** This issue occurred as two RAPs using a static IP address tried to establish sessions using the same RAP credentials. This issue was not limited to any specific switch or RAP model.
84628 86814 87497	**Symptom:** OAW-S3 switch module in a OAW-6000 switch unexpectedly rebooted. Log files for the event listed the reason for the reboot as **Datapath timeout**. This issue is fixed by validating the bridge entries for VoIP clients. **Scenario:** This issue occurred when an invalid bridge value was computed and stored in an internal module (datapath). This issue was observed in OAW-S3 switch module running AOS-W 6.2.0.0.
85519	**Symptom:** One or more SSH (Secure Shell) sessions to a switch failed when multiple simultaneous SSH sessions occurred. The updates are made to sshd (SSH Daemon) process in AOS-W 6.3.1.0 to avoid this issue . **Scenario:** This issue was observed in AOS-W 6.1, 6.2, and 6.3.
85688	**Symptom:** The Virtual Intranet Access VPN (VIA-VPN) Authentication using RSA SecureID was not functioning for both New PIN and Next Tokencode modes. This issue was resolved by changes to the code that maintain the state of RADIUS exchange. **Scenario:** This issue was observed in AOS-W 6.3.0.0 while performing VIA-VPN authentication with an RSA server using RSA SecureID.
86687	**Symptom:** The switch's SSH configuration has been modified to reduce a potential vulnerability to DOS attacks. **Scenario:** This issue was identified on switches running AOS-W 6.3.0.0.
86867	**Symptom:** When a user-role and the ACL configured as the ip access-group on the interface for APs/RAPs have the same name, the AP/RAP traffic is hitting the user-role ACL instead of the ip access-group ACL. **Scenario:** This issue was observed on a switch running AOS-W 6.2.1.2. **Workaround:** Do not create an ACL for the IP access-group that has a name matching that of any user-role in the configuration.
88165	**Symptom** Clients using a wired connection are assigned an incorrect user role **Scenario**: This bug is applicable for wired clients, and is not specific to a switch type of software version. This issue occurs when information about an AP wired connection gets overwritten by similar information from another AP, resulting in a loss of wired information on the first AP, and preventing users associated with that AP from falling into their user role.
88386	**Symptom:** User roles disappeared randomly after a switch reloaded. Internal code changes fixed this issue. **Scenario:** The issue occurred when many user roles were added, or roles with heavy configurations exceeded the buffer space on the switch. This issue was not specific to any AOS-W version or switch model.

Switch-Datapath

Table 232: *Switch-Datapath Fixed Issues*

Bug ID	Description
84071	**Symptom:** A switch stopped responding and unexpectedly rebooted. The log files for the event listed the reason for the reboot as **Datapath exception**. This issue occurred on OAW-4550/4650/4750 Series switch running AOS-W 6.2.1.0. **Scenario:** This issue occurred when an SSL encapsulated invalid ESP frame was received and processed by the switch.

Switch-Platform

Table 233: *Switch-Platform Fixed Issues*

Bug ID	Description
76447	**Symptom:** An OAW-S3 switch stopped responding and rebooted. The switch listed the reason for the crash as a switch processor kernel panic. This issue was resolved by internal improvements to hardware register access. **Scenario:** This issue was observed in local OAW-S3 switches running AOS-W 6.1.3.5.
81555	**Symptom:** A switch crashed and rebooted after upgrading the software from AOS-W 6.1.3.6 to AOS-W 6.1.3.7. The log files for the event listed the reason for the crash as a watchdog timeout. The interrupt handler for packet parsing was modified to ensure that CPU was not overwhelmed with the traffic packets. **Scenario:** In a high traffic deployment, a race condition triggered the switch crash. This issue was not specific to any switch model.

High Availability

Table 234: *High Availability Fixed Issues*

Bug ID	Description
86798	**Symptom:** When APs were connected to switches using the high availability: fast failover feature in a master\master topology, OmniVista could not see information about rogue APs from the active master switch. Improvements to the way master IP information for each switch is saved resolves this issue. **Scenario:** When the high availability fast failover feature was enabled between two master switches acting as HA-Active and HA-Standby switches, the active switch's master IP address stored in the AP was overwritten by the master IP address from the standby switch. This caused WLAN Management System (WMS) information to be sent to the standby switch instead of the active switch.

Local Database

Table 235: *Local Database Fixed Issues*

Bug ID	Description
84494	**Symptom:** A switch unexpectedly rebooted, with the log files for the event listing the reason for the reboot as **Nanny rebooted machine - udbserver process died**. **Scenario:** This issue occurred on a standalone master OAW-4550 switch with one associated OAW-AP135 access point, and was resolved by internal code changes.
88019	**Symptom:** A warning message **WARNING: This switch has RAP whitelist data stored in pre-6.3 format, which is consuming .....running the command 'local-userdb-ap del all** appeared, when a user logged into a switch. This issue is fixed by deleting the warning file, when all the old entries are deleted. **Scenario:** This issue occurred when a switch was upgraded from a previous version of AOS-W to 6.3 or later. This issue was not specific to any switch model or release version.

Multicast

Table 236: *Multicast Fixed Issues*

Bug ID	Description
88138	**Symptom:** One of the proxy group entries aged out after issuing the **show ip igmp proxy-group** command. This crashed the multicast module in the switch. Changes to the internal code of the multicast module fixed the issue. **Scenario:** This issue was not limited to a specific switch model and was observed in AOS-W 6.3.0.1.

RADIUS

Table 237: *RADIUS Fixed Issues*

Bug ID	Description
85848	**Symptom:** The **Calling_Station_Id** was sent an IP address instead of MAC address even though the option “Use IP address for calling station ID” was not selected in the AAA server. This issue is fixed in 6.3.1.0, by adding a new check box for the MAC address. **Scenario:** This issue was observed when the user executed the **aaa authentication-server radius x** command, and was not specific to any switch model.
87814	**Symptom:** On client disconnection, the RADIUS accounting STOP record packet counter reset to zero. Changes to the internal code fixed the issue. **Scenario:** This issue occurred when an AP was provisioned in decrypt-tunnel mode with RADIUS accounting enabled. This issue was not limited to a specific switch model and was observed in AOS-W 6.3.0.0 or later.

Remote AP

Table 238: *Remote AP Fixed Issues*

Bug ID	Description
85473	**Symptom:** A OAW-RAP3WN AP using a USB modem was unable to come up until it rebooted. Changes to how the OAW-RAP3WN determines the modem product ID has resolved this issue. **Scenario:** This issue occurred on a OAW-RAP3WN AP running AOS-W 6.2.1.2 connected to a Huawei E156 modem.
86082	**Symptom:** OAW-AP225 failed to respond. Enhancements in the internal code fixed this issue. **Scenario:** This issue was observed on when Point-to-point protocol over Ethernet (PPPoE) was enabled on OAW-AP220 Series access points.
86934	**Symptom:** The AP failed during boot up when the Huawei modem E1371 was used. An internal code error when using this modem caused the issue. **Scenario:** This issue was observed on a OAW-RAP108 and OAW-RAP109 running AOS-W 6.3.
87105	**Symptom:** Printers connected to the wired port of a remote AP (RAP) in tunnel mode intermittently fall into the wrong VLAN. This issue is resolved by improvements that ensure that the remote AP configuration state is properly cleared when its connection is reset. **Scenario:** This issue occurred on a OAW-RAP5 remote AP running AOS-W 6.2.1.2, when configuration settings was not properly cleared on a remote AP that reset its connection to the switch. As a result, the RAP's ethernet interface was brought up in bridge mode first, then changed to tunnel mode. This caused a configuration conflict between the switch and the RAP, as the switch managed the RAP as a remote bridge user, and the RAP operated as a user in tunnel mode.

SNMP

Table 239: *SNMP Fixed Issues*

Bug ID	Description
87691	**Symptom:** There was a mismatch in the interface index value across the entire Interface table and AMAP table. The aipAMAPportConnection table returned a non-existent iflNdex value. **Scenario:** This issue was observed on all switches running AOS-W version 6.2.1.2 or later.

Startup Wizard

Table 240: *Startup Wizard Fixed Issues*

Bug ID	Description
85312	**Symptom:** An error message **Error: Very high throughput must be enabled to enable 80 MHz channel usage** appeared on the **Finish** page of the Campus WLAN wizard. This issue was resolved by enabling the high-throughput or very-high-throughput settings in the 802.11a or 802.11g radio profiles before enabling 40 MHz and 80 MHz, and disabling 80 MHz and 40 MHz, before disabling the throughput setting. **Scenario:** This error occurred when a WLAN is configured with a, a+n, b/g, or b/g+n radio types.

Web UI

Table 241: *Web UI Fixed Issues*

Bug ID	Description
80233	**Symptom:** The **Monitoring > Access Points and Monitoring > Network > All Access Points** page of the switch WebUI showed APs as down, even if they are showed as up in the command-line interface. This issue is fixed by improvements to the local management switch (LMS) IP on the master switch and now the status of APs is displayed accurately on the WebUI. **Scenario:** This issue was observed on a OAW-6000 master switch with two local switches running AOS-W 6.2.0.2 in a master/local topology.
83820	**Symptom:** Dashboard page was not getting loaded in the WebUI. This issue was fixed by disabling the compatibility mode on the IE. **Scenario:** The issue occurred when the user tried to access the WebUI in IE8 in compatibility mode (This mode is used to support websites that were developed for older versions of IE browser). The issue was not specific to a switch model or a software version.
84151 85229 85569 86554	**Symptom:** The **Security Summary** page in the WebUI timed out if the event table in the WMS database became very large. This issue was resolved by enabling a periodic clean-up of the WMS event table entries. **Scenario:** This issue was observed when too many APs where terminating on a switch. This issue was not limited to any specific switch model.

Voice

Table 242: *Voice Fixed Issues*

Bug ID	Description
83403 86180 86369	**Symptom:** The clients were disconnected from the network due to an internal module crash. This issue was resolved by not prioritizing the subsequent RTP sessions for the SCCP calls for the clients. **Scenario:** This issue was observed while handling SCCP state transition, hence an internal module (STM) crashed. This issue occurred on switches running AOS-W 6.1 and 6.2 versions, and was not limited to a specific switch model.
86224	**Symptom:** Calls dropped after 30 seconds when performing a blindly transferred SIP call. **Scenario:** This issue was observed on the OAW-S3 switch module running AOS-W version 6.2.1. It occurred when Ascom phones sent a DELTS request upon receiving either an "invite" message from the SIP server or after sending a "180 Ringing" message back to the server.

WMM

Table 243: *WMM Fixed Issues*

Bug ID	Description
68503	**Symptom:** When the same Differentiated Service Code Point (DSCP) value is mapped to two different access categories, the lower of the two is used for the downstream traffic. This issue was resolved by mapping the higher value to the downstream traffic. **Scenario:** This issue was observed on switches running AOS-W 6.2 or earlier in tunnel and decrypt-tunnel forwarding modes.

The following issues and limitations are observed in AOS-W 6.3.1.x releases. Applicable workarounds are included.

Known Issues and Limitations in AOS-W 6.3.1.16

Activate

Table 244: *Activate Known Issues*

Bug ID	Description
107116	**Symptom:** The switch did not download the complete whitelist database from Activate. **Scenario:** This issue is observed when running a script from the switch to download the whitelist database from Activate. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.5. **Workaround:** None.

AMON

Table 245: *AMON Known Issues*

Bug ID	Description
96739	**Symptom:** The **Clients** page in the AOS-W WebUI does not display user-related information such as **User Name**, **Client IP**, **User Role**, and **Device Type**. **Scenario:** This issue is observed in the **Monitoring > Switch > Clients** page of the WebUI after upgrading the switch from the AOS-W 6.1.3.10 to 6.3.1.2 version. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.2. **Workaround:** None.
109446	**Symptom:** A master switch crashes due to low available memory. **Scenario:** This issue occurs when a Station Management (STM) process displays a large memory footprint due to a resource leak. This issue is observed in OAW-4704 switches running AOS-W 6.3.1.9. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.9. **Workaround:** None.

AP-Datapath

Table 246: *AP-Datapath Known Issues*

Bug ID	Description
113962	**Symptom:** When a client starts roaming from one AP to another, the phones get stuck at Key1. **Scenario:** This issue is observed in Netlink phones after the switch was upgraded from AOS-W 6.1.3.4 to 6.3.1.14. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.14. **Workaround:** None.

AP-Platform

Table 247: *AP-Platform Known Issues*

Bug ID	Description
113372 113455	**Symptom:** When all available channels on an outdoor access point are blacklisted after radar-detection, the access point stays in APM mode. The access point does not come out of APM mode after 30 minutes and does not provide service until it is rebooted. **Scenario:** This issue occurs in OAW-AP175P access points connected to switches running AOS-W 6.3.1.5. This issue occurs when all available channels on an outdoor access point are blacklisted after radar-detection and non-DFS channels are not available. **Platform:** Any outdoor access point provisioned as mesh-portal. **Reported Version:** AOS-W 6.3.1.5. **Workaround:** None.

AP-Wireless

Table 248: *AP-Wireless Known Issues*

Bug ID	Description
108650	**Symptom:** When clients associated with OAW-AP105 access points, some of then exhibited retry rates that were higher than expected. The retry rates can be observed in the switch dashboard, CLI, or AP radio statistics. **Scenario:** This issue is observed when the OAW-AP105 access point is upgraded from AOS-W 6.1.x to AOS-W 6.3.x. **Platform:** OAW-AP105 access point. **Reported Version:** AOS-W 6.3.1.9. **Workaround:** None.
110597	**Symptom:** When the access point detects a false RADAR, it changes the channel. **Scenario:** This issue is observed in OAW-AP105 and OAW-AP175 access points connected to switches running AOS-W 6.3.1.9. **Platform:** OAW-AP105 and OAW-AP175 access points. **Reported Version:** AOS-W 6.3.1.9. **Workaround:** None.
110939 114326	**Symptom:** The CPU load on OAW-AP135 access points is high when there is an increase in the number of customers using video meetings. **Scenario:** This issue is observed in OAW-AP135 access points connected to switches running AOS-W 6.3.1.5. **Platform:** OAW-AP135 access points. **Reported Version:** AOS-W 6.3.1.5. **Workaround:** None.
111395	**Symptom:** Multiple APs reboot when U-APSD and Quiet-IE are disabled dynamically. **Scenario:** This issue is observed in OAW-AP220 Series access points connected to switches running AOS-W 6.3.1.5. **Platform:** OAW-AP220 Series. **Reported Version:** AOS-W 6. 3.1.5. **Workaround:** None.

Configuration

Table 249: *Configuration Known Issues*

Bug ID	Description
93922	**Symptom:** A custom banner with the **#** delimiter is added as part of the **show running-config** command output. **Scenario:** This issue is observed when an administrator configures the banner using the **banner motd** command in the switch with the **#** delimiter. This issue is not limited to a specific switch model and is observed in AOS-W 6.3.1.1. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.1. **Workaround:** None.

Switch-Datapath

Table 250: *Switch-Datapath Known Issues*

Bug ID	Description
93817	**Symptom:** An internal error occurs in the master switch while provisioning APs associated with a specific local switch. **Scenario:** This issue is observed in OAW-4504XM switches running AOS-W 6.3.1.1 in a master-local topology. **Platform:** OAW-4504XM switches. **Reported Version:** AOS-W 6.3.1.1. **Workaround:** None.
95532	**Symptom:** A switch reboots unexpectedly. The log files for the event listed the reason for the reboot as **datapath timeout**. **Scenario:** This issue is observed in OAW-4550 switches running AOS-W 6.3.1.1. **Platform:** OAW-4550 switches. **Reported Version:** AOS-W 6.3.1.1. **Workaround:** None.
111275	**Symptom:** A switch reboots unexpectedly. The log files for the event listed the reason for the reboot as **datapath timeout**. **Scenario:** This issue is observed in OAW-S3 switches running AOS-W 6.3.1.7. **Platform:** OAW-S3 switches. **Reported Version:** AOS-W 6.3.1.7. **Workaround:** None.
112780	**Symptom:** A switch reboots randomly. The log files for the event list the reason for the reboot as **datapath timeout**. **Scenario:** This issue is observed in OAW-4704 switches running AOS-W 6.3.1.8. **Platform:** OAW-4704 switches. **Reported Version:** AOS-W 6.3.1.8. **Workaround:** None.

Switch-Platform

Table 251: *Switch-Platform Known Issues*

Bug ID	Description
104139 104729 107907 108026 108194	**Symptom:** WMS and database modules reboot unexpectedly. **Scenario**: This issue is observed in all switches running AOS-W 6.3.x and later versions. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.6. **Workaround**: None.
100707 107293 109473 110196 113087	**Symptom:** A switch reboots unexpectedly when executing a cache instruction. The log files for the event list the reason for the reboot as **kernel panic**. **Scenario**: This issue is observed in OAW-4704 switches running AOS-W 6.3.1.4 in a master-local topology. **Platform:** OAW-4704 switches. **Reported Version:** AOS-W 6.3.1.4. **Workaround**: None.
104680 106067 106365 106965 106967 107529 107629 107812 107981 108251 108735 108909 109462 109826 111503 111597 112724 112730 112926 113571 114212	**Symptom:** The **httpd** module crashes and restarts unexpectedly. **Scenario:** This issue is observed in OAW-4750 switches running AOS-W 6.3.1.8 and is caused by high CPU utilization during captive portal authentication. **Platform:** OAW-4750 switches. **Reported Version:** AOS-W 6.3.1.8. **Workaround:** None.
107925	**Symptom:** An administrator is unable to access the switch through the CLI or WebUI. **Scenario:** This issue is observed when the **fpcli** process on the switch fails. 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:** None.
107980	**Symptom:** The **STM** process on a local switch crashes and reboots. The log file for the event lists the reason as **Reboot Cause: illegal instruction**. **Scenario**: This issue is observed on OAW-4750 switches running AOS-W 6.3.1.10. **Platform:** OAW-4750 switches. **Reported Version:** AOS-W 6.3.1.10. **Workaround:** None.
107989	**Symptom:** A switch reboots unexpectedly. The log file for the event lists the reason as **Reboot Cause: kernel panic**. **Scenario**: This issue is observed when a OAW-4x04 Series switch is upgraded from AOS-W 6.3.1.7 to AOS-W 6.3.1.10. **Platform:** OAW-4x04 Series switches.

Table 251: *Switch-Platform Known Issues*

Bug ID	Description
	Reported Version: AOS-W 6.3.1.10. **Workaround**: None.
108731	**Symptom:** OAW-S3 switch reboots unexpectedly. The log file for the event listed the reason as **Reboot Cause: kernel panic**. **Scenario**: This issue occurs due to memory corruption. This issue is observed on OAW-S3, OAW-4504, OAW-4604, and OAW-4704 switches running any version of AOS-W. **Platform:** OAW-S3, OAW-4504, OAW-4604, and OAW-4704 switches. **Reported Version:** AOS-W 6.3.1.4. **Workaround**: None.
112436	**Symptom:** A switch stops responding to Remote APs (RAPs). **Scenario**: This issue is observed with RAPs connected to OAW-6000 Series switches running AOS-W 6.3.1.5 in a master-local-standby topology. **Platform:** OAW-6000 Series switches. **Reported Version:** AOS-W 6.3.1.4. **Workaround**: None.
113684 113687	**Symptom:** The WLAN Management System (WMS) process crashed multiple times on the standby switch, which resulted in switch reboot. **Scenario**: This issue is observed in OAW-4550 switches running AOS-W 6.3.1.17 in a master-local topology. **Platform:** OAW-4550 switches. **Reported Version:** AOS-W 6.3.1.17. **Workaround**: None.

DHCP

Table 252: *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 DHCP **option 82** parameters are configured on the VLAN interface. This issue is observed in switches running AOS-W 6.1.3.x or 6.3.x. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.7. **Workaround:** None.

Licensing

Table 253: *Licensing Known Issues*

Bug ID	Description
100234	**Symptom:** The ACL configuration on the local switch is out of sync with the master switch when both the master and standby switch are rebooted simultaneously. **Scenario:** This issue is observed in a master-standby topology where all the licenses are installed on the master switch. This issue is not limited to a specific switch model and is observed in AOS-W 6.3.1.5. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.5. **Workaround:** None.

Master-Local

Table 254: *Master-Local Known Issues*

Bug ID	Description
103970	**Symptom:** Some local switches do not form an IPsec link with the master switch. Restarting the **IKE** process on the affected local switch helps to form the IPSEC link, but other local switches randomly get disconnected from the master switch. **Scenario**: This issue is observed in switches running AOS-W 6.3.1.8 in a master-local topology. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.8. **Workaround**: None.
111482	**Symptom:** An Access Control List (ACL) that has a system defined **vrrp_ip** alias fails to synchronize with the local switch. **Scenario:** This issue is observed on switch reboot. Upon reboot, the net destination does not exist when the ACL configuration is applied. This issue is observed in switches running AOS-W 6.3.1.13. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.13. **Workaround:** None.

Mesh

Table 255: *Mesh Known Issues*

Bug ID	Description
111386	**Symptom:** Packets lose 3% on G radio between OAW-AP104 as portal and OAW-AP175 as the mesh point. **Scenario:** This issue is observed in OAW-AP104 and OAW-AP175 connected to switches running AOS-W 6.3.1.12. **Platform:** OAW-AP104 and OAW-AP175 access points. **Reported Version:** AOS-W 6.3.1.12. **Workaround:** None.

Known Issues and Limitations in AOS-W 6.3.1.15

No Support for Mesh in 802.11ac Access Points

Wireless mesh is not supported in OAW-AP200 Series, OAW-AP210 Series, OAW-AP220 Series, and OAW-AP270 Series 802.11ac access points in current AOS-W version.

802.1X

Table 256: *802.1X Known Issues*

Bug ID	Description
111437	**Symptom:** Scanners disconnect unexpectedly and the log files for the event list the reason as **replay counter errors**. **Scenario:** This issue is observed when the operation mode is set to WPA (Wi-Fi Protected Access)/WPA2-PSK (WPA- Pre-Shared Key) encryption. This issue occurs in OAW-4604 switches running AOS-W 6.3.1.7. **Platform:** OAW-4604 switch. **Reported Version:** AOS-W 6.3.1.7. **Workaround:** Increase wpa-key period in 802.1X profile.

AMON

Table 257: *AMON Known Issues*

Bug ID	Description
100764 99665	**Symptom:** The **Dashboard** > **Performance** page of the AOS-W WebUI does not display, **Goodput**, **Client Health**, and **SNR** data. **Scenario:** This issue is observed in OAW-S3 switches running AOS-W 6.3.1.6. **Platform:** OAW-S3 switches. **Reported Version:** AOS-W 6.3.1.6. **Workaround:** None.

AP-Platform

Table 258: *AP-Platform Known Issues*

Bug ID	Description
109274	**Symptom:** Although clients associate with an AP, they neither obtain an IP address nor have data connectivity. **Scenario:** This issue is observed in OAW-AP125 access points connected to switches running AOS-W 6.3.1.8 in master-local topology with 802.1X authentication. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.8. **Workaround:** Disconnect and reconnect the client.
111587	**Symptom:** The master switch does not respond when the **show ap tech-support** command is executed, after the AP terminates on the local switch. **Scenario:** This issue is observed when the CLI request is blocked by the AP firewall as it does not have IPSec connection to the master switch. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.8. **Workaround:** None.
111139	**Symptom:** Station Management Module (STM) restarts and crashes again. **Scenario:** This issue occurs when STM initialization fails as the STM is unable to find a table in the MySQL database. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.x.0. **Workaround:** None.

AP-Wireless

Table 259: *AP-Wireless Known Issues*

Bug ID	Description
107584	**Symptom:** An OAW-AP70 access point reboots and crashes when out of memory. **Scenario:** This issue is observed in OAW-AP70 access points connected to OAW-4x04 Series switches running AOS-W 6.3.1.3 in a master-local topology. **Platform:** OAW-AP70 access points. **Reported Version:** AOS-W 6.3.1.3. **Workaround:** None.
110135	**Symptom:** Clients disconnect unexpectedly from the network. The log files for the event listed multiple internal deauthentication errors. **Scenario:** This issue is observed in OAW-AP70, OAW-AP125, and OAW-AP225 access points connected to OAW-S3 switches running AOS-W 6.3.1.13. **Platform:** OAW-AP70, OAW-AP125, and OAW-AP225 access points. **Reported Version:** AOS-W 6.3.1.13. **Workaround:** None.
110581	**Symptom:** An AP crashed and the log files for the event listed the reason for the crash as **kernel page fault at virtual address 00000000, epc == c08f2734, ra == c08f4be**. **Scenario:** This issue is observed in OAW-AP105 access points connected to switches running AOS-W 6.3.1.13. **Platform:** OAW-AP105 access points. **Reported Version:** AOS-W 6.3.1.13. **Workaround:** None.
111257	**Symptom:** OAW-AP225 access points reboot unexpectedly. The log files for the event listed the reason as **Reboot caused by kernel panic: Fatal exception in interrupt**. **Scenario:** This issue is observed in OAW-AP225 access points connected to switches running AOS-W 6.3.1.13 in a master-local topology. **Platform:** OAW-AP225 access points. **Reported Version:** AOS-W 6.3.1.13. **Workaround:** None.

ARM

Table 260: *ARM Known Issues*

Bug ID	Description
111543	**Symptom:** Adaptive Radio Management (ARM) is not functional in the Egypt country domain. **Scenario:** This issue is observed when 40 MHz assignment is enabled in the ARM profile. This issue is observed in 802.11n and 802.11ac-capable access points running AOS-W 6.3.1.14. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.14. **Workaround:** None.

Base OS Security

Table 261: *Base OS Security Known Issues*

Bug ID	Description
107059	**Symptom:** When some wireless clients connect to the 802.1X SSID and get an IP address, the IP is either not reflected in the user table or there is a delay in the entry being registered. **Scenario:** The **show datapath user** command displays a **C** flag for the clients who are impacted. 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:** Offload the switch by reducing the value of the **web-server web-max-clients** parameter and the number of APs terminating on the switch.
109838	**Symptom:** The switch displays an incorrect number of net destinations in the WebUI. **Scenario:** This issue occurs when there is a space before the net destination name. This issue is seen in switches running AOS-W 6.3.x. **Platform:** All platform. **Reported Version:** AOS-W 6.3.1.12. **Workaround:** None.
111762	**Symptom:** The output of the **show running-config** command displays the Network Time Protocol (NTP) MD5 secret key in plain text. **Scenario:** This issue is observed when the **encrypt enable** command is enabled on the switch. This issue is not limited to a specific switch model or release version. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.13. **Workaround:** None.

Switch-Datapath

Table 262: *Switch-Datapath Known Issues*

Bug ID	Description
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 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

Switch-Platform

Table 263: *Switch-Platform Known Issues*

Bug ID	Description
103456	**Symptom:** A local switch reboots unexpectedly. The log files for the event listed the reason for the reboot as **Control Processor Kernel Panic**. **Scenario**: This issue is observed in OAW-4650 switches running AOS-W 6.3.1.7 in a master-local topology. **Platform:** OAW-4650 switches. **Reported Version:** AOS-W 6.3.1.7. **Workaround**: None.
109316	**Symptom:** Due to low available memory a warning message is displayed. **Scenario**: This issue occurs in OAW-4604 switches running AOS-W 6.3.1.5. **Platform:** OAW-4604 switches with 1G memory. **Reported Version:** AOS-W 6.3.1.5. **Workaround**: None.
109840	**Symptom:** Switch reboots unexpectedly. The log file for the event listed the reason as **Nanny rebooted machine low on free memory (Intent:cause:register 34:86:0)**. **Scenario**: This issue occurs in OAW-4604 switches running AOS-W 6.3.1.8 in master-local topology. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.8. **Workaround**: None.
111384	**Symptom:** A switch reboots unexpectedly. The log file for the event listed the reason as **kernel panic**. **Scenario:** This issue is observed in OAW-4650 switches running AOS-W 6.3.1.5. **Platform:** OAW-4650 switches. **Reported Version:** AOS-W 6.3.1.5. **Workaround:** None.

IPsec

Table 264: *IPsec Known Issues*

Bug ID	Description
102315	**Symptom:** In a master-local topology, very low download speed is experienced over site-to-site VPN with two switches running AOS-W 6.3.1.x. **Scenario:** This issue **Platform:** . **Reported Version:**AOS-W 6.3.1.12. **Workaround:** None.
108454	**Symptom:** Remote AP (RAP) does not failover to the standby switch. **Scenario:** This issue is observed only when the RAP uses certificate and not PSK for authentication. From the IKE logs, the RAP keeps initiating a new IPsec tunnel. This issue is observed in switches running AOS-W 6.3.1.4 in a master-standby topology. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.4. **Workaround:** None.

Licensing

Table 265: *Licensing Known Issues*

Bug ID	Description
106241	**Symptom:** The local switch displays an incorrect AP license usage. **Scenario:** On issuing the **show ap license-usage** and the **show active ap** commands, there is a discrepancy in the number of AP licenses used and the number of active APs on the local switch. This issue is seen when centralized licensing is enabled on the switch. This issue 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.

Remote AP

Table 266: *Remote AP Known Issues*

Bug ID	Description
111165	**Symptom:** Verizon Wireless USB760 modem on OAW-RAP5WN fails to establish IPsec tunnel with the switch. **Scenario:** This issue is observed on switches running AOS-W 6.3.1.13. **Platform:** OAW-RAP5WN **Reported Version:** AOS-W 6.3.1.13. **Workaround:** None.

Voice

Table 267: *Voice Known Issues*

Bug ID	Description
102955	**Symptom**: Phones get disconnected when a RAP drops keepalive packets. This issue is observed when the RAP's wired port is configured in the split-tunnel mode. **Scenario**: This issue is observed in OAW-RAP2WG running AOS-W 6.3.1.7. **Platform**: All platforms. **Reported Version**: AOS-W 6.3.1.7. **Workaround**: None.
111263	**Symptom:** The **show voice call-cdrs detail** command displays incorrect IP DSCP and WMM values. **Scenario:** This is an issue with the output of the command and is observed in switches running AOS-W 6.3.1.2. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.2. **Workaround:** To display the correct values, issue the **show datapath session** command and look for the values under the **ToS** column heading.

VRRP

Table 268: *VRRP Known Issues*

Bug ID	Description
109968	**Symptom:** After reboot, the VRRP master with preemption disabled regains master state when uplink switch is running RSTP. **Scenario:** This issue is observed when a VRRP master with STP disabled connects to an intermediate device with RSTP enabled. Since STP 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.
109845	**Symptom:** After upgrading to 6.4.2.2, the VRRP routed through L2 GRE tunnel for non-routable VLAN is in backup state. **Scenario:** This issue is observed when VRRP instances in the tunneled VLANs are in backup state and not handled when receiving the link status of the VLAN. This issue is observed in OAW-4306G and OAW-4550 switches running AOS-W 6.4.2.2. **Platform:** OAW-4306G and OAW-4550 switches. **Reported Version:** AOS-W 6.4.2.2. **Workaround:** None.

Known Issues and Limitations in AOS-W 6.3.1.14

Air Management-IDS

Table 269: *Air Management-IDS Known Issues*

Bug ID	Description
104711	**Symptom:** 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 issues 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. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.5. **Workaround:** None.

AP-Datapath

Table 270: *AP-Datapath Known Issues*

Bug ID	Description
104694	**Symptom:** A wired client is unable to access a wireless client although both the clients are on the same IP subnet. **Scenario:** This issue is observed when the Remote AP is in the bridge forwarding mode and the wireless client is idle. This issue is observed on OAW-4550 switches with OAW-AP225 access points functioning as a Remote AP and running AOS-W 6.3.1.8. **Platform:** OAW-AP225 access points. **Reported Version:** AOS-W 6.3.1.8. **Workaround:** None.

AP-Platform

Table 271: *AP-Platform Known Issues*

Bug ID	Description
106364	**Symptom:** OAW-AP124 reboots randomly. The log files listed the reason for the reboot as **PCI ERROR [MR_WABT]: PCI master abort detected on write**. **Scenario:** This issue is observed in OAW-AP124 access points when connected to a switch as a campus AP or to a mesh network. This issue is observed in OAW-S3 switches running AOS-W 6.3.1.5. **Platform:** OAW-AP124 access points. **Reported Version:** AOS-W 6.3.1.5. **Workaround:** None.
110139	**Symptom:** An AP terminating on a backup switch fails to fallback to the primary switch although it looses connection to the backup switch. However, after the AP reboots it connects to the primary switch. **Scenario:** This issue is observed when CPSec is disabled. This issue is not limited to a specific switch model or release version. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.13. **Workaround:** None.

AP-Wireless

Table 272: *AP-Wireless Known Issues*

Bug ID	Description
108877	**Symptom:** An AP crashes after upgrading to AOS-W 6.3.1.12. **Scenario:** This issue is observed in OAW-AP105 access points connected to OAW-4550 switches running AOS-W in a master-local topology. **Platform:** OAW-AP105 access points. **Reported Version:** AOS-W 6.3.1.12. **Workaround:** None.
108995	**Symptom:** There is a random drop in the performance of OAW-AP225. **Scenario:** This issue is observed in OAW-AP225 access points connected to switches running AOS-W in a master-local topology. **Platform:** OAW-AP225 access points. **Reported Version:** AOS-W 6.3.1.12. **Workaround:** Reboot OAW-AP225 or disable and enable the radio.
109810	**Symptom:** When scanning is enabled on OAW-AP105, there is an increase in the frequency of radio reset. This results in interrupting the flow of data traffic for all associated clients. **Scenario:** This issue is observed in OAW-AP105 access points connected to OAW-S3 switches running AOS-W 6.1.3.9. **Platform:** OAW-AP105 access points. **Reported Version:** AOS-W 6.1.3.9. **Workaround:** None.

Table 272: *AP-Wireless Known Issues*

Bug ID	Description
110000	**Symptom:** OAW-AP124 reboots unexpectedly. The log files for the event listed the reason for the reboot as **kernel crash**. **Scenario:** This issue is observed in OAW-AP124 access points connected to OAW-4750 switches running AOS-W 6.3.1.5, in a master-local topology. **Platform:** OAW-AP124 access points. **Reported Version:** AOS-W 6.3.1.5. **Workaround:** None.
110027	**Symptom:** APs reboot randomly. **Scenario:** This issue is observed in OAW-AP120 Series access points connected to switches running AOS-W 6.3.1.5. **Platform:** OAW-AP120 Series access points. **Reported Version:** AOS-W 6.3.1.5. **Workaround:** None.

Authentication

Table 273: *Authentication Known Issues*

Bug ID	Description
107527	**Symptom:** Wired bridge user is mapped with incorrect ACLs even though the user is mapped with correct user role. **Scenario:** This issue is observed in RAPs connected to switches running AOS-W 6.3.1.8. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.8. **Workaround:** Allow all traffic associated with an **unauthenticated** role, to the IP address of the switch.

Base OS Security

Table 274: *Base OS Security Known Issues*

Bug ID	Description
107895	**Symptom:** Clients are unable to connect to the switch when enforce-dhcp is enabled in the AAA profile. **Scenario:** This issue is observed in the OAW-4704 switches running AOS-W 6.3.1.5. **Platform:** OAW-4704 switches. **Reported Version:** AOS-W 6.3.1.5. **Workaround:** None.
109591	**Symptom: Authentication** module does not respond to show commands from the webserver. **Scenario:** This issue is observed when the **tacacs-accounting** parameter is configured for show commands and all the servers configured in the server-group are not reachable. This issue is not specific to any switch or AOS-W version. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.9. **Workaround:** Remove **tacacs-accounting** parameter from the show commands.
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 version. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.8. **Workaround:** None.

Table 274: *Base OS Security Known Issues*

Bug ID	Description
110209	**Symptom:** If MAC authentication fails during re-authentication, user is not placed in initial/logon role. **Scenario:** This issue is observed when MAC-based authentication and 802.1X authentication are configured with L2 authentication fail-through enabled in AAA profile. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.10. **Workaround:** Use only MAC-based authentication.

Switch-Platform

Table 275: *Switch-Platform Known Issues*

Bug ID	Description
109893	**Symptom:** An internal process crashes in the switch. **Scenario:** This issue is observed in OAW-S3 and OAW-4704 switches running AOS-W 6.3.1.2 in a master-local topology. **Platform:** OAW-S3 and OAW-4704 switches. **Reported Version:** AOS-W 6.3.1.2. **Workaround:** None.
109980	**Symptom:** A local switch crashes and reboots unexpectedly. The log files for the event listed the reason for the reboot as **kernel panic**. **Scenario**: This issue is observed in OAW-6000 Series switches running AOS-W 6.3.1.8, in a master-local topology. **Platform:** OAW-6000 Series switches. **Reported Version:** AOS-W 6.3.1.8. **Workaround**: None.

Master Redundancy

Table 276: *Master Redundancy Known Issues*

Bug ID	Description
108519	**Symptom:** When the **show database synchronize** command is executed, the system displays a **FAILED** message and the standby switch is out of sync with the master. Additionally, the system is in an inconsistent state during switchover. **Scenario:** The standby switch database is out-of-sync with the master switch and any switchover during an out-of-sync state causes the switch to be in an inconsistent state. This issue is observed in OAW-6000 Series switches running AOS-W 6.3.1.9, in a master-standby topology. **Platform:** OAW-6000 Series switches. **Reported Version:** AOS-W 6.3.1.9. **Workaround:** None.

Station Management

Table 277: *Station Management Known Issues*

Bug ID	Description
109619	**Symptom:** Clients are unable to associate with an AP. The log files for the event list the reason as **AP is resource constrained**. **Scenario**: This issue is observed due to a resource constraint on the AP when the user connects to the AP for the first time and 802.11r is enabled in the SSID profile. 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:** 802.11r profiles assigned to SSID profiles, should have 802.11r enabled.

Known Issues and Limitations in AOS-W 6.3.1.13

AP-Wireless

Table 278: *AP-Wireless Known Issues*

Bug ID	Description
107197	**Symptom:** The calls made between Vocera badges connected in 2.4G radio sometimes are of bad quality. **Scenario:** This issue is observed in OAW-AP225 connected to switches 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 279: *Base OS Security Known Issues*

Bug ID	Description
106690	**Symptom:** Session ACL with destination as **Netdestination vrrp_ip** applied on the port is not getting hit on the local switch . **Scenario:** This issue is observed during 802.1X authentication of wired and wireless clients. This issue is observed in master–local network topology and is not limited to a specific switch model or release version. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.5. **Workaround:** None.
107688	**Symptom:** After MAC-authentication, when the client L2 roams from one AP to another, the switch does not send re-authentication requests for the session timeout values received by the CPPM. **Scenario:** This issue is observed when the session timeout is sent from an external server to switches. **Platform:** All platforms. **Reported Version:** AOS-W 6.1.3.8. **Workaround:** None.
107895	**Symptom:** The client does not connect to the switch when the **enforce-dhcp** is enabled on the AAA profile. **Scenario:** This issue is observed in the OAW-4704 switches running AOS-W 6.3.1.5. **Platform:** OAW-4704 switches. **Reported Version:** AOS-W 6.3.1.5. **Workaround:** None.

Captive Portal

Table 280: *Captive portal Known Issues*

Bug ID	Description
107681	**Symptom:** Delay in Captive Portal login page or Captive Portal authentication page for wireless clients. **Scenario:** This issue is observed when wireless clients are connected in split-tunnel mode with device-classification enabled (by default). **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.8. **Workaround:** Clear the AAA device cache entries periodically.

Certificate Manager

Table 281: *Certificate Manager Known Issues*

Bug ID	Description
100856	**Symptom:** WebUI user certificate authentication does not work after upgrade to AOS-W 6.3.1.5. **Scenario:** This issue is observed in OAW-4550/4650/4750 Series switch that uses certificate-based web authentication. **Platform:** OAW-4550/4650/4750 Series. **Reported Version:** AOS-W 6.3.1.7. **Workaround:** Use user name and password-based authentication.

Configuration

Table 282: *Configuration Known Issues*

Bug ID	Description
107978	**Symptom:** Information in the tech-support-logs file on the switch is missing. **Scenario:** This issue is observed in OAW-4650 switches running AOS-W 6.3.1.4. **Platform:** OAW-4650 switches. **Reported Version:** AOS-W 6.3.1.4. **Workaround:** None.

Switch-Datapath

Table 283: *Switch-Datapath Known Issues*

Bug ID	Description
95286 98653 98654	**Symptom:** A master switch crashes. The log files for the event listed the reason as **datapath timeout**. **Scenario:** This issue is observed in OAW-4650 switches running AOS-W 6.3.1.1. **Platform:** OAW-4550/4650/4750 Series switches. **Reported Version:** AOS-W 6.3.1.1. **Workaround:** None.
108007	**Symptom:** An AP does not connect to a master switch. This issue occurs when an AP and master switch are located in different locations and are connected through IPsec tunnel. **Scenario:** This issue is observed in OAW-4704 switches running AOS-W 6.3.1.9. **Platform:** OAW-4704 switches. **Reported Version:** AOS-W 6.3.1.9. **Workaround:** None.
108152	**Symptom:** A switch stops responding and reboots. The log files for the event listed the reason for the crash as **datapath timeout**. **Scenario:** This issue is observed in OAW-S3 switches running AOS-W 6.3.1.5. **Platform:** OAW-S3 switches. **Reported Version:** AOS-W 6.3.1.5. **Workaround:** None.

IPsec

Table 284: *IPsec Known Issues*

Bug ID	Description
108038	**Symptom:** When the RAP rebootstrap threshold is high and if the RAP rebootstraps and moves to a different switch because of load balancer, the GRE tunnels on the previous switch to the inner IP of the RAP persists until the RAP rebootstrap is detected. This may result in some BC/MC traffic that is directed to the inner IP of the RAP to be sent in clear text. **Scenario:** This issue is observed when GRE tunnels exist for the inner IP of a RAP even though there is no IPsec security association. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.6. **Workaround:** None.

Remote AP

Table 285: *Remote AP Known Issues*

Bug ID	Description
108030	**Symptom**: RAP does not come up on the switch. **Scenario**: This issue is observed in a master-local topology on OAW-4650 switches running AOS-W 6.3.1.7 **Platform**: OAW-4650 switches. **Reported Version**: AOS-W 6.3.1.7. **Workaround**: None.

Known Issues and Limitations in AOS-W 6.3.1.11

The following issues and limitations are observed in AOS-W 6.3.1.11. Applicable workarounds are included.

AP-Platform

Table 286: *AP-Platform Known Issues*

Bug ID	Description
105930	**Symptom:** Access Points reboot when the customer executes the **show ap debug client-stats <client-mac>** command. **Scenario:** This issue is observed when a message is sent to the AP after the command is executed and if the response is larger than the network MTU size then it is fragmented. If there is an issue with the network the response does not reach the switch, so the switch waits for a period of time, and sends the request again. During this timeframe, no other AP messages are processed which causes other APs to reboot. This issue is observed in APs running AOS-W 6.3 or later versions. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.9. **Workaround:** If this issue is observed do not execute the debug command.
106689	**Symptom:** The station management module on a local switch crashes causing all APs to failover to the master switch. **Scenario:** This issue occurs due to memory corruption and is observed on OAW-4x50 Series switches running AOS-W 6.3.1.9. **Platform:** OAW-4x50 Series switches. **Reported Version:** AOS-W 6.3.1.9. **Workaround:** None.

Base OS Security

Table 287: *Base OS Security Known Issues*

Bug ID	Description
106121	**Symptom:** SNMP traps for ARP spoofing are not sent. **Scenario:** This issue is observed when **Prohibit ARP Spoofing** is enabled. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.9. **Workaround:** None.

Captive Portal

Table 288: *Captive Portal Known Issues*

Bug ID	Description
105811	**Symptom:** Captive portal users are not able to view the login page and are unable to authenticate their credentials after accessing the page. **Scenario:** This issue is observed on OAW-S3 switches and is not limited to any specific version of AOS-W. This issue is observed when clients are configured to a use a forward proxy for Internet traffic and when user traffic trying to access captive portal increases to an excess of 250 users. **Platform:** OAW-S3 switches. **Reported Version:** AOS-W 6.3.1.9. **Workaround:** None
106431	**Symptom:** Captive portal login page does not appear and authentication is incomplete for users associated with APs terminating on OAW-4750 switch. **Scenario:** This issue is observed in OAW-4750 switches where an external CPPM is used for authentication and when MAC caching is enabled on CPPM. **Platform:** OAW-4750 switch. **Reported Version:** AOS-W 6.3.1.6. **Workaround:** Set web-max-clients under web-server to 150 and set the default values for CP logon min, CP logon max, and CP logon cpu threshold.

Switch-Datapath

Table 289: *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.
102597	**Symptom:** A local switch reboots unexpectedly. The log files for the event listed the reason for the reboot as **datapath timeout**. **Scenario:** This issue is observed on OAW-S3 switch running AOS-W 6.3.1.5. **Platform:** OAW-S3 switch. **Reported Version:** AOS-W 6.3.1.5. **Workaround:** None.
104824	**Symptom:** Wireless clients are unable to pass traffic after obtaining the DHCP IP address. **Scenario:** This issue is observed on switches running AOS-W 6.3.1.6. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.6. **Workaround:** None.
105967	**Symptom:** Although guest users receive the IP address, some guest users are unable to pass traffic. **Scenario:** This issue is observed on switches running AOS-W 6.3.1.6. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.6. **Workaround:** None.

Switch-Platform

Table 290: *Switch-Platform Known Issues*

Bug ID	Description
93480 95071 95444 97548 97835 98115 98262	**Symptom:** The command-line interface of a switch running AOS-W 6.2.x.x and 6.3.x x can become unresponsive. The output of the **show process monitor statistics** command shows multiple switch processes that are unresponsive. **Scenario**: This issue occurs on a master switch that was previously configured as a local switch. **Platform:** OAW-4704 switches. **Reported Version:** AOS-W 6.3.1.1. **Workaround**: The workaround to this issue requires shell access to the switch. Contact customer support for details.
104729	**Symptom:** Station Management (STM) and WLAN Management System (WMS) crashes continuously. **Scenario**: This issue occurs due to database table corruption. This issue is observed in switches running AOS-W 6.3.x and later. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.9. **Workaround**: Execute the `wms reinit-db` command that re-initializes the WMS database.
106426	**Symptom:** A master switch is very slow and does not respond to some output commands. Processes such as CFGM, STM, and WMS stops responding. **Scenario**: This issue is observed on OAW-S3 switches in a master-local topology running AOS-W 6.3.x and 6.4.x. **Platform:** OAW-S3 switches. **Reported Version:** AOS-W 6.3.1.8. **Workaround**: None.

Master-Redundancy

Table 291: *Master-Redundancy Known Issues*

Bug ID	Description
104636 104989	**Symptom:** 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 **dbsync** process causes this issue. This issue is observed in a master-standby topology running AOS-W 6.3.x. **Platform:** OAW-4650 switch. **Reported Version:** AOS-W 6.3.1.8. **Workaround:** If there is no custom Captive Portal data, disable **database synchronize captive-portal-custom**. If there is custom Captive Portal data, follow the steps mentioned below: 1. Enable **database synchronize captive-portal-custom**. 2. Under **enable** mode, issue the **database synchronize** command to manually synchronize the database. Captive Portal custom pages will be synchronized to the standby switch. 3. Disable **database synchronize captive-portal-custom**. 4. Repeat steps 1-3 whenever Captive Portal custom pages change.

Station Management

Table 292: *Station Management Known Issues*

Bug ID	Description
106430	**Symptom**: The station management module crashes and the switch reboots causing all APs to failover to the master switch. **Scenario**: This issue occurs due to memory corruption in the station management module. **Platform**: All platforms. **Reported Version**: AOS-W 6.3.1.6. **Workaround**: None.

TACACS

Table 293: *TACACS Known Issues*

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

Known Issues and Limitations in AOS-W 6.3.1.10

The following issues and limitations are observed in AOS-W 6.3.1.10. Applicable workarounds are included.

AP-Platform

Table 294: *AP-Platform Known Issues*

Bug ID	Description
98691 99575	**Symptom:** The status of the AP shows down in the master switch although it is up in the local switch. **Scenario:** This issue is seen in a master-local topology when the master and local switches are upgraded to AOS-W 6.3.1.5. This issue is observed in OAW-4550/4650/4750 Series switch running AOS-W 6.3.1.4. **Platform:** OAW-4550/4650/4750 Series. **Reported Version:** AOS-W 6.3.1.4. **Workaround:** Reboot the APs that show the status as down.
105120	**Symptom:** An AP provisioned with LMS and backup-LMS in AP system profile is initially terminating on primary LMS. When the switch associating with the AP and switch is rebooted, the AP is not re-associating with the primary switch unless the AP is manually rebooted. **Scenario:** This issue is observed in a setup where: • Both LMS and backup-LMS exists in AP system profile. • AP receives at least three different LMS IPs during reboot. In this case, the first IP is the master switch IP, the second IP is the server IP, and the third IP is the dns resolution of Alcatel-Lucent-master switch. • CPSEC is enabled and RAP included. This issue is triggered when the number of LMS IPs are not set correctly. The number of IPs received must not exceed two. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.5. **Workaround:** Change the AP boot parameters so that AP receives no more than two LMS IPs. Do not configure LMS and backup-LMS in the AP system profile, if it is not required.
104268	**Symptom:** In the master switch, the OAW-AP65 devices that were removed are displayed as 'up' although they are no longer present on the local switch. **Scenario:** This issue is observed in the master-local topology running AOS-W 6.3.1.8. **Platform:** OAW-AP65 access points. **Reported Version:** AOS-W 6.3.1.8. **Workaround:** Reset the link between master and local to show the status of all APs as ‘down’.

AP-Wireless

Table 295: *AP-Wireless Known Issues*

Bug ID	Description
100371	**Symptom:** Communication badges are unable to connect to OAW-AP225 intermittently. **Scenario:** This issue is observed in OAW-AP225 connected to switch running AOS-W 6.3.1.6. **Platform:** OAW-AP225 access points. **Reported Version:** AOS-W 6.3.1.6.

Base OS Security

Table 296: *Base OS Security Known Issues*

Bug ID	Description
104275	**Symptom:** 801.X authentication for wired clients is not being processed as the switch is unable to send the radius requests. **Scenario:** This issue is observed on all the switches running AOS-W 6.3.1.6. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.6. **Workaround:** Restart authmgr.
104674	**Symptom:** A client connected to a OAW-4550 switch is unable to communicate on RAP bridge. **Scenario:** This issue is observed in RAP bridge mode on OAW-4550 switches with OAW-AP105 devices running AOS-W 6.3.1.5. **Platform:** OAW-4550 switches. **Reported Version:** AOS-W 6.3.1.5. **Workaround:** None.

Certificate Manager

Table 297: *Certificate Manager Known Issues*

Bug ID	Description
100856	**Symptom:** Web UI user certificate authentication does not work after upgrade to AOS-W 6.3.1.5. **Scenario:** This issue is observed in OAW-4550/4650/4750 Series switch that uses certificate-based web authentication. **Platform:** OAW-4550/4650/4750 Series switches **Reported Version:** AOS-W 6.3.1.7. **Workaround:** Use user name and password-based authentication.

Switch-Datapath

Table 298: *Switch-Datapath Known Issues*

Bug ID	Description
95286 98653 98654	**Symptom:** A master switch crashes with the log message, **datapath timeout**. **Scenario:** This issue is observed in OAW-4650 switches running AOS-W 6.3.1.1. **Platform:** OAW-4550/4650/4750 Series switches. **Reported Version:** AOS-W 6.3.1.1. **Workaround:** None.
96672	**Symptom:** A local OAW-S3 switch crashes and reboots with reboot cause **Datapath timeout**. **Scenario:** This issue occurs on the OAW-S3 switch after upgrading to AOS-W 6.3.1.2. **Platform:** OAW-S3 switches. **Reported Version:** AOS-W 6.3.1.2. **Workaround:** None.
101931	**Symptom:** The Address Resolution Protocol (ARP) entries age out and are not refreshed on the default gateway of the switch. **Scenario**: This issue is observed in OAW-6000 Series switches running AOS-W 6.3.1.6. **Platform:** OAW-6000 Series switches. **Reported Version:** AOS-W 6.3.1.6. **Workaround**: None.

Table 298: *Switch-Datapath Known Issues*

Bug ID	Description
104272 104273	**Symptom:** The OAW-4550 and OAW-S3 switches reboots unexpectedly and the logs for the event listed the reason for the crash as **datapath timeout**. **Scenario:** This issue is observed when the OAW-AP225 is introduced in the network and any form of packet loop exists between OAW-AP225 and the switch. This issue is observed in OAW-4550 and OAW-S3 switches running AOS-W 6.3.1.5 and above. **Platform:** OAW-AP225 access points. **Reported Version:** AOS-W 6.3.1.5. **Workaround:** Correct the network configuration in the switch, intermediate switches, and AP to avoid the packet loop.
104824	**Symptom:** Wireless clients are unable to pass traffic after obtaining the DHCP IP address. **Scenario:** This issue is observed on switches running AOS-W 6.3.1.6. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.6. **Workaround:** None.
105285	**Symptom:** Wireless clients are unable to browse the internet. **Scenario:** Following are the observations: • Wireless clients are unable to ping the default gateway. • The clients associate and authenticate successfully. • The clients do not lose access to the IP subnet. • The ARP responses to the default gateway is successful. • Client's ARP table has a record of the default gateway. • DNS queries receive response from servers. This issue is seen on a master-local topology. This issue is observed in OAW-6000 Series switches (local) running AOS-W 6.3.1.5. **Platform:** OAW-6000 Series switches. **Reported Version:** AOS-W 6.3.1.5. **Workaround:** None.

Switch-Platform

Table 299: *Switch-Platform Known Issues*

Bug ID	Description
95071 95444 97548 97835 98115 98262 104279	**Symptom:** The command-line interface of a switch running AOS-W 6.2.x.x and 6.3.x x can become unresponsive. The output of the **show process monitor statistics** command shows multiple switch processes that are unresponsive. **Scenario**: This issue occurs on a master switch that was previously configured as a local switch. **Platform:** OAW-4704 switches. **Reported Version:** AOS-W 6.3.1.1. **Workaround**: The workaround to this issue requires shell access to the switch. Contact customer support for details.
103406	**Symptom:** A master switch reboots unexpectedly. The log files for the event listed the reason for the reboot as **Hard Watchdog reset (Intent:cause:register ee:ee:50)**. **Scenario**: This issue is observed when OAW-4x50 switches is upgraded from AOS-W 6.1.4.1 to AOS-W 6.3.1.8. **Platform:** OAW-4x50 switches. **Reported Version:** AOS-W 6.3.1.8. **Workaround**: None.
103416	**Symptom:** A master switch reboots and remains in **cpboot** state.

Table 299: *Switch-Platform Known Issues*

Bug ID	Description
103536	**Scenario**: This issue is observed in OAW-4704 switches running AOS-W 6.3.1.5 in a master-local topology. **Platform:** OAW-4704 switches. **Reported Version:** AOS-W 6.3.1.5. **Workaround**: None.
104724	**Symptom:** A switch reboots unexpectedly and the log files for the event indicate the reasons for the reboot are soft watchdog reset and panic dump is empty. **Scenario**: This issue is observed in OAW-4704 switches running AOS-W 6.3.1.8 **Platform:** OAW-4704 switches. **Reported Version:** AOS-W 6.3.1.8. **Workaround**: None
104729	**Symptom:** Station Management (STM) and WLAN Management System (WMS) crashes continuously. **Scenario**: This issue occurs due to database table corruption. This issue is observed in switches running AOS-W 6.3.x and later. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.9. **Workaround**: This issue is fixed by executing the **wms reinit-db** command that re-initializes the WMS database.
104932	**Symptom:** Switch is not responding and does not produce a crash file. **Scenario**: This issue is observed in OAW-4704 switches running AOS-W 6.3.1.9 **Platform:** OAW-4704 switches. **Reported Version:** AOS-W 6.3.1.9. **Workaround**: Reboot the switch.

Remote AP

Table 300: *Remote AP Known Issues*

Bug ID	Description
102205	**Symptom:** Sierra U320 modem is not functional. **Scenario:** This issue is observed in OAW-RAP155 running AOS-W 6.3.1.6. **Platform:** OAW-RAP155. **Reported Version:** AOS-W 6.3.1.6. **Workaround:** None.
102870	**Symptom**: VoIP phones connected to Ethernet port 2 of OAW-RAP155 acquires an IP address from incorrect VLAN in the tunnel mode. **Scenario**: This issue is observed on OAW-RAP155 running AOS-W 6.3.1.1. **Platform**: OAW-RAP155. **Reported Version**: AOS-W 6.3.1.1. **Workaround**: None.

Voice

Table 301: *Voice Known Issues*

Bug ID	Description

Known Issues and Limitations in AOS-W 6.3.1.9

The following issues and limitations are observed in AOS-W 6.3.1.9. Applicable workarounds are included.

Air Management-IDS

Table 302: *Air Management-IDS Known Issues*

Bug ID	Description
101207	**Symptom:** A master switch reboots unexpectedly. The log files for the event listed the reason as **Nanny rebooted machine - low on free memory**. **Scenario:** This issue is seen when the switch's Warehouse Management System (WMS) database becomes very large in size. This issue is observed in OAW-4604 switches running as a master with multiple local switches. **Platform:** OAW-4604 switches. **Reported Version:** AOS-W 6.3.1.6. **Workaround:** Limit the memory usage of WMS.

AP-Platform

Table 303: *AP-Platform Known Issues*

Bug ID	Description
102637	**Symptom:** OAW-AP105 devices are unable to reassemble PAPI fragments. **Scenario:** This issue is observed in switches running AOS-W 6.3.1.7 with OAW-AP105. **Platform:** OAW-AP105 access points. **Reported Version:** AOS-W 6.3.1.7. **Workaround:** None.

AP Regulatory

Table 304: *AP Regulatory Known Issues*

Bug ID	Description
101265	**Symptom:** Command `show ap active` shows maxEIRP as 0. **Scenario:** This issue is observed in OAW-AP225 connected to switches running AOS-W 6.3.1.6. **Platform:** OAW-AP225 access points. **Reported Version:** AOS-W 6.3.1.6. **Workaround:** None.

AP-Wireless

Table 305: *AP-Wireless Known Issues*

Bug ID	Description
101371	**Symptom**: Communication badges are unable to connect to OAW-AP225 intermittently. **Scenario**: This issue is observed in OAW-AP225 switch running on 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 306: *Base OS Security Known Issues*

Bug ID	Description
103355	**Symptom:** In a master-local setup, enabling the **ssh mgmt-auth public-key** parameter on the master switch synchronizes the configuration on the local switch. But disabling the same parameter on the master switch does not synchronize the configuration on the local switch. **Scenario:** This issue is observed in a master-local deployment, and is not limited to a specific switch or a release version. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.7. **Workaround:** None.

Captive Portal

Table 307: *Captive Portal Known Issues*

Bug ID	Description
104031	**Symptom:** Curl script fails to load guest portals. **Scenario:** With AOS-W 6.3.1.5 security vulnerability enhancement, the GUI of a switch implicitly sends an extra parameter UIDARUBA with value as SESSION ID as part of configuration changing URLs or URLs that perform any kind of write operation on switches. Scripts that use curl command to send similar URLS, for example, **captiveportal_import.html** does not send the extra parameter. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.5. **Workaround:** Add UIDARUBA as one of the argument for the URL **captiveportal_import.html** while performing a POST request.

Switch-Datapath

Table 308: *Switch-Datapath Known Issues*

Bug ID	Description
100817	**Symptom:** The OAW-4x50 local switch reboots unexpectedly. The log files for the event listed the reason for the reboot as **datapath exception**. **Scenario:** This issue is observed on the Serial Gigabit Media Independent Interface (SGMII) (port 0 or port 1) in the OAW-4550/4650/4750 Series switches running AOS-W 6.3.1.6. **Platform:** OAW-4550/4650/4750 Series switches. **Reported Version:** AOS-W 6.3.1.6. **Workaround:** None.
103503	**Symptom:** In split tunnel mode, traffic originating from the client is not captured using the `packet-capture datapath wifi-client` command. Only traffic going to the client is captured. **Scenario:** This issue is observed in OAW-4750 switches running AOS-W 6.3.1.7. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.7. **Workaround:** None.
103914	**Symptom:** Switch reloads because of datapath timeout. **Scenario:** This issue is observed in OAW-4550/4650/4750 Series switches that use 100 Mbps link. **Platform:** OAW-4550/4650/4750 Series switches. **Reported Version:** AOS-W 6.3.1.8. **Workaround:** Use 1 Gbps link.

IPsec

Table 309: *IPsec Known Issues*

Bug ID	Description
102433	**Symptom:** OAW-RAP3WN Remote AP (RAP) frequently rebootstraps. **Scenario:** This issue is observed when the SAPD process on the RAP detects a missed heartbeat and the RAP rebootstraps. This issue is observed on OAW-RAP3WN running AOS-W 6.3.1.7. **Platform:** OAW-RAP3WN. **Reported Version:** AOS-W 6.3.1.7. **Workaround:** None.

WebUI

Table 310: *WebUI Known Issues*

Bug ID	Description
101989	**Symptom:** The AP status is sometimes displayed as inactive when the user tries to view the client activity in the **Monitoring** tab of the switch WebUI. **Scenario:** This issue is observed in OAW-4604 Series switches running AOS-W 6.2.1.x. and 6.3.1.x. **Platform:** OAW-4604 Series switches. **Reported Version:** AOS-W 6.3.1.6. **Workaround:** None.
107290	**Symptom:** Many interfering devices using the corporate SSIDs is displayed in the **Security** tab of the switch WebUI. **Scenario:** This issue is observed in a master-standby setup in OAW-4550/4650/4750 Series switches running AOS-W 6.3.1.x. **Platform:** OAW-4550/4650/4750 Series switches. **Reported Version:** AOS-W 6.3.1.1. **Workaround:** None.

Known Issues and Limitations in AOS-W 6.3.1.8

The following issues and limitations are observed in AOS-W 6.3.1.8. Applicable workarounds are included.

Air Management-IDS

Table 311: *Air Management -IDS Known Issues*

Bug ID	Description
101207	**Symptom:** A master switch reboots unexpectedly. The log files for the event listed the reason as **Nanny rebooted machine - low on free memory**. **Scenario:** This issue is seen when the switch's Warehouse Management System (WMS) database becomes very large in size. This issue is observed in OAW-4604 switches running as a master with multiple local switches. **Platform:** OAW-4604 switches. **Reported Version:** AOS-W 6.3.1.6. **Workaround:** Limit the memory usage of WMS.

AP-Wireless

Table 312: *AP-Wireless Known Issues*

Bug ID	Description
99684	**Symptom:** The last Virtual AP's (VAP) Enhanced Distributed Channel Access (EDCA) profile, applies to all VAPs. **Scenario:** This issue occurs in OAW-AP225 access points connected to switches running AOS-W 6.3 and 6.4. **Platform:** OAW-AP225 access points. **Reported Version:** AOS-W 6.3.1.6. **Workaround:** None.
100390	**Symptom**: OAW-AP93H device crashes and reboots, the log files for the event list the reason for the crash as **Unable to handle kernel paging request at virtual address 000106f4**. **Scenario**: This issue is observed in OAW-AP93H running on AOS-W 6.3.1.5 version. **Platform:** OAW-AP93H access points. **Reported Version:** AOS-W 6.3.1.5. **Workaround:** None.
100533	**Symptom**: In a good RF environment, with no other operations, Spectralink 8440 sometimes roams to a suboptimal AP. **Scenario**: This issue is observed in Spectralink 8440 802.11g devices running firmware 4.3.1.0174. **Platform:** OAW-AP135 access points. **Reported Version:** AOS-W 6.3.1.1. **Workaround:** None.

Base OS Security

Table 313: *Base OS Security Known Issues*

Bug ID	Description
98833	**Symptom:** Auth module on the local switch reboots randomly. **Scenario:** This issue is observed in the FIPS version, when termination is enabled. This issue is observed in switches running AOS-W 6.3 and above. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.4. **Workaround:** None.

Switch-Datapath

Table 314: *Switch-Datapath Known Issues*

Bug ID	Description
100359	**Symptom:** Clients using phones connected to wired ports of RAPs experience poor call quality. **Scenario:** This issue is observed with OAW-RAP2WG, OAW-RAP3WN, and OAW-RAP5WN running AOS-W 6.3.1.0. **Platform:** OAW-RAP2WG, OAW-RAP3WN, and OAW-RAP5WN remote access points. **Reported Version:** AOS-W 6.3.1.0. **Workaround:** None.
100817	**Symptom:** The OAW-4x50 local switch reboots unexpectedly. The log files for the event listed the reason for the reboot as **datapath exception**. **Scenario:** This issue is observed on the Serial Gigabit Media Independent Interface (SGMII) (port 0 or port 1) in the OAW-4550/4650/4750 Series switches running AOS-W 6.3.1.6. **Platform:** OAW-4550/4650/4750 Series switches. **Reported Version:** AOS-W 6.3.1.6. **Workaround:** None.

Known Issues and Limitations in AOS-W 6.3.1.7

The following issues and limitations are observed in AOS-W 6.3.1.7. Applicable workarounds are included.

AP-Platform

Table 315: *AP-Platform Known Issues*

Bug ID	Description
95056	**Symptom:** An OAW-AP120 Series device crashes with the log message **Unhandled kernel unaligned access**. **Scenario:** This issue occurs on OAW-AP120 Series models running AOS-W 6.3.1.2. **Platform:** OAW-AP120 Series access points. **Reported Version:** AOS-W 6.3.1.2. **Workaround:** None.
95260 95266 95337	**Symptom:** An AP occasionally reboots with crash information **cache_alloc_refill**. **Scenario:** This issue occurs on the OAW-AP120 Series models running AOS-W 6.3.1.2. **Platform:** OAW-AP120 Series access points. **Reported Version:** AOS-W 6.3.1.2. **Workaround:** None.
95764	**Symptom:**OAW-AP125 device crashes and reboots, the log files for the event list the reason for the crash as **Kernel unaligned instruction access**. **Scenario:** This issue occurs in OAW-AP125 access points connected to switches running AOS-W 6.3.1.2. **Platform:** OAW-AP120 Series access points. **Reported Version:** AOS-W 6.3.1.2. **Workaround**: None.

AP-Wireless

Table 316: *AP-Wireless Known Issues*

Bug ID	Description
97415	**Symptom:** An access point crashed and rebooted, the log files for the event listed the reason for the crash as **kernel panic**. **Scenario:** This issue is observed in OAW-AP225 access points connected to switches running AOS-W 6.3.1.2. **Platform:** OAW-AP225 access points. **Reported Version:** AOS-W 6.3.1.2. **Workaround:** None
98786	**Symptom:** Multiple APs crash in the network. Users are able to connect to the network and receive the IP address correctly but unable to pass traffic. No Address Resolution Protocol (ARP) entry is found in the switch for these users. **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

ARM

Table 317: *ARM Known Issues*

Bug ID	Description
97935	**Symptom**: OAW-AP135 device is displayed in the ID flag after it is upgraded from AOS-W 6.1.3.4 to 6.3.1.1. **Scenario**: This issue is observed in OAW-4306G switches running AOS-W 6.3.1.1. **Platform:** OAW-AP135 access points. **Reported Version:** AOS-W 6.3.1.1. **Workaround:** None.

Configuration

Table 318: *Configuration Known Issues*

Bug ID	Description
99325	**Symptom:** The ACLs are lost on a standby switch. **Scenario:** This issue is observed on OAW-4650 switches running AOS-W 6.3.1. **Platform:** OAW-4650 switches. **Reported Version:** AOS-W 6.3.1.3. **Workaround:** From the master switch, execute the **clear master-local-session <standby IP>** command.
99934	**Symptom:** User-roles are not present on some local switches after a reboot. **Scenario:** This issue is observed in a master-local setup after upgrading the switch from AOS-W 6.3.1.4 to AOS-W 6.3.1.5. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.4. **Workaround:** None.

Switch-Datapath

Table 319: *Switch-Datapath Known Issues*

Bug ID	Description
95113 95086 95088 95111 95114 95115 95116 95117 95123 95124	**Symptom**: An iPad connected in tunnel mode using CCMP encryption becomes unreachable from the network once Airplay mirroring is initiated from iPad to Apple TV. **Scenario**: This issue occurs when an iPad is connected to a wireless network in forward-mode: Tunnel and opmodes: wpa2-aes/wpa2-psk-aes. This issue is observed in switches and APs running AOS-W 6.3.X.X or 6.4.0.0. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.2. **Workaround**: Disable **Multiple Tx Replay Counters** parameter under SSID profile.

Switch-Platform

Table 320: *Switch-Platform Known Issues*

Bug ID	Description
94862	**Symptom:** The master switch reboots unexpectedly with the message: **user reboot (shell)**. **Scenario:** This issue occurs on the OAW-4550/4650/4750 Series switches with OAW-AP225 devices following an upgrade to AOS-W 6.3.1.3. **Platform:** OAW-AP225 access points. **Reported Version:** AOS-W 6.3.1.2. **Workaround:** None
98202	**Symptom:** A switch stops responding and reboots. The log files for the event listed the reason as **soft watchdog reset**. **Scenario:** This issue is seen during datapath core dump. This issue is observed on OAW-4550/4650/4750 Series switch running AOS-W 6.3.1.2. **Platform:** OAW-4550/4650/4750 Series switches. **Reported Version:** AOS-W 6.3.1.2. **Workaround:** None.
100206	**Symptom:** The switch reboots unexpectedly with the reason as **User Reboot (shell)** at startup. **Scenario:** This issue is observed on OAW-4x50 switches running AOS-W 6.3.1.5. **Platform:** OAW-4x50 switches. **Reported Version:** AOS-W 6.3.1.5. **Workaround**: None.

Master Redundancy

Table 321: *Master Redundancy Known Issues*

Bug ID	Description
98198	**Symptom:** When the user upgrades the switch from 6.1.3.10 to 6.3.1.2, the upgrade fails due to database error and VRRP transition failure. **Scenario:** This issue is observed in switches running AOS-W 6.3.1.2. **Platform:** OAW-S3 switches. **Reported Version:** AOS-W 6.3.1.2. **Workaround:** None.

Startup Wizard

Table 322: *Startup Wizard Known Issues*

Bug ID	Description
100485	**Symptom:** Switch, campus, and Remote AP wizards come up blank with **JS error** in Internet Explorer 9. **Scenario:** This issue is not limited to a specific switch model and is observed in AOS-W 6.3.1.7. **Platform:** All platforms. **Reported Version:** AOS-W 6.3.1.7. **Workaround:** Use Firefox, Internet Explorer 10, Internet Explorer 11, or Safari 5.1.7.

Known Issues and Limitations in AOS-W 6.3.1.6

The following issues and limitations are observed in AOS-W 6.3.1.6. Applicable workarounds are included.

AP-Platform

Table 323: *AP-Platform Known Issues*

Bug ID	Description
96944	**Symptom:** When APs and switches are on the same vlan, HA lite failover with control plane security (CPSec) fails. **Scenario:** APs configured with HA lite and CPSec fails to respond in the Standby mode. This issue is observed in switches running AOS-W 6.3.1.3. **Workaround :** None.

Captive Portal

Table 324: *Captive Portal Known Issues*

Bug ID	Description
97170	**Symptom:** Captive Portal clients are timed out after they are redirected to the external Captive Portal. **Scenario:** This issue is observed on switches where the volume of RAP termination is high and when Captive Portal clients behind RAPs simultaneously try to get authenticated. This issue is observed in OAW-4604, OAW-4704, and OAW-S3 switches. **Workaround:** None.

Hardware Management

Table 325: *Hardware Management Known Issues*

Bug ID	Description
87717	**Symptom:** The switches returns the error, **No such Instance currently exists** while performing an SNMP query on the **wlsxSysExtCpuUsedPercent** OID. **Scenario:** This issue is observed because the hardware monitoring process sometimes fails to respond to the SNMP queries in OAW-4306 and OAW-4306G switches. **Workaround:** None.

OSPF

Table 326: *OSPF Known Issues*

Bug ID	Description
98496	**Symptom:** The traffic from an AP to a switch follows an equal-cost multi-path (ecmp) routing, which is unpredictable. **Scenario:** This issue is observed in the network topology where the ecmp path is defined. This issue is observed in a local switches running AOS-W 6.3.1.1. **Workaround:** Avoid ecmp route configuration.

Known Issues and Limitations prior to AOS-W 6.3.1.6

The following are the known issues and limitations observed in AOS-W 6.3.1.x.

Advanced Monitoring

Table 327: *Advanced Monitoring Known Issues*

Bug ID	Description
88392	**Symptom:** The **Reference count** column in the output of the **show mgmt-server profile <profile-name>** command displays an incorrect reference count value due to an architectural limitation. **Scenario:** This issue is not limited to any specific switch model. **Workaround:** None.
88752 87809	**Symptom:** A crash is observed in the firewall visibility due to DNS cache corruption. **Scenario:** The trigger of this issue is not known and this issue is not limited to any specific switch model or release version. **Workaround:** None.

Air Management

Table 328: *Air Management Known Issues*

Bug ID	Description
86804	**Symptom:** The master switch reboots periodically and displays the message "Nanny rebooted machine - low on free memory." **Scenario:** This issue is observed on the OAW-4504XM switches running AOS-W version 6.3. It occurs when the OAW-4504XM switch is near its memory limit and the customer upgrades to a newer version of AOS-W software that requires more memory than the OAW-4504XM switch is capable of handling. **Workaround:** Tune or disable some features in order to use less memory.

Air Management-IDS

Table 329: *Air Management- IDS Known Issues*

Bug ID	Description
79913	**Symptom**: When configuring an AP in Air Monitor (AM) mode, a user has the option to select the **rare** scan-mode, causing the AP to scan most frequencies in the spectrum, even if they are non-standard channels. Currently some OAW-AP220 Series APs configured to use the **rare** scan mode cannot scan non-standard channels that do not belong to some country's regulatory domain. **Scenario**: This issue occurs on OAW-AP220 Series access points running AOS-W 6.3. **Workaround**: None.

AP-Datapath

Table 330: *AP-Datapath Known Issues*

Bug ID	Description
97147	**Symptom:** The value of session time in the accounting stop request is incorrect for some clients. **Scenario:** This issue is observed when the clients are connected to a RAP in split-tunnel mode using Captive Portal. This issue is not limited to any specific switch model or release version. **Workaround:** None.

AP-Platform

Table 331: *AP-Platform Known Issues*

Bug ID	Description
87138	**Symptom:** The **show running-config** command output does not display the default rf ht-radio profiles (default-a and default-g). **Scenario:** This issue is observed on OAW-4x04 Series switches running AOS-W 6.3 in an all master deployment. **Workaround:** Make any minor configuration change to the default rf ht-radio profiles (default-a and default-g) and revert it.
93344	**Symptom**: Clients are unable to connect to some APs. **Scenario**: This issue is observed in OAW-AP220 Series connected to switches running AOS-W 6.3.1.1. **Workaround**: None
93876	**Symptom:** Occasionally, the CPSEC Campus APs (CAP) unexpectedly reboot. **Scenario:** This issue occurs in all AP platforms with CPESEC and Campus APs (CAP) and may be caused by IKEv2 timing out. **Workaround:** None.

AP-Wireless

Table 332: *AP-Wireless Known Issues*

Bug ID	Description
84884	**Symptom:** Fragmented EAP frames are not sent with the same data rate as a non-fragmented EAP frames. **Scenario:** This issue occurs on 802.11ac access points running AOS-W 6.3.0.0 or later. **Workaround:** None.
87231	**Symptom:** A high CPU utilization is noticed on OAW-AP105 after upgrading to 6.3. However, the client performance is not impacted. **Scenario:** This issue is observed on OAW-AP105 running AOS-W 6.3 deployed in a high Wi-Fi or non-Wi-Fi interference environment. **Workaround:** None

88124	**Symptom**: 802.11ac MacOS clients are unable to pass traffic to APs in tunnel forwarding mode.
	Scenario: This issue may be triggered by issues in the client Broadcom drivers, when there are three MPDUs in an AMSDU packet.
	Workaround: Change the **Maximum number of MSDUs in an A-MSDU** parameters in the high-throughput SSID profile to a value of 2.
	`wlan ht-ssid-profile <profile>`
	`max-tx-a-msdu-count-be 2`
	`max-tx-a-msdu-count-bk 2`

Bug ID	Description
	`max-tx-a-msdu-count-vi 2`
88512	**Symptom**: AnOAW-AP225 access point transmitting A-MPDU aggregate traffic can perform excessive retries. **Scenario**: This issue occurs on an OAW-AP225 in a network environment with a busy channel and a large number of Intel clients. **Workaround**: None.
93342	**Symptom:** There is no traffic from all clients on 802.11g capable access points. **Scenario**: This issue is observed in OAW-AP220 Series connected to switches running AOS-W 6.3.1.1. **Workaround**: None.
93380 93494 93687 93744	**Symptom:** Occasionally, an AP stops responding and reboots. **Scenario:** This issue is observed because of Ethernet connectivity problem leading to loss of connectivity between the AP and switch. This issue occurs on OAW-AP224 and OAW-AP225 models and not limited to a specific AOS-W version. **Workaround**: Ensure that the Ethernet connection issues does not lead to loss of connectivity between the AP and the switch.
93813	**Symptom:** The AP rebooted unexpectedly. **Scenario:** This issue occurs when an internal process fails. This issue is observed in OAW-AP125 connected to switches running AOS-W 6.3.1.0. **Workaround:** None.

Base OS Security

Table 333: *Base OS Security Known Issues*

Bug ID	Description
50206	**Symptom:** Secure Shell (SSH) access to a switch fails to authenticate local database when the RADIUS server is not responsive. **Scenario:** This issue occurs when multiple authentication servers are configured with local authentication enabled. This issue is not specific to any switch model and release version. **Workaround:** None.
86867	**Symptom:** When a user-role and the ACL configured as the ip access-group on the interface for APs/RAPs have the same name, the AP/RAP traffic is hitting the user-role ACL instead of the ip access-group ACL. **Scenario:** This issue is observed on a switch running AOS-W 6.2.1.2. **Workaround:** Do not create an ACL for the IP access-group that has a name matching that of any user-role in the configuration.

Captive Portal

Table 334: *Captive Portal Known Issues*

Bug ID	Description
87294	**Symptom:** Captive Portal (CP) whitelist mapped to the user-role does not get synchronized with the standby switch. **Scenario:** The administrator creates a net-destination and adds it to the CP profile whitelist mapped to the user-role in the master switch. This configuration does not get synchronized with the standby switch. This issue is observed in AOS-W 6.2.1.2 and is not limited to a specific switch model. **Workaround:** None

Switch-Datapath

Table 335: *Switch-Datapath Known Issues*

Bug ID	Description
74428 88758	**Symptom:** On the RJ45 ports 0/0/0 and 0/0/1, if the port speed is forced from 1 Gbps to 10/100 Mbps when traffic is flowing, traffic forwarding on the port can stop in an unintended manner. **Scenario:** This issue has been observed on OAW-4550/4650/4750 Series switches running AOS-W 6.2 in configurations or topologies where traffic is flowing. The trigger is unknown. **Workaround:** Change the speed on the port following these steps: 1. Shut the port. 2. Change the speed on the port. 3. Open the port.
82824	**Symptom**: In some cases, when the number of users is high (more than 16k), a user may be flagged as IP spoofed user with the **Enforce DHCP** parameter is enabled in the AP group's AAA profile. **Scenario**: This issue is observed in switches running AOS-W 6.3. **Workaround**: Disable the **enforce_dhcp** parameter in the AP group's AAA profile.
85368	**Symptom:** After booting up and logging into the switch, the configured message of the day banner does not display. Instead, a portion of the configuration displays. **Scenario:** This issue is observed in switches running AOS-W 6.2 and 6.3, after upgrading a switch with a "banner motd" config that has more than 255 characters in one line. This issue occurs in old versions such as AOS-W 6.1.X-FIPS that do not validate the length per line. **Workaround:** Change the banner to comply with the new character limit per line. You can have more than 1 line of 255 characters. Run the **write-mem** command afterward to fix this issue.
93203 94200	**Symptom:** A local switch reboots unexpectedly. The log files for the event listed the reason for the reboot as **datapath exception**. **Scenario:** This issue is observed in OAW-4650 switch running AOS-W 6.3.1.1 in a master-local topology.
94267	**Symptom**: After an upgrade to AOS-W 6.3.1.x, clients are unexpectedly disconnected from the network, or are unable to pass traffic for 2-3 minutes after roaming between APs. **Scenario**: This issue is observed in Psion Omni handled scanners roaming between OAW-AP175 and OAW-AP120 Series running AOS-W 6.3.1.1. **Workaround**: None.

Switch-Platform

Table 336: *Switch-Platform Known Issues*

Bug ID	Description
84022 86005 86572 87410 87587 85628 82875 88434 88921 88332 88351 89818	**Symptom:** A switch rebooted unexpectedly. **Scenario:** This reboot is caused by a soft watchdog reset. This was observed on AOS-W 6.1.3.x, 6.2.1.x, and 6.3.x, and is not limited to specific switch model. **Workaround:** None.
93465	**Symptom:** A local switch reboots unexpectedly. The log files for the event listed the reason for the reboot as **Control Processor Kernel Panic**. **Scenario:** This issue occurs when the switch releases the memory of corrupted data packets. This issue is observed in OAW-4x04 Series and OAW-S3 switches running AOS-W 6.3.1.1 in a master-local topology. **Workaround:** None.
96923	**Symptom:** When a switch reboots after the upgrade it gets stuck on Mobility Processor Image uptodate page. **Scenario:** This issue is observed when the switch is upgraded from AOS-W 6.3.1.2 to 6.3.1.3 version. **Workaround:** Pressing Esc + Ctrl K followed by few return key presses reboots the switch.
97283	**Symptom:** A local switch crashed and rebooted. The log files for the event listed the reason for the reboot as **watchdog timeout**. **Scenario:** This issue is observed in OAW-4x04 Series switches and OAW-S3 switches running AOS-W 6.3.1.1. **Workaround:** None.
97532	**Symptom:** Users are unable to upgrade a switch using the secure copy method (`scp` command) from Linux. **Scenario:** This issue is observed if the password contains a space. This issue is not limited to any specific switch model or release version. **Workaround:** Use an escape sequence or place the password in double quotes. This can be done only from the Linux shell in the switch.

DHCP

Table 337: *DHCP Known Issues*

Bug ID	Description
94345	**Symptom:** The Symbol N410 barcode scanner and Android devices do not receive an IP address from the internal DHCP server. **Scenario:** This issue is observed on switches running AOS-W 6.3.1.1 and occurs when the switch's internal DHCP is configured to serve IP addresses for these devices. **Workaround:** Use an external DHCP server.

ESI

Table 338: *ESI Known Issues*

Bug ID	Description
88042	**Symptom:** The http traffic from a user is not redirected to the ESI server, even when the ESI server is reachable and the http traffic redirection for the corresponding user role is enabled. **Scenario:** The trigger of this issue is not known. This issue is observed on OAW-4750-US switches running AOS-W 6.3 in a master-local topology. **Workaround:** None

High Availability

Table 339: *High Availability Known Issues*

Bug ID	Description
80206	**Symptom:** The high availability:fast failover feature introduced in AOS-W 6.3 does not support a deployment model where a VRRP-based redundant master pair (a master switch and standby-master switch) is also configured as high availability active-standby pair. **Scenario:** This topology is not supported because the high availability: fast failover feature does not allow the APs to form standby tunnels to the standby master. **Workaround:** None

IPSec

Table 340: *IPSec Known Issues*

Bug ID	Description
80460	**Symptom:** Remote client and Site-to-Site VPN performance is low and does not scale to the switch's limit when IKEv2 with GCM256-EC384 encryption algorithm is configured. **Scenario:** This issue impacts the OAW-4306G switches, OAW-4704 switches, and OAW-4550/4650/4750 Series switches, and occurs when the IKE session is established to a standby unit in a failover deployment. **Workaround:** None.

Local Database

Table 341: *Local Database Known Issues*

Bug ID	Description
95277	**Symptom:** The remote AP whitelist on a master switch is not correctly synchronizing entries to local switches. **Scenario**: This issue occurs in AOS-W 6.3.x.x when the **description** field of a remote whitelist entry contains an apostrophe ('). **Workaround**: Remove the apostrophe from the whitelist entry description.

Master-Local

Table 342: *Master-Local Known Issues*

Bug ID	Description
88430	**Symptom:** User-role configuration is lost after upgrading master, standby, and local switches to AOS-W 6.3.1. **Scenario:** This issue is observed on a OAW-4550/4650/4750 Series switch running AOS-W 6.3.1. **Workaround:** Disabling the configuration snapshot by executing the **cfgm set sync-type complete** command on master and standby switches prevents partial configuration loss. Wait for at least five (5) minutes after the upgraded master and standby have rebooted before reloading the upgraded local switch.

Master-Redundancy

Table 343: *Master-Redundancy Known Issues*

Bug ID	Description
75367	**Symptom**: Enabling web-server debug logging using the CLI command **logging level debugging system subcat webserver** does not take effect until you restart the HTTPD process. **Scenario**: This happens on all switch models running AOS-W 3.x, 5.x, and 6.x software versions when web-server debug logging mode is enabled. **Workaround**: Restart the HTTPD process in order to enable debug logging.
80041 87946 87032 88067	**Symptom:** The `show database synchronize` command from the CLI displays the **FAILED** message. The standby switch database is out-of-sync with the master switch, and any switchover during the out-of-sync state causes the switch to be in an inconsistent state. **Scenario:** This issue occurs in switches running AOS-W 6.3.0.0, in a master-standby configuration. **Workaround:** None.

Port-Channel

Table 344: *Port-Channel Known Issues*

Bug ID	Description
86077	**Symptom:** Users are unable to add a port member to a port-channel due to a speed mismatch error. **Scenario:** This issue occurs if a port-channel member has a different speed when connected to an RJ-45 connector. This issue is observed in OAW-4750 switches running AOS-W 6.3.2.0. **Workaround:** None.

Remote AP

Table 345: *Remote AP Known Issues*

Bug ID	Description
83002	**Symptom**: A wireless client connected to a backup virtual AP, configured in bridge forwarding mode, is unable to get an IP address from an assigned VLAN. **Scenario**: This issue occurs when the switch upgraded to AOS-W 6.2. **Workaround**: Once the AP connects to the switch, remove the virtual AP profile from the ap-group/ap-name configuration, then return the virtual AP profile to the ap-group/ap-name settings.
85249	**Symptom:** A degradation of Transmission Control Protocol (TCP) throughput by 9 to 11 Mbps is observed on a RAP. **Scenario:** This issue occurs in RAPs with any forwarding mode and not specific to any AP model. **Workaround:** None.
89861	**Symptom**: If a OAW-RAP108/ OAW-RAP109 with a USB modem is powered with a Power over Ethernet (PoE) injector, the remote AP might not have sufficient power to activate the USB port, preventing the AP from detecting the USB modem. **Scenario**: This issue is identified on OAW-RAP108/ OAW-RAP109 remote APs powered only by PoE, without an external power source. **Workaround**: Connect a OAW-RAP108/ OAW-RAP109 remote AP with a USB modem to an external power source.
88497	**Symptom:** A OAW-RAP5WN AP using a Sierra Wireless AirCard 313U modem can stop responding when an associated client sends traffic. **Scenario:** This issue only occurs in a 3G network when the AP's cellular network preference setting is configured to use **auto** mode. **Workaround:** Configure the cellular network preference settings in the OAW-RAP5WN AP to use **4G-only** mode to connect to the network.
95277	**Symptom:** When a OAW-RAP3WN is provisioned with an UML295 modem with cellular network preference 3G-only, OAW-RAP3WN does not come up as a cellular RAP. Once OAW-RAP3WN reboots, it comes up as a cellular RAP with 4G-only. **Scenario:** This issue occurs on switches running AOS-W 6.3.1.3. **Workaround:** None.
95997	**Symptom:** A RAP looses connectivity to a switch occasionally only when connected to a UML295 modem as uplink in the bridge mode. **Scenario:** This issue occurs on switches running AOS-W 6.3.1.3. **Workaround:** None.
97516	**Symptom:** OAW-RAP108 is unable to connect to Huawei E176 3G modem. **Scenario:** This issue is observed in OAW-RAP108 running AOS-W 6.3.1.2 in RAP mode. **Workaround:** Use a different supported modem other than Huawei E176 3G.

Station Management

Table 346: *Station Management Known Issues*

Bug ID	Description
82012	**Symptom**: An internal switch process stops responding and restarts, preventing the switch from servicing clients. **Scenario**: This issue is identified when the switch upgrades its image, and is triggered when the switch expects IKEv2 information that is missing from the mysql global AP database. **Workaround**: None.
91758	**Symptom**: Stationary Macbook laptops unexpectedly disassociates from APs, and are temporarily unable to pass traffic for 3-5 minutes during a period when many users on the network roam between APs. **Scenario**: This issue occurs in a network with a OAW-4704 switches running AOS-W 6.3.1.1 with ARM channel assignment and scanning features enabled. **Workaround**: Disable ARM channel assignment and scanning features.
96897	**Symptom:** Stale user entries are not deleted from the user-table. **Scenario:** When a client with two entries for the same mac address and when the older IP address is assigned to a different client, the user-table displays both the entries. This issue is observed on OAW-S3 switches running AOS-W 6.3.1.2 or later. **Workaround:** None.

Voice

Table 347: *Voice Known Issues*

Bug ID	Description
89258	**Symptom:** Lync SDN API-based ALG does not work when clients are behind NAT. **Scenario:** When the user VLANs to which Lync clients are connected have IP NAT inside, or the Lync users are behind a NAT, the Lync SDN API based Lync ALG is not be able to prioritize the Lync traffic. Apart from this, it does not provide the visibility information to these calls through either CLI or dashboard. This issue is observed on a switch running AOS-W 6.3.1. **Workaround:** None.

WebUI

Table 348: *WebUI Known Issues*

Bug ID	Description
55981	**Symptom:** When a user views the Spectrum UI with saved preferences from a newer version of AOS-W, the UI displays charts incorrectly. **Scenario:** After downgrading from a newer version of AOS-W, such as from 6.2.x to 6.1.x with saved Spectrum preferences, the Spectrum UI displays charts incorrectly. This is due to the difference between the Spectrum UI in 6.2 and previous versions. **Workaround:** Use the command **ap spectrum clear-webui-view-settings** on the switch to delete the saved preferences.
77542	**Symptom:** Upgrading from a local file does not work on the OAW-4306 Series switch. **Scenario**: For the local file upgrade to be successful, the switch must have at least 75 MB of free memory. When upgraded to AOS-W 6.2, the OAW-4306 Series switch has only 77 MB of free memory remaining. And when the browser UI is launched, the free memory is decreased to 75 MB. In this case, the local file upgrade will fail. It is recommended that you do not use the local file upgrade function in the switch has less than 80 MB of free memory. **Workaround:** None. Use the USB, TFTP, SCP, or CLI option to upgrade instead.
82611	**Symptom**: The **Dashboard > Access Points** page of the WebUI of a switch running AOS-W 6.2.0.3 does not correctly display AP information. **Scenario**: Accessing the **Dashboard > Access Points** page can trigger the following error in the switch log files: **An internal system error has occurred at file mon_mgr.c function mon_mgr_proc_trend_query line 4142 error PAPI_Send failed: Cannot allocate memory**. This issue is not related to a memory allocation error. **Workaround**: None.
93993	**Symptom:** The **Security** page under the **Dashboard** tab of the switch's WebUI does not display any statistics. **Scenario:** This issue occurs when there is a large number of entries in the WLAN Management System (WMS) database table. This issue is observed when a OAW-4704 master switch is upgraded to AOS-W 6.3.1.1 in a master-local topology. **Workaround:** None.
94723	**Symptom:** The number of radios displayed in the WebUI **Dashboard** is incorrect. **Scenario:** This issue occurs when the AP is rebooted. This issue is observed in switches running AOS-W 6.3. **Workaround:** None.
97281	**Symptom:** Users are unable to configure the extended ACLs using the WebUI. **Scenario:** This issue is observed when PEF license is not installed. This issue is not limited to any specific switch model or release version. **Workaround:** Configure ACL from the CLI.
97710	**Symptom:** The WebUI displays the error, **can't do cli:SID validation failed** when a client logs in after upgrading the switch using the UI. **Scenario:** This issue is observed when a switch is upgraded from 6.1, 6.2, 6.3, or 6.4 to 6.3.1.4. This issue is not limited to any specific switch model. **Workaround:** Clear the browser cache after the image is upgraded.

Issues Under Investigation

The following issues have been reported in AOS-W 6.3.1.16 and are being investigated.

AP-Platform

Table 349: *AP-Platform Issues Under Investigation*

Bug ID	Description
101977	**Symptom:** OAW-AP105 reboots with reason **Testing TPM... Failed -- Rebooting** after upgrading switches from AOS-W 6.1.3.7 to AOS-W 6.3.1.7.
109857	**Symptom:** The AP status is indicated as UP in the database of the master switch even after the AP is removed from the local switch.

AP-Wireless

Table 350: *AP-Wireless Issues Under Investigation*

Bug ID	Description
114143	**Symptom:** When two clients are connected to OAW-AP225 access point, the file transfer speed is very low.

Base OS Security

Table 351: *Base OS Security Issues Under Investigation*

Bug ID	Description
107502 112086	**Symptom:** Bridge mode RAP users are listed in user table of the switch with wrong BSSID. Although the clients get a DHCP assigned IP address in the right VLAN, there is no connectivity.

Captive Portal

Table 352: *Captive Portal Issues Under Investigation*

Bug ID	Description
106014	**Symptom:** Captive Portal redirects wired clients to incorrect web page. This issue is observed in OAW-S3 switches running AOS-W 6.3.1.5.
113376	**Symptom:** Captive Portal unable to redirect and Virtual Router Redundancy Protocol (VRRP) is not able to failover correctly.

Switch-Platform

Table 353: *Switch-Platform Issues Under Investigation*

Bug ID	Description
109839	**Symptom:** The fw_visbility module crashes on a local switch.
111191 111276	**Symptom:** Kernel module crashes and the log files for the event listed the reason for the crash as **hr_timer logic**.

Licensing

Table 354: *Licensing Issues Under Investigation*

Bug ID	Description
106243	**Symptom:** AP count using the **show ap license-usage** command shows discrepancies with the **show ap database** command. The switches are running in a master-local topology. This issue is observed in a OAW-4704 switch running AOS-W 6.3.1.3.

OSPF

Table 355: *Open Shortest Path First (OSPF) Issues Under Investigation*

Bug ID	Description
110409	**Symptom:** The switch drops OSPF adjacency due to high network usage.

WebUI

Table 356: *WebUI Issues Under Investigation*

Bug ID	Description
112425	**Symptom:** User is unable to login to the WebUI of the switch.

Web Server

Table 357: *Web Server Issues Under Investigation*

Bug ID	Description
107596	**Symptom: Httpd_wrap** process is locked in initializing state after upgrading a switch from AOS-W 6.1.3.1 to AOS-W 6.3.1.9. Hence, guest users do not get CP page and GUI is inaccessible.

This chapter details 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

- If your deployment includes OmniVista, you must upgrade to OmniVista 7.7.10. For more information, see AOS-W-OmniVista Cross-Site Request Forgery Mitigation on page 32.
- 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 in 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-4550/4650/4750 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 below ACL, both ACE entries could not be configured in AOS-W 6.3. Once the second ACE entry is added, the first would be over written.

```
(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 multi-switch 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 Multi-Switch Network on page 200.)
- RFPlan and RFLocate are deprecated on the switch. Use VisualRF Plan or VisualRF in OmniVista as replacements for RFPlan and RFLocate. VisualRF adds significant features including 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.

Installing the FIPS Version of AOS-W 6.3.1.x

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

Before Installing FIPS Software

Before you install a FIPS version of software on a switch that is currently running a non-FIPS version of the software, you must reset the configuration to the factory default or you cannot login to the CLI or WebUI. Do this by running the **write erase** command just prior to rebooting the switch. This is the only supported method of moving from non-FIPS software to FIPS software.

Important Points to Remember and Best Practices

Ensure a successful upgrade and optimize your upgrade procedure by taking the recommended actions listed below. 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 during the upgrade, such as configuration changes, hardware upgrades, or changes to the rest of the network. 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 issuing 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.
- 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 are not valid options.
- 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 the current AOS-W release, assess your software license requirements and load any new or expanded licenses you require. For a detailed description of these new license modules, refer to the "Software Licenses" chapter in the 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:

- Issue 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.
- Issue the **show storage** command to confirm that there is at least 60 MB of flash available for an upgrade using the CLI, or at least 75 MB of flash 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 issue the **halt** command before power cycling.

If the output of the **show storage** command indicates that insufficient flash memory space is available, you must free up additional 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 memory before upgrading:

- **Crash Data:** Issue 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 199 to copy the **crash.tar** file to an external server, then issue 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 199 to back up the flash directory to a file named **flash.tar.gz**, then issue the **tar clean flash** command to delete the file from the switch.
- **Log files:** Issue 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 199 to copy the **logs.tar** file to an external server, then issue 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 on 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. Enter **enable** mode in the CLI on the switch, and enter the following command:

   ```
   (host) # write memory
   ```
2. Use 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> <remot
   e 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 Multi-Switch Network

In a multi-switch 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 199.

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 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 requirements are met before starting the upgrade process. See Memory Requirements on page 198 for details.
- User scalability on both the OAW-4306 switch and the OAW-4306G switch has been revised down 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
  - OAW-IAP-VPN

Install Using the WebUI

Confirm that there is at least 60 MB of free memory and at least 75 MB of flash available for an upgrade using the WebUI. For details, see Memory Requirements on page 198.

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 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 to step 11 of the procedure described in Upgrading From a Recent Version of AOS-W to install the interim version of AOS-W, 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 202 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 pre-loaded 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.

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

1. Login to the WebUI to verify all your switches are up after the reboot.

2. Navigate to **Monitoring > 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 199 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 202. 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 Access Points 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 omit 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 available for an upgrade using the CLI. For details, see Memory Requirements on page 198.

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, 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 202 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:

   ```
   (hostname)# ping <ftphost>
   ```

   or

   ```
   (hostname)# ping <tftphost>
   ```

   or

   ```
   (hostname)# ping <scphost>
   ```

4. Use the **show image version** command to check 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**.

   ```
   (hostname) #show image version
   ```

5. Use the **copy** command to load the new image onto the non-boot partition:

   ```
   (hostname)# copy ftp: <ftphost> <ftpusername> <image filename> system: partition <0|1>
   ```

   or

   ```
   (hostname)# copy tftp: <tftphost> <image filename> system: partition <0|1>
   ```

   or

   ```
   (hostname)# copy scp: <scphost> <scpusername> <image filename> system: partition <0|1>
   ```

   or

   ```
   (hostname)# copy usb: partition <partition-number> <image filename> system: partition <0|1>
   ```

The USB option is only available on the OAW-4550/4650/4750 Series switches.

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

   ```
   (hostname)# show image version
   ```

7. Reboot the switch:

   ```
   (hostname)# reload
   ```

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

   ```
   (hostname)# show version
   ```

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

1. Login to the command-line interface to verify all your switches are up after the reboot.
2. Issue the **show ap active** command to determine if your APs are up and ready to accept clients.
3. Issue 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 199 for information on creating a backup.

Downgrading

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

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).

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 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 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 pre-upgrade software version, you must perform the following steps:

1. Back up your switch. For details, see Backing up Critical Data on page 199.
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:
   - 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 sections describe how to use the WebUI to downgrade the software on the switch.

1. If the saved pre-upgrade 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 pre-upgrade 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 pre-upgrade configuration file by navigating to the **Maintenance > Switch > Boot Parameters** page.
   a. Select the saved pre-upgrade 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 pre-upgrade 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 sections describe how to use the CLI to downgrade the software on the switch.

1. If the saved pre-upgrade 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 pre-upgrade configuration file.

```
# 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:

```
#show image version
---------------------------------
Partition               : 0:0 (/dev/hda2)
Software Version        : AOS-W 6.3.1.5(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 6.3.1.6(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:

```
# boot system partition 0
```

5. Reboot the switch:

```
# reload
```

6. When the boot process is complete, verify that the switch is using the correct software:

```
# 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 recreate 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.