AOS-W 6.4.1.0

Release Notes

AOS-W 6.4.1.0 is a software maintenance release that introduces fixes to the issues identified in previous releases, some software enhancements and new hardware support. For more information on the features described in the following sections, see the *AOS-W 6.4.x User Guide*, *AOS-W 6.4.x CLI Reference Guide*, and *AOS-W 6.x MIB Reference Guide*.

See the Upgrade Procedure on page 93 for instructions on how to upgrade your switch to this release.

Chapter Overview

- Features in 6.4.x Releases on page 13 provides description of features and enhancements introduced in AOS-W 6.4.x release versions.
- Regulatory Updates on page 29 describes the regulatory updates in AOS-W 6.4.x release versions.
- Resolved Issues on page 31 describes the issues resolved in AOS-W 6.4.x release versions.
- Known Issues and Limitations on page 77 describes the known and outstanding issues identified in previous AOS-W 6.4.x release versions.
- Upgrade Procedure on page 93 describes the procedures for upgrading a switch to AOS-W 6.4.1.0.

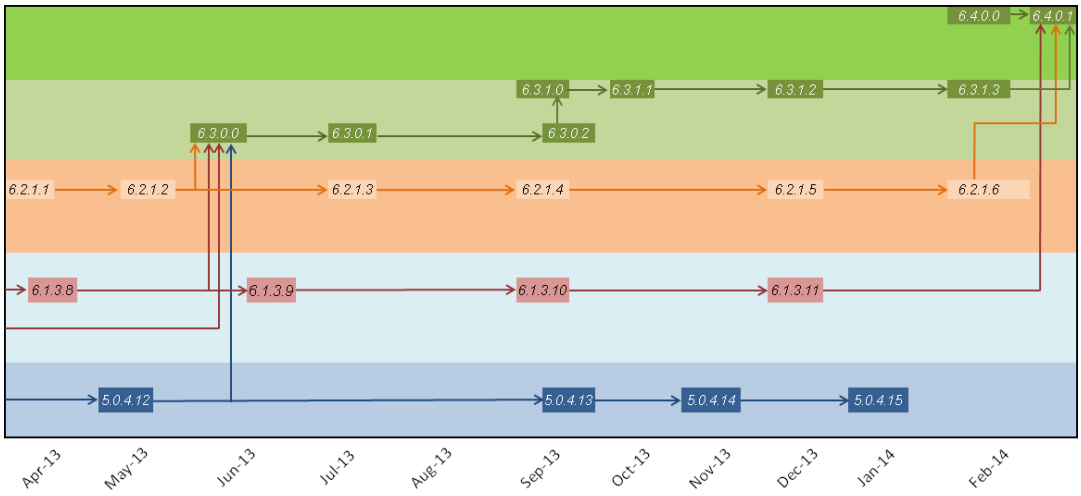
Release Mapping

This version of AOS-W is based off of the AOS-W 6.4.0.1 release. AOS-W 6.4.0.1 includes features and bug fixes from the following releases:

- 6.4.0.3 and all earlier 6.4.x.x releases.
- 6.3.1.7 and all earlier 6.3.x.x releases
- 6.2.1.8 and all earlier 6.2.x.x releases
- 6.1.3.12 and all earlier 6.1.x.x and 6.0.x.x releases
- 5.0.4.15 and all earlier 5.0.x.x releases

The following illustration shows the patch and maintenance releases that are included in their entirety in AOS-W 6.4.0.1:

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



Supported Browsers

The following browsers are officially supported for use with AOS-W 6.4.1.0 WebUI:

- Microsoft Internet Explorer 10.x and 11 on Windows 7 and Windows 8
- Mozilla Firefox 23 or higher on Windows Vista, Windows 7, and MacOS
- Apple Safari 5.1.7 or higher on MacOS

Contacting Support

Table 1: *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 6.4.x release versions. For more information about features introduced in AOS-W 6.4.x, refer to the *AOS-W 6.4.x User Guide*.

Features Introduced in AOS-W 6.4.1.0

This section describes the new features and enhancements introduced in AOS-W 6.4.1.0.

For more information on these features, see the *AOS-W 6.4.x User Guide*.

AP-Platform

Support for OAW-AP103H

The Alcatel-Lucent OAW-AP103H wireless access point supports the IEEE 802.11n standard for high-performance WLAN. It is a dual radio, 2x2:2 802.11n access point. This access point uses MIMO (Multiple-Input, Multiple-Output) technology and other high-throughput mode techniques to deliver high-performance 802.11n 2.4 GHz or 5 GHz functionality while simultaneously supporting existing 802.11a/b/g wireless services. OAW-AP103H is equipped with a total of three active Ethernet ports (ENET 0-2). It is a wall-box type access point. The OAW-AP103H access point works only with an Alcatel-Lucent switch.

The Alcatel-Lucent OAW-AP103H access point provides the following capabilities:

- Wireless transceiver
- Protocol-independent networking functionality
- IEEE 802.11a/b/g/n operation as a wireless access point
- IEEE 802.11a/b/g/n operation as a wireless air monitor
- Compatibility with IEEE 802.3af PoE
- Central management configuration and upgrades through a switch

For more information, see the *Alcatel-Lucent OAW-AP103H Wireless Access Point Installation Guide*.

Support for OAW-AP200 Series

The Alcatel-Lucent OAW-AP200 Series (OAW-AP204 and OAW-AP205) wireless access points support the IEEE 802.11ac and 802.11n standards for high-performance WLAN. It is a dual radio, 2x2:2 802.11ac access point. These access points use MIMO (Multiple-Input, Multiple-Output) technology and other high-throughput mode techniques to deliver high-performance, 802.11n 2.4 GHz and 802.11ac 5 GHz functionality while simultaneously supporting legacy 802.11a/b/g wireless services.

The Alcatel-Lucent OAW-AP200 Series access point provides the following capabilities:

- Wireless transceiver
- Protocol-independent networking functionality
- IEEE 802.11a/b/g/n/ac operation as a wireless access point
- IEEE 802.11a/b/g/n/ac operation as a wireless air monitor
- Compatibility with IEEE 802.3af PoE
- Central management configuration and upgrades through a switch

For more information, see the *Alcatel-Lucent OAW-AP200 Series Wireless Access Point Installation Guide*.

AP Regulatory

Downloadable Regulatory Table

The downloadable regulatory table features allows new regulatory approvals to be distributed without waiting for a new software patch and upgrade. A separate file, called the Regulatory-Cert, containing AP regulatory information will be released periodically on the customer support site. The Regulatory-Cert file can then be uploaded to the Alcatel-Lucent switch and pushed to deployed APs.

Switch-Platform

OAW-40xx Series Switches

The Alcatel-Lucent OAW-40xx Series switches is an integrated switch platform. The platform acts as a software services platform targeting small to medium branch offices and enterprise networks.

The OAW-40xx Series switches include three models that provide varying levels of scalability.

Table 2: *Alcatel-Lucent OAW-40xx Series Switches*

Model	Number of APs Supported	Number of Users Supported
OWA-4005	16	1024
OAW-4010	32	2048
OAW-4030	64	4096

For more information, see the installation guide for each switch model.

AirGroup

The following AirGroup service changes are effective in AOS-W 6.4.1.0:

- The **Chromecast** service is renamed to **DIAL**.
- The **googlecast** service is introduced.

AP Fast Failover Support for Bridge-mode Virtual AP

High Availability (HA) support for bridge mode in Campus AP is introduced in AOS-W 6.4.1.0. In previous versions of AOS-W the fast failover feature for Campus AP was supported using tunnel or decrypt mode. Now support has been extended to bridge mode as well.

AP Fast Failover on bridge forwarding mode virtual AP is supported on OAW-4x50 Series switches only.

DHCP Lease Limit

The following table outlines the maximum number of DHCP leases supported for the new OAW-40xx Series switches.

Table 3: *DHCP Lease Limit*

Platform	DHCP Lease Limit
OWA-4005	512
OAW-4010	1024
OAW-4030	2048

Selective Multicast Stream

The selective multicast group is based only on the packets learned through Internet Group Management Protocol (IGMP).

- When **broadcast-filter all** parameter is enabled, the switch would allow multicast packets to be forwarded only if the following conditions are met:
  - packets originating from the wired side have a destination address range of 225.0.0.0 - 239.255.255.255
  - a station has subscribed to a multicast group.
- When IGMP snooping/proxy is disabled, the switch is not aware of the IGMP membership and drops the multicast flow.
- If Dynamic Multicast Optimization (DMO) is enabled, the packets are sent with 802.11 unicast header.
- If AirGroup is enabled, mDNS (SSDP) packets are sent to the AirGroup application. The common address for mDNS is 224.0.0.251 and SSDP is 239.255.255.250.

Security

Authentication Profile based User Idle Timeout

Starting with AOS-W 6.4.1.0, the **user-idle-timeout** parameter under AAA profile accepts a value of 0. Entering a value of 0, L3 user state is removed immediately upon disassociation. In other words, the switch deletes the user immediately after disassociation or disconnection from the wireless network. If RADIUS accounting is configured, the switch sends an accounting STOP message to the RADIUS server.

User idle timeout of 0 should not be configured for wired, split-tunnel, VIA, and VPN users. It is applicable only for wireless users in tunnel and decrypt-tunnel forwarding modes.

Global Firewall Parameters

This feature works only when L3 user entry exists on the switch.

Starting with AOS-W 6.4.1.0, Address Resolution Protocol (ARP) and Gratuitous ARP packets from wired and wireless clients can be monitored or policed beyond a configured threshold value. The following new parameters are introduced as part of the global firewall parameters:

- **Monitor/police ARP attack**
- **Monitor/police Gratuitous ARP attack**

Additional options to drop excessive packets or blacklist a client is introduced.

Blacklisting of wired clients is not supported.

Features Introduced in AOS-W 6.4.0.2

This section describes the new features introduced in AOS-W 6.4.0.2.

AOS-W-OV3600 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, OV3600 must be upgraded to OV3600 7.7.10 so that it includes the session-ID in its requests.

Upgrade Recommendations

- Upgrade to OV3600 7.7.10 to maintain full functionality.
- Upgrade switches to AOS-W 6.4.0.2 to mitigate CSRF. Switches that are not upgraded will continue to work with the upgraded OV3600 7.7.10 as switches with older AOS-W software image ignore the session-ID in the request.

Fixed Software Versions

- AOS-W 6.4.0.2
- OV3600 7.7.10

Frequently Asked Questions

Q. What happens if I upgrade AOS-W but not OV3600?

A. If you upgrade the switch to AOS-W 6.4.0.2, OV3600 must also be upgraded to version 7.7.10 to maintain full functionality. If OV3600 7.7.10 patch is not applied, client monitoring, AppRF information, and push certificate will not work on the switch with AOS-W 6.4.0.2 software image.

Q. What happens if I upgrade to OV3600 7.7.10 but not all switches to AOS-W 6.4.0.2?

A. If you upgrade to OV3600 7.7.10, switches that are not upgraded to AOS-W 6.4.0.2 will continue to work with the upgraded OV3600 7.7.10, but will 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

EAP-MD5 Support

The switch does not support EAP-MD5 authentication for wireless clients. In AOS-W 6.3.x and AOS-W 6.4, EAP-MD5 authentication for wired clients failed. This issue is fixed in AOS-W 6.4.0.2.

Regulatory Updates

The following table describes regulatory enhancements introduced in AOS-W 6.4.0.2.

Contact your local Alcatel-Lucent sales representative on device availability and support for the countries listed in the following table.

Table 4: *Regulatory Domain Updates*

Regulatory Domain	Change
India	Added support for OAW-AP175DC access point.
Senegal	Added support for OAW-AP134 and OAW-AP135 access points.

Periodic regulatory changes may require modifications to the list of channels supported by an AP. For a complete list of channels supported by an 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>**.

The following example shows indoor, outdoor and DFS channels supported by an 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
```

Features Introduced in AOS-W 6.4.0.0

This section describes the new features introduced in AOS-W 6.4.0.0.

AP-Platform

Support for the OAW-AP270 Series

The Alcatel-Lucent OAW-AP274 and OAW-AP275 are environmentally hardened, outdoor rated, dual-radio IEEE 802.11ac wireless access points. These access points use MIMO (Multiple-in, Multiple-out) technology and other high-throughput mode techniques to deliver high-performance, 802.11ac 2.4 GHz and 5 GHz functionality while simultaneously supporting existing 802.11a/b/g/n wireless services.

Support for the OAW-AP103

The Alcatel-Lucent OAW-AP103 wireless access point supports the IEEE 802.11n standard for high-performance WLAN. This access point uses MIMO (Multiple-in, Multiple-out) technology and other high-throughput mode techniques to deliver high performance, 802.11n 2.4 GHz or 5 GHz functionality while simultaneously supporting existing 802.11a/b/g wireless services.

Hotspot 2.0

Hotspot 2.0 is a Wi-Fi Alliance Passpoint specification based upon the 802.11u protocol that provides wireless clients with a streamlined mechanism to discover and authenticate to suitable networks, and allows mobile users the ability to roam between partner networks without additional authentication.

AOS-W 6.4 supports Hotspot 2.0 with enhanced network discovery and selection. Clients can receive general information about the network identity, venue and type via management frames from the Alcatel-Lucent AP. Clients can also query APs for information about the network's available IP address type (IPv4 or IPv6), roaming partners, and supported authentication methods, and receive that information in Information Elements from the AP.

AOS-W 6.4 supports several ANQP and H2QP profile types for defining Hotspot data. The following table describes the profiles in the Hotspot profile set.

Table 5: *ANQP and H2QP Profiles referenced by an Advertisement Profile*

Profile	Description
Hotspot Advertisement profile	An advertisement profile defines a collection of ANQP and H2QP profiles. Each hotspot 2.0 profile is associated with one advertisement profile, which in turn references one of each type of ANQP and H2QP profile.
ANQP 3GPP Cellular Network profile	Use this profile to define priority information for a 3rd Generation Partnership Project (3GPP) Cellular Network used by hotspots that have roaming relationships with cellular operators.
ANQP Domain Name profile	Use this profile to specify the hotspot operator domain name.
ANQP IP Address Availability profile	Use this profile to specify the types of IPv4 and IPv6 IP addresses available in the hotspot network.
ANQP NAI Realm profile	This profile identifies and describes a Network Access Identifier (NAI) realm accessible using the AP, and the method that this NAI realm uses for authentication.
ANQP Network Authentication profile	Use the ANQP Network Authentication profile to define the authentication type used by the hotspot network.
ANQP Roaming Consortium profile	Name of the ANQP Roaming Consortium profile to be associated with this WLAN advertisement profile.
ANQP Venue Name profile	Use this profile to specify the venue group and venue type information be sent in an Access network Query Protocol (ANQP) information element in a Generic Advertisement Service (GAS) query response.
H2QP Connection Capability profile	Use this profile to specify hotspot protocol and port capabilities.
H2QP Operating Class Indication profile	Use this profile to specify the channels on which the hotspot is capable of operating.
H2QP Operator Friendly Name profile	Use this profile to define the operator-friendly name sent by devices using this profile.
H2QP WAN Metrics profile	Use this profile to specify the WAN status and link metrics for your hotspot.

OAW-AP220 Series Enhancements

The following enhancements have been made to the OAW-AP220 Series access point:

- DTIM per VAP support
- CAC and TSPEC handling
- Multi-client performance tuning

OAW-AP130 Series Functionality Improvements when Powered Over 802.3af (POE)

Starting with AOS-W 6.4, all features and both Ethernet ports of the OAW-AP130 Series are supported when the AP is powered by 802.3af POE.

Franklin Wireless U770 4G Modem Support

AOS-W 6.4 introduces support of the Franklin Wireless U770 4G USB cellular modem for the Sprint LTE service on the OAW-RAP155.

Huawei E3276 LTE Modem Support

AOS-W 6.4 introduces support of the Huawei E3276 LTE USB cellular modem on the OAW-RAP3WN, OAW-RAP108, OAW-RAP109, and OAW-RAP155.

Authentication

Authentication Server Limits

Starting with AOS-W 6.4, a maximum of 128 LDAP, RADIUS, and TACACS servers, each can be configured on the switch.

EAP-MD5 Support

The switch does not support EAP-MD5 authentication for wireless clients. In AOS-W 6.3.x and AOS-W 6.4, EAP-MD5 authentication for wired clients fails. This issue is under investigation and expected to be fixed in the upcoming AOS-W 6.3.x and AOS-W 6.4.x patch releases.

Switch-Platform

AirGroup

Default Behavior Changes

Starting from AOS-W 6.4, AirGroup is disabled by default. If you upgrade from an existing non-AirGroup version to AirGroup 6.4 or perform the fresh installation of AOS-W 6.4, AirGroup is disabled by default. If you run an earlier version of AOS-W with the AirGroup enabled and upgrade to AOS-W 6.4, AirGroup feature is enabled.

The following AirGroup features are introduced in AOS-W 6.4:

AirGroup DLNA UPnP Support

AOS-W 6.4 introduces the support for DLNA (Digital Living Network Alliance), a network standard that is derived from UPnP (Universal Plug and Play) in addition to the existing mDNS protocol. DLNA uses the Simple Service Discovery Protocol (SSDP) for service discovery on the network. DLNA provides the ability to share digital media between multimedia devices like Windows and Android, similar to how mDNS supports Zero Configuration Networking to Apple® devices and services.

AOS-W 6.4 ensures that DLNA seamlessly works with the current mDNS implementation. All the features and policies that are applicable to mDNS are extended to DLNA. This ensures full interoperability between compliant devices.

AirGroup mDNS Static Records

AirGroup processes mDNS packets advertised by servers and creates the relevant cache entries. When a query comes from a user, AirGroup responds with the appropriate cache entries with the relevant policies applied. Starting from AOS-W 6.4, AirGroup provides the ability for an administrator to add the mDNS static records to the cache.

Group Based Device Sharing

AOS-W 6.4 AirGroup supports the sharing of AirGroup devices such as AppleTV, or Printers to a **User Group** using CPPM. This is an enhancement to features that support device sharing based upon the user's username, user-role, and location.

AirGroup-WebUI Monitoring Dashboard Enhancements

This release of AOS-W provides the following enhancements to the AirGroup WebUI:

- **Usage** - You can view the following enhancements in the **Usage** page of the WebUI:
  - The AirGroup service names in the **AirGroup** row are now clickable. If you click a service, you are redirected to the **Dashboard** > **AirGroup** page that displays a list of AirGroup servers filtered by Service Name.
- **Clients** - You can view the following enhancements in the **Clients** page of the WebUI:
  - Under **Dashboard** > **Clients**, a new **AirGroup** column is added to display the devices that are listed as mDNS, DLNA, or both. If a device does not support both **mDNS** and **DLNA**, this field is blank.
- **AirGroup** - You can view the following enhancements in the **AirGroup** page of the WebUI:
  - A new **AirGroup type** column is added and this column specifies if the type of the AirGroup device is mDNS, DLNA or both.
  - The MAC address of each AirGroup user and server is now clickable. If you click MAC link, you are redirected to the **Dashboard** > **Clients** > **Summary page** > **AirGroup** tab. If an AirGroup user or AirGroup server is a wired trusted client, the MAC address is not clickable.

AirGroup-Limitations

The AirGroup feature has the following limitations in AOS-W 6.4:

- AirGroup's DLNA discovery works across VLANs, however, media streaming from Windows Media Server does not work across VLANs. This limitation is a result of Digital Rights Management (DRM) support in Windows Media Server, which restricts media sharing across VLANs. Media streaming works only when both client and server are connected to the same VLAN.
- Android devices cannot discover media server while using the native music and video player applications and when they are connected across VLANs. For example, Samsung Tab 3 cannot discover the media server on Samsung Galaxy S4 while using the native music and video player applications. Android devices can discover media server when they are connected in the same VLAN. This restriction is caused by Samsung devices.
- Xbox cannot be added as an extender to the Windows clients using the Windows Media Center application with the AirGroup feature enabled. You need to disable the AirGroup feature before adding Xbox as an extender.

AppRF 2.0

The AppRF 2.0 feature improves application visibility and control by allowing you to configure and view access control list (ACL), bandwidth application, and application category-specific data. AppRF 2.0 supports a Deep Packet Inspection (DPI) engine for application detection for over a thousand applications. All wired and wireless traffic that traverses the switch can now be categorized and controlled by application and application category.

AppRF 2.0 provides the ability to:

- permit or deny an application or application category for a specific role. For example, you can block bandwidth monopolizing applications on a guest role within an enterprise.
- rate limit an application or application category, such as video streaming applications, for a specific role.
- mark different L2/L3 Quality of Service (QoS) for an application or application category for a user role. For example, you can mark video and voice sessions that originate from wireless users with different priorities so that traffic is prioritized accordingly in your network.

Policy Configuration

Access control lists now contain new application and application category options that let you permit or deny an application /application category on a given role.

Global Session ACL

A new session ACL has been added named "global-sacl." This session, by default, is in position one for every user role configured on the switch. The global-sacl session ACL has the following properties:

- cannot be deleted.
- always remains at position one in every role and its position cannot be modified.
- contains only application rules.
- can be modified in the WebUI and dashboard on a master switch.
- any modifications to it results in the regeneration of ACE's of all roles.

Role Default Session ACL

You can configure role-specific application configuration using the WebUI and dashboard. For example, you can deny the facebook application on the guest role using the dashboard without having to change the firewall configuration.

A new role session ACL named apprf-"role-name"-sacl has been added. This session, by default, is in position one for every user role configured on the switch.

The string "apprf" is added to the beginning and "sacl" to the end of a role's name to form a unique name for role default session ACL. This session ACL is in position 2 of the given user role after the global session ACL and takes the next higher priority after global policy rules.

The predefined role session ACL has the following properties:

- cannot be deleted through the WebUI or CLI. It is only deleted automatically when the corresponding role is deleted.
- always remains at position 2 in every role and its position cannot be modified.
- contains only application rules.
- can be modified using the WebUI or dashboard on a master switch, however any modification results in the regeneration of ACE's for that role.
- cannot be applied to any other role.

Bandwidth Contract Configuration

Bandwidth contract configuration lets you configure bandwidth contracts for both the global or application-specific levels.

Global Bandwidth Contract Configuration

You can configure bandwidth contracts to limit application and application categories on an application or global level.

Role-Specific Bandwidth Contracts

Application-specific bandwidth contracts (unlike "generic" bandwidth-contracts) allow you to control or reserve rates for specific applications only on a per-role basis. An optional exclude list is provided that allows you to exclude applications or application categories on which a generic user/role bandwidth-contract is not applied. The exclude list enables you to give specific enterprise applications priority over other user traffic.

Important points regarding bandwidth contracts include:

- Application bandwidth contracts are per-role by default.
- When an application bandwidth-contract is configured for both a category and an application within the category, always apply the most specific bandwidth contract.

AppRF Dashboard Application Visibility

The AppRF Dashboard Application Visibility feature allows you to configure both application and application category policies within a given user role.

The **AppRF** page on the **Dashboard** tab displays the PEF summary of all the sessions in the switch aggregated by users, devices, destinations, applications, WLANs, and roles.The elements are now represented in box charts instead of pie charts.

Applications and Application Categories containers are only displayed on OAW-4x50 Series switches. The remaining switch platforms will retain AOS-W 6.3.x.x Firewall charts (i.e. without new application classification box chart).

Branch

Centralized BID Allocation

In a Master-Local switch setup, the Master switch runs the Branch ID (BID) allocation algorithm to allocate BID to the branches terminating on it and to the Local switches.

Switch LLDP Support

AOS-W 6.4 provides support for Link Layer Discovery Protocol (LLDP) on switches to advertise identity information and capabilities to other nodes on the network, and store the information discovered about the neighbors.

High Availability

This section describes High Availability features added or modified in AOS-W 6.4.

High Availability Configuration Using the WebUI

The high availability profiles introduced in AOS-W 6.3 can now be configured using the **Configuration > Advanced Services Redundancy** window of the AOS-W 6.4 WebUI. In previous releases, high availability profiles were configured in the **HA** section of the **Configuration > Advanced Services > All Profile Management** window. This section of the WebUI is removed in AOS-W 6.4.

Client State Synchronization

State synchronization improves failover performance by synchronizing client authentication state information from the active switch to the standby switch, allowing clients to authenticate on the standby switch without repeating the complete 802.1X authentication process. This feature requires you to configure the high availability group profile with a pre-shared key. The switches use this key to establish the IPsec tunnels through which they send state synchronization information.

The state synchronization feature limits each high availability group to one IPv4 standby switch and one IPv6 standby switch, or one pair of dual-mode IPv4 and IPv6 switches. Therefore, this feature can only be enabled in high-availability deployments that use the following topologies for each IPv4 or IPv6 switch pair.

- **Active/Active Model**: In this model, two switches are deployed in dual mode. Switch one acts as a 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 will fail over to the other switch, thereby providing high availability redundancy to all APs in the cluster.
- **Active/Standby Model**: In this model, the active switch supports up to 100% of its rated capacity of APs, while the other switch in standby mode is idle. If the active switch fails, all APs served by the active switch will failover to the standby switch.

High Availability Inter-switch Heartbeats

The high availability inter-switch heartbeat feature allows faster AP failover from an active switch to a standby switch, especially in situations where the active switch reboots or loses connectivity to the network.

The inter-switch heartbeat feature works independently from the AP mechanism that sends heartbeats from the AP to the switch. If enabled, the inter-switch heartbeat feature supersedes the AP's heartbeat to its switch. As a result, if a standby switch detects missed inter-switch heartbeats from the active switch, it triggers the standby APs to

failover to the standby switch, even if those APs have not detected any missed heartbeats between the APs and the APs' active switch.

Use this feature with caution in deployments where the active and standby switches are separated over high-latency WAN links.

When this feature is enabled, the standby switch starts sending regular heartbeats to an AP's active switch as soon as the AP has an UP status on the standby switch. The standby switch initially flags the active switch as *unreachable*, but changes its status to *reachable* as soon as the active switch sends a heartbeat response. If the active switch later becomes unreachable for the number of heartbeats defined by the heartbeat threshold (by default, five missed heartbeats), the standby switch immediately detects this error, and informs the APs using the standby switch to fail over from the active switch to the standby switch. If, however, the standby switch never receives an initial heartbeat response from the active switch, and therefore never marks the active switch as initially reachable, the standby switch will not initiate a failover.

Extended Standby Switch Capacity

The standby switch oversubscription feature allows a standby switch to support connections to standby APs beyond the switch's original rated AP capacity. This feature is an enhancement from the high availability feature introduced in AOS-W 6.3, which requires the standby switch have a AP capacity equal to or greater than the total AP capacity of all the active switches it supports.

Starting with AOS-W 6.4, an OAW-4x50 Series switch acting as a standby switch can oversubscribe to standby APs by up to four times that switch's rated AP capacity, and a standby OAW-S3 switch module or OAW-4704 switch can oversubscribe by up to two times its rated AP capacity, as long as the tunnels consuming the standby APs do not exceed the maximum tunnel capacity for that standby switch.

OAW-4504XM, OAW-4604, and OAW-4306 Series switches do not support this feature.

Features not Supported on OAW-4306 Series Switches

The OAW-4306 Series switch platforms do not support the following features in AOS-W 6.4.

- AirGroup
- AppRF 1.0/Firewall Visibility
- IF-MAP
- AP Image Preload
- Centralized Image Upgrade
- IAP-VPN

Control Plane Bandwidth Contracts Values

Beginning with AOS-W 6.4, control plane bandwidth contracts are configured in packets per second (pps) instead of bits per second (bps). This makes performance more predictable. The bandwidth contract range is now 1 to 65536 pps. Additionally, show commands related to control plane bandwidth contracts display pps. The formula used to convert bps to pps is **pps=bps/(256 x 8)**.

Automatic GRE from IAP

AOS-W 6.4 introduces automatic GRE tunnel formation between the switch and Instant access points. Manual configuration of GRE is no longer required on the switch. This feature uses the existing IPSec connection with the switch to send control information to set up the GRE tunnel. Since the GRE control information is exchanged through a secure tunnel, security and authentication is addressed.

DHCP Lease Limit

The following table provides the maximum number of DHCP leases supported per switch platform.

Table 6: *DHCP Lease Limit*

Platform	DHCP Lease Limit
OAW-4306	256
OAW-4306G/OAW-4306G	512
OAW-4504XM	512
OAW-4604	512
OAW-4704, OAW-S3	512
OAW-4550	5120
OAW-4650	10240
OAW-4750	15360

IPv6

This section describes IPv6 features added or modified in AOS-W 6.4.

Multicast Listener Discovery (MLDv2) Snooping

This release of AOS-W supports Source Specific Multicast (SSM) and Dynamic Multicast Optimization (DMO) as part of the IPv6 MLDv2 feature.

Source Specific Multicast

The Source Specific Multicast (SSM) supports delivery of multicast packets that originate only from a specific source address requested by the receiver. You can forward multicast streams to the clients if the source and group match the client subscribed source group pairs (S,G).

The switch supports the following IPv6 multicast source filtering modes:

- Include - In Include mode, the reception of packets sent to a specified multicast address is enabled only from the source addresses listed in the source list. The default IPv6 SSM address range is FF3X::4000:1 – FF3X::FFFF:FFFF, and the hosts subscribing to SSM groups can only be in the Include mode.
- Exclude - In Exclude mode, the reception of packets sent to a specific multicast address is enabled from all source addresses. If there is a client in the Exclude mode, the subscription is treated as an MLDv1 join.

Dynamic Multicast Optimization

In a scenario where multiple clients are associated to an AP and one client subscribes to a multicast stream, all clients associated to the AP receive the stream, as the packets are directed to the multicast MAC address. To restrict the multicast stream to only subscribed clients, Dynamic Multicast Optimization (DMO) sends the stream to the unicast MAC address of the subscribed clients. DMO is currently supported for both IPv4 and IPv6.

Understanding MLDv2 Limitations

The following are the MLDv2 limitations:

- Switch cannot route multicast packets.
- For mobility clients mld proxy should be used.

- VLAN pool scenario stream is forwarded to clients in both the VLANs even if the client from one of the VLANs is subscribed.
- DMO is not applicable for wired clients in switches.

Static IPv6 GRE Tunnel Support

Static IPv6 L2/L3 GRE tunnels can be established between Alcatel-Lucent devices and other devices that support IPv6 GRE tunnel. IPv4 and IPv6 L2 GRE tunnels carry both IPv6 and IPv4 traffic. The IPv6 traffic can also be redirected over the IPv4 L3 GRE tunnel.

The following options for directing traffic into the tunnel are introduced for IPv6:

- Static route, redirects traffic to the IP address of the tunnel.
- Firewall policy (session-based ACL), redirects traffic to the specified tunnel ID.

If a VLAN interface has multiple IPv6 addresses configured, one of them is used as the tunnel source IPv6 address. If the selected IPv6 address is deleted from the VLAN interface, then the tunnel source IP is re-configured with the next available IPv6 address.

Important Points to Remember

- By default a GRE Tunnel Interface is in IPv4 L3 mode.
- IPv6 configurations are allowed on an IPv4 Tunnel only if the tunnel mode is set to IPv6. Similarly, IPv4 configurations are allowed on an IPv6 Tunnel only if the tunnel mode is set to IP.

Understanding Static IPv6 GRE Tunnel Limitations

AOS-W does not support the following functions for Static IPv6 GRE Tunnels:

- IPv6 Auto configuration and IPv6 Neighbor Discovery mechanisms do not apply to IPv6 tunnels.
- Tunnel encapsulation limit and MTU discovery options on the IPv6 tunnels.
- You cannot use IPv6 GRE for a master-local setup as IPSec is not supported in this release.

IGMPv3 Support

AOS-W 6.4 supports IGMPv3 functionality that makes Alcatel-Lucent switch aware of Source Specific Multicast (SSM) and optimizes network bandwidth. The SSM functionality is an extension of IP multicast where the datagram traffic is forwarded to receivers from only those multicast sources to which the receivers have explicitly joined. By default, the multicast group range of 232.0.0.0 through 232.255.255.255 (232/8) is reserved for SSM by IANA (Internet Assigned Numbers Authority).

IPv6 Enhancements

This release of AOS-W provides the following IPv6 enhancements on the AP:

- DNS based ipv6 switch discovery
- FTP support for image upgrade in an IPv6 network
- DHCPv6 client support

VRRPv3 Support on Switches

Virtual Router Redundancy Protocol (VRRP) eliminates a single point of failure by providing an election mechanism, among the switches, to elect a master switch. The master switch owns the configured virtual IPv6 address for the VRRP instance. When the master switch becomes unavailable, a backup switch steps in as the master and takes ownership of the virtual IPv6 address.

VRRPv2 support over IPv4 is already present on the Alcatel-Lucent Mobility Switches. VRRPv3 support over IPv6 is introduced in the current version of AOS-W.

Depending on your redundancy solution, you can configure the VRRP parameters on your master and local switches. The following parameters are added in this release.

- IP version - Select IPv4 \ IPv6 from the drop-down list.
- IP \ IPv6 Address - Based on the selection made in the IP version field, either IP Address \ IPv6 Address is displayed. This is the virtual IP address that is owned by the elected VRRP master. Ensure that the same IP address and VRRP ID is used on each member of the redundant pair. Note: The IP address must be unique and cannot be the loopback address of the switch. Only one global IPv6 address can be configured on a VRRP instance.

Understanding VRRP Limitations

- It is not recommended to enable preemption on the master redundancy model. If preemption is disabled and if there is a failover, the new primary switch remains the primary switch even when the original master is active again. The new primary switch does not revert to its original state unless forced by the administrator. Disabling preemption prevents the master from “flapping” between two switches and allows the administrator to investigate the cause of the outage.
- VRRP v2 over IPv4 supports the master-master redundancy model. However, this support is not available in VRRP v3 over IPv6. This model will be supported once support for IPsec over IPv6 is added. Currently only master-local and local-local redundancy are supported.

Security

Palo Alto Networks Firewall Integration

User-Identification (User-ID) feature of the Palo Alto Networks (PAN) firewall allows network administrators to configure and enforce firewall policies based on user and user groups. User-ID identifies the user on the network based on the IP address of the device which the user is logged into. Additionally, firewall policy can be applied based on the type of device the user is using to connect to the network. Since the Alcatel-Lucent switch maintains the network and user information of the clients on the network, it is the best source to provide the information for the User-ID feature on the PAN firewall.

Application Single Sign-On Using L2 Network Information

This feature allows single sign-on (SSO) for different web-based applications using Layer 2 authentication information. Single sign-on for web-based application uses Security Assertion Markup Language (SAML), which happens between the web service provider and an identity provider (IDP) that the web server trusts. A request made from the client to a web server is redirected to the IDP for authentication. If the user has already been authenticated using L2 credentials, the IDP server already knows the authentication details and returns a SAML response, redirecting the client browser to the web-based application. The user enters the web-based application without needing to enter the credentials again.

Enabling application SSO using L2 network information requires configuration on the switch and on the IDP server. The Alcatel-Lucent ClearPass Policy Manager (CPPM) is the only IDP supported.

802.11w Support

AOS-W supports the IEEE 802.11w standard, also known as Management Frame Protection (MFP). MFP makes it difficult for an attacker to deny service by spoofing Deauth and Disassoc management frames.

MFP is configured on a virtual AP (VAP) as part of the **wlan ssid-profile**. There are two parameters that can be configured; **mfp-capable** and **mfp-required**. Both the parameters are disabled by default.

Ability to Disable Factory-Default IKE/IPsec Profiles

This feature enables you to disable default IKE policies, default IPsec dynamic maps, and site-to-site IPsec maps. You can do this by using the **crypto isakmp policy**, **crypto dynamic-map**, and **crypto-local ipsec-map** CLI

commands. Or, use the WebUI and navigate to **Advanced Services > VPN Services > IPSEC** and **Advanced Services > VPN Services > Site-To-Site**.

AOS/ClearPass Guest Login URL Hash

This feature enhances the security for the ClearPass Guest login URL. A new parameter called **url_hash_key** (disabled by default) has been added to the Captive Portal profile so that ClearPass can trust and ensure that the client MAC address in the redirect URL has not been tampered by anyone.

Authentication Server Load Balancing

Load balancing of authentication servers ensures that the authentication load is split across multiple authentication servers, thus avoiding any one particular authentication server from being overloaded. Authentication Server Load Balancing functionality enables the Alcatel-Lucent Mobility Switch to perform load balancing of authentication requests destined to external authentication servers (Radius/LDAP etc). This prevents any one authentication server from having to handle the full load during heavy authentication periods, such as at the start of the business day.

Enhancements in the User Authentication Failure Traps

The output of the **show snmp trap-queue** command has been enhanced to support the information such as Server IP address, user MAC, AP name, authentication failure details, authentication request time out, authentication server down, and up traps messages that are sent to the host.

RADIUS Accounting on Multiple Servers

AOS-W 6.4 provides support for the switches to send RADIUS accounting to multiple RADIUS servers. The switch notifies all the RADIUS servers to track the status of authenticated users. Accounting messages are sent to all the servers configured in the server group in a sequential order.

RADIUS Accounting for VIA and VPN Users

RADIUS Accounting is now supported for VIA and VPN users. A knob has been added under the **AAA Authentication VIA Auth profile** and the **AAA Authentication VPN profile** to enable this feature.

Spectrum Analysis

AP Platform Support for Spectrum Analysis

Starting with AOS-W 6.3.1.0 and AOS-W 6.4, OAW-AP120 Series access points do not support the spectrum analysis feature, and cannot be configured as a spectrum monitor or hybrid AP.

Voice and Video

Unified Communication and Collaboration

This section describes the Unified Communication and Collaboration (UCC) feature introduced in AOS-W 6.4. The Unified Communications Manager (UCM) is the core solution component of this feature. UCC addresses the onslaught of mobile devices that use voice, video, and collaboration applications. This reduces the cost of voice infrastructure for communication and collaboration needs.

UCC continues to support all existing functionality provided by AOS-W 6.3.x. Following are the new sub-features introduced in AOS-W 6.4.

- UCC Dashboard in the WebUI
- UCC **show** commands
- UCC– OV3600 Integration
- Changes to Call Admission Control

- Per User Role Lync Call Prioritization
- Dynamically Open Firewall for UCC Clients using STUN
- UCC Call Quality Metrics

AP Support

AOS-W 6.3.x.x will be the last release to support the OAW-RAP5 access point. AOS-W 6.3 will be supported at least through October 31st 2018. Individual AP support dates will vary based on their end of sale date.

Table 7: *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-AP120, OAW-AP121 (802.11a/b/g)	31-Jan-2012	TBD
OAW-AP120, OAW-AP121 (802.11a/n or 802.11b/g/n)	31-Jan-2012	TBD
OAW-AP124, OAW-AP125 (802.11a/b/g)	1-Aug-2013	TBD
OAW-AP124, OAW-AP125 (802.11a/n and 802.11b/g/n)	1-Aug-2013	TBD
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

MIB and Trap Enhancements

Modified Traps

The following traps are modified in AOS-W 6.4:

- wlsxMgmtUserAuthenticationFailed
- wlsxNUserAuthenticationFailed
- wlsxNAuthServerReqTimeOut
- wlsxNAuthServerTimeOut
- wlsNAuthServerIsDown
- wlsNAuthServerUp

This chapter describes the regulatory updates in AOS-W 6.4.x release versions.

Periodic regulatory changes may require modifications to the list of channels supported by an AP. For a complete list of channels supported by an 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 6.4.0.2

The following table describes regulatory enhancements introduced in AOS-W 6.4.0.2.

Table 8: *Regulatory Domain Updates*

Regulatory Domain	Change
India	Support for OAW-AP175DC access point
Senegal	Support for OAW-AP134 and OAW-AP135 access points

Regulatory Updates in AOS-W 6.4.0.0

The following table describes regulatory enhancements introduced in AOS-W 6.4.0.0.

Table 9: *Regulatory Domain Updates*

Regulatory Domain	Change
Argentina, Uruguay, and Vietnam	Support for OAW-AP92 and OAW-AP93 access points
Uruguay	Support for OAW-AP104 and OAW-AP105 access points
Argentina, Chile, Israel, and Taiwan	Support for OAW-RAP108 and OAW-RAP109 access points
Thailand, Indonesia	Support for the OAW-RAP109 remote access point
Australia, Argentina, Brazil, Chile, China, Colombia, Egypt, Hong Kong, India, Indonesia, Israel, Malaysia, Mexico, New Zealand, Qatar, Russia, Saudi Arabia, Singapore, South Korea, South Africa, Taiwan, Thailand, Trinidad and Tobago, UAE, and Ukraine	Support for OAW-AP110 Series access points

Regulatory Domain	Change
Australia, Chile, China, Egypt, Hong Kong, India, Indonesia, Israel, Japan, Malaysia, Mexico, New Zealand, Qatar, Russia, Saudi Arabia, Singapore, South Africa, Taiwan, Thailand, and Ukraine	Support for OAW-RAP155 and OAW-RAP155P access points
Costa Rica	Support for OAW-AP130 Series access points
Indonesia	Support for OAW-AP175 access points
Nigeria	Support for OAW-AP105 access points
Argentina, Brazil, Chile, India, Indonesia, Israel, Mexico, Philippines, Russia, Taiwan, Trinidad and Tobago, and Ukraine	Support for OAW-AP220 Series access points
China	Support for the OAW-AP224 access point
Argentina, Chile, and Israel	Support for the OAW-RAP3WN and OAW-RAP3WNP access points
Serbia and Montenegro	In addition to the **CS** country code used for both Serbia and Montenegro combined, AOS-W now supports the **RS** country code for Serbia and the **ME** country code for Montenegro.

The following example shows indoor, outdoor and DFS channels supported by an 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
```

This chapter describes the issues resolved in AOS-W 6.4.x release versions.

Resolved Issues in AOS-W 6.4.1.0

The following issues are resolved in AOS-W 6.4.1.0.

AirGroup

Table 10: *AirGroup Fixed Issues*

Bug ID	Description
96233 96235 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 release 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 release version.
97771	**Symptom:** When the user tried to access Google® Chromecast the following error was displayed, **selected device is no longer online**. This issue is resolved by ensuring that the MAC multicast address for Simple Service Discovery Protocol (SSDP) packets is generated correctly. **Scenario:** This issue was observed if a user tried to connect to Chromecast when Airgroup service was enabled. This issue was caused because the switch was not receiving DLNA response from Chromecast for multicast DLNA queries, resulting in missing cache entries on the switch for DIAL service from Chromecast. This issue is observed in all switches running AOS-W 6.4 and later.
100002	**Symptom:** The CPPM server was flooded with AirGroup authorization requests from the switch. The fix ensures that the switch does not send AirGroup authorization requests if an AirGroup device changes its IP address. **Scenario**: This issue was observed on switches running AOS-W 6.3 and later. This issue is observed when a switch sends out RADIUS requests each time an AirGroup user changes the IP address.

Air Management-IDS

Table 11: *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 have fixed this issue. **Scenario:** This issue was identified in an OAW-6000 switch running AOS-W 6.2.0.2 in a master-local topology.
96206	**Symptom:** The WMS module periodically failed to respond to SNMP requests 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. This issue was not limited to any specific switch model or AOS-W release version.

AP Regulatory

Table 12: *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 for EU countries. **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 for EU countries.
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. **Scenario:** This issue was observed when the value of configured tx-power was larger than the MaxEIRP.

AP-Platform

Table 13: *AP-Platform Fixed Issues*

Bug ID	Description
95472 96239	**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.
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.

Table 13: *AP-Platform Fixed Issues*

Bug ID	Description
97544	**Symptom:** OAW-RAP109 could not be used on un-restricted switches that do not have Japan country code. This issue is resolved by mapping the country code in AP regulatory domain profile to the AP regulatory domain enforcement. **Scenario:** This issue was observed when the Instant AP with Japan Stock-Keeping Unit (SKU) was converted to Remote AP running AOS-W 6.3.1.3.
100586	**Symptom:** OAW-AP120 Series (802.11 a/b/g) access point models stopped working after upgrading to AOS-W 6.4.x. Support for OAW-AP120 Series (802.11 a/b/g) access point models are enabled in AOS-W 6.4.x. **Scenario:** This issue was observed in OAW-AP120 Series (802.11 a/b/g) access point models running AOS-W 6.4.x.

AP-Wireless

Table 14: *AP-Wireless Fixed Issues*

Bug ID	Description
83716	**Symptom:** Some of the IEEE 801.11g beacon transmit rates are not supported by OAW-AP220 Series devices. This issue is resolved by allowing beacon transmit rates support for non-basic IEEE 801.11g. **Scenario:** This issue was triggered when non-basic IEEE 801.11g was not allowed to set down at brcm driver. This issue was observed in OAW-AP220 Series devices and OAW-AP270 Series running AOS-W 6.3.0.0.
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.
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.
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 on OAW-AP220 Series running AOS-W 6.3.1.2 version.
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 6.4.x.

Table 14: *AP-Wireless Fixed Issues*

Bug ID	Description
99833 100559	**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.
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 and later versions.
100652 100731	**Symptom:** OAW-AP225 access point was 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.

ARM

Table 15: *ARM Fixed Issues*

Bug ID	Description
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.

Authentication

Table 16: *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 release version.

Base OS Security

Table 17: *Base OS Security Fixed Issues*

Bug ID	Description
88563 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. **Scenario:** This issue was observed during any crypto operation that uses Diffie-Hellman key exchange.
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.
95367	**Symptom:** Issuing the **show rules <role-name>** command from the switch's CLI 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 ACL was configured with spaces in their names. This was not limited to any specific switch model or AOS-W release version.
96755	**Symptom:** Wired 802.1X using EAP-MD5 authentication failed. This issue is resolved by the modifying the authentication code to allow the wired-clients that perform authentication using EAP-MD5 authentication framework. **Scenario:** This Issue was observed when wired clients connected directly either to the switch or to the Ethernet port of a Campus AP or Remote AP. This issue was not limited to a specific switch model or AOS-W release version.
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 parallely processed, but PSK was initiated before MAC Authentication VLAN update. This issue was observed in AOS-W 6.3.1.1.
98492	**Symptom:** When the customer roamed from a 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.
100248	**Symptom:** The Authentication module crashed on an OAW-4550 switch. This issue is resolved by adding preventive checks that prevent a wired user with zero MAC address, and by adding logs and error stats counters to identify occurrence of such crashes. **Scenario:** This issue was observed in a network where the Remote AP and a wired user were on the same switch. This issue is specific to OAW-4550 switches running AOS-W 6.4.0.3.

Captive Portal

Table 18: *Captive Portal Fixed Issues*

Bug ID	Description
98992	**Symptom:** After upgrading from AOS-W 6.1.3.9 to AOS-W 6.3.1.4, captive portal 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 captive portal configuration is complete. **Scenario:** This issue was observed only when multiple CP Authentication configurations were created. This issue was observed in switches running AOS-W 6.4 and AOS-W 6.3.1.3 or later versions.

Certificate Manager

Table 19: *Certificate Manager Fixed Issues*

Bug ID	Description
98565	**Symptom:** When the customer tried to upload a CA Certificate, an error message was displayed - **Not a CA certificate**. This issue is resolved by making code level changes to check if CA is set to true when the certificate is uploaded. **Scenario:** This issue was observed when the customer tried to upload a RAP custom certificate.

Configuration

Table 20: *Configuration Fixed Issues*

Bug ID	Description
95535 95582 99934 100234	**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.

Switch-Datapath

Table 21: *Switch-Datapath Fixed Issues*

Bug ID	Description
84585 92227 92228 92883 94200	**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 OAW-4x50 Series switch connected to 2000 APs when Gratuitous ARP messages were replicated and sent to clients. **Duplicate Bugs:** The following bug IDs have reported similar issues: 96860, 98380
93582	**Symptom:** An 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.
97223	**Symptom:** An L3 GRE tunnel between an 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 devices use the same protocol number in the GRE keep-alive packets. **Scenario:** This issue was observed when Alcatel-Lucent and Cisco devices used different protocol numbers in GRE keep-alive packets, and both the devices dropped the keep-alive 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 6.4.x.
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. **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 6.4.x, in a master-local topology.

Table 21: *Switch-Datapath Fixed Issues*

Bug ID	Description
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 fragments 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.
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. **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.
99483	**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
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.

Switch-Platform

Table 22: *Switch-Platform Fixed Issues*

Bug ID	Description
74428 88758	**Symptom:** On dual-media RJ45 ports 0/0/0 and 0/0/1, if the port speed was forced from/to 1 Gbps to/from 10/100 Mbps when traffic was flowing, traffic forwarding on the port stopped in an unintended manner. This issue is resolved by disabling the port to stop the traffic on the port before changing the speed and re-enabling the port after changing the speed. **Scenario:** This issue was observed in OAW-4x50 Series switches running AOS-W 6.2 in configurations or topologies where traffic is flowing.
76059 85289 92255 93467 93827	**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-4x50 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. **Duplicate Bugs:** The following bug IDs have reported similar issues: 95431, 96293, 96791, 96827, 98196, 99287, 99360, 99362, 99472, 99568, 100857, 100858, 101476
91097 96923	**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.
91541 94045 95079	**Symptom:** A switch rebooted due to low memory. Changes to the switch software fixed this issue.

Table 22: *Switch-Platform Fixed Issues*

Bug ID	Description
	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.
94427 96347 97456 97468 97938	**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. **Duplicate Bugs:** The following bug IDs have reported similar issues: 98425, 98656, 99448, 99919
96712 99920	**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**. Internal changes in the AOS-W code fixed this issue. **Scenario:** This issue was observed in OAW-4750 switches running AOS-W 6.2.1.4.
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.
97388 97658 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 AOS-W release version.
97411 97816 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 occurs due to database table corruption. This issue was observed in switches running AOS-W 6.3 and AOS-W 6.4.
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 various race condition 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-4x50 Series switch running AOS-W 6.3.1.2.
98873 100421	**Symptom:** An 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 in OAW-4306G switch running 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.
99208 99210 99211 99212 99213	**Symptom:** A switch crashes 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 is observed when IGMP snooping or proxy is enabled and users perform multicast streaming. This issue occurs when the user's DHCP pool range is too vast (more than 2 million addresses). This issue is not limited to any specific switch model or AOS-W version.

DHCP

Table 23: *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 release version.

LLDP

Table 24: *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 6.2.1.7.

Local Database

Table 25: *Local Database Fixed Issues*

Bug ID	Description
95277	**Symptom:** Any RAP whitelist entry with special characters failed to synchronize with any switch, and synchronization failed for subsequent whitelist entries. The issue is resolved by correcting the handling of special characters for every field in RAP and CPSEC whitelist entries so that synchronization can happens properly. **Scenario:** This issue was observed where RAP and CPSEC whitelist entries are synchronized on switches running AOS-W 6.3.1.2.

IPsec

Table 26: *IPsec Fixed Issues*

Bug ID	Description
97775 100139	**Symptom:** If a user entered a wrong password, the AOS-W VIA application did not prompt thrice for a password retry. This issue is resolved by sending the **XAUTH STATUS FAIL** message to the AOS-W VIA client before deleting the IKE/IPSec session of the AOS-W 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 AOS-W VIA client.
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 (IAP) manager. **Scenario:** This issue occurred when the 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-4x50 Series switch models, and occurred on AOS-W running 6.3 or later.
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.

Master-Redundancy

Table 27: *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.
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 issue is caused when the user upgrades to AOS-W 6.3 and executes the **write erase all** command.

RADIUS

Table 28: *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.
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 revoking authentication. **Scenario:** This issue was observed when the switch revoked authentication for user entries with multiple IP addresses. This issue was not limited to any specific switch model or AOS-W release version.

Remote AP

Table 29: *Remote AP Fixed Issues*

Bug ID	Description
95572	**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 issues was observed when the OAW-4504XM switch was upgraded from AOS-W 6.1.3.6 to AOS-W 6.3.1.2.
97009	**Symptom:** A RAP failed to establish a PPPoE connection when the RAP's up-link 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.
99466	**Symptom:** The output of the **show iap table** command incorrectly displayed the status of iap (branch) as UP with older tunnel inner ip, after the isakmpd process crashed. The fix ensures that the status of the iap (branch) is updated properly with the new inner ip. **Scenario:** This issue is observed in switches running AOS-W 6.3 and 6.4.

Role/VLAN Derivation

Table 30: *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.
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 switches running AOS-W 6.2.1.4.
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.

Routing

Table 31: *Routing Fixed Issues*

Bug ID	Description
94746	**Symptom:** When the loopback IP address was used as the switch-ip, the switch was not reachable from a wired network after reboot for a specific configuration and timing. The switch was reachable only from the same subnet to which the switch's uplink belongs. This issue was not seen when a VLAN interface was used as the switch-ip. This issue is resolved by maintaining the correct sequence for appropriate execution of the two internal threads . **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-4x50 Series switches running AOS-W 6.3.1.0.

Startup Wizard

Table 32: *Startup Wizard Fixed Issues*

Bug ID	Description
98110	**Symptom:** Mobility Switch **Setup Wizard** page was stuck with Java script error when you clicked **Next** on the **VLANs and IP Interfaces** tab of the switch's WebUI. Changes in the internal XML code fixed this issue. **Scenario:** This issue was not limited to any specific switch model and was observed in AOS-W 6.4.0.2.
98159	**Symptom: Campus WLAN Wizard** page was stuck in **Role Assignment** step when you clicked **Next** on the **Authentication Server** step of the switch's WebUI using Microsoft® Internet Explorer 10 or Internet Explorer 11. Changes in the internal XML code fixed this issue. **Scenario:** This issue is not limited to any specific switch model and is observed in AOS-W 6.4.0.2.

Station Management

Table 33: *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 Station Management module. **Scenario:** This issue was not limited to any specific switch model or AOS-W release version.
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 34: *Voice Fixed Issues*

Bug ID	Description
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.

WebUI

Table 35: *WebUI Fixed Issues*

Bug ID	Description
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.
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.
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 AOS-W 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.
99356	**Symptom:** The WebUI incorrectly displayed that the interface was selected under IGMP in the **Network > IP > IP Interface > Edit VLAN** page even though a port channel was configured in the CLI. The fix ensures that the WebUI correctly displays the configured port channel when IGMP proxy is configured on a VLAN interface. **Scenario:** This issue was observed when the ip igmp **proxy port-channel** command was executed on a VLAN interface. This issue was observed in all the switch platforms.
99471	**Symptom:** The WebUI could not disable IGMP proxy when it was enabled under IGMP in the **Network > IP > IP Interface > Edit VLAN** page. The fix adds a new **Enable IGMP** checkbox under VLAN to enable or disable the IGMP options selected. **Scenario:** The WebUI did not allow disabling both IGMP snooping and IGMP proxy together once either of the radio buttons was selected. This issue was not limited to any specific switch model or AOS-W version.
99961 100373 100771	**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.
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.

XML API

Table 36: *XML API Fixed Issues*

Bug ID	Description
97102 99101	**Symptom:** RADIUS accounting START message did not trigger 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 of AOS-W and AOS-W 6.3 or later versions. **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 AOS-W release version.

Resolved Issues in AOS-W 6.4.0.3

The following issues were resolved in AOS-W 6.4.0.3.

Base OS Security

Table 37: *Base OS Security Fixed Issue*

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 change fixed the issue. **Scenario:** This issue was observed in switches running AOS-W 6.3 or later versions.

Resolved Issues in AOS-W 6.4.0.2

The following issues were resolved in AOS-W 6.4.0.2.

AirGroup

Table 38: *AirGroup 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 was not specific to any switch model.

Application Monitoring (AMON)

Table 39: *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 40: *AP-Platform Fixed Issues*

Bug ID	Description
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 3.4.4.3 and above, or AOS-W 5.0.x (5.0.3.1 or later), or AOS-W 6.0.x (6.0.1.0 or later) to AOS-W 6.4.0.1, APs failed to upgrade to AOS-W 6.4.0.1. A defensive check is made in affected API so that PAPI messages which are smaller than PAPI header size are handled properly in AOS-W 6.0.x compared to AOS-W 5.0.x. **Scenario:** This issue was observed in APs running AOS-W 3.x, or AOS-W 5.0.x (5.0.3.1 or later) or AOS-W 6.0.x (6.0.1.0 or later). APs running AOS-W 6.1 and later versions are 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 mapping the country code in AP regulatory domain profile to the AP regulatory domain enforcement. **Scenario:** This issue was observed when the Instant AP with Japan Stock-Keeping Unit (SKU) was converted to Remote AP running AOS-W 6.3.1.3.

AP-Regulatory

Table 41: *AP-Regulatory Fixed Issues*

Bug ID	Description
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 42: *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 on OAW-AP220 Series running AOS-W 6.3.1.2 version.
97818	**Symptom:** Zebra® QL 420 Plus mobile printer 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 43: *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 44: *Base OS Security Fixed Issues*

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

Captive Portal

Table 45: *Captive Portal Fixed Issues*

Bug ID	Description
92927 94414 97765	**Symptom:** When Apple® 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 46: *Switch-Datapath Fixed Issues*

Bug ID	Description
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.
93582	**Symptom:** AnOAW-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.
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-4x50 Series switches running AOS-W 6.3.

Switch-Platform

Table 47: *Switch-Platform Fixed Issues*

Bug ID	Description
96420 88234 91172 93465 93913	**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. **Duplicate Bugs:** The following bug IDs have reported similar issues: 94754, 95664, 97384, 97761

IPSec

Table 48: *IPSec Fixed Issues*

Bug ID	Description
95634 97749	**Symptom:** Site-to-Site IPsec VPN tunnels randomly lost connectivity on anOAW-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 anOAW-4550 switch running AOS-W 6.3.1.2.

Mobility

Table 49: *Mobility Fixed Issues*

Bug ID	Description
83927	**Symptom:** When the primary HA went down, the alternate HA did not become the home agent for a roaming client although the **auth-sta-roam** parameter was disabled. This issue is resolved by creating a user-entry on the alternate HA using user information from the primary HA when the primary HA goes down. **Scenario:** This issue was observed on switches running AOS-W 6.3 in a setup containing an HA, FA, and an alternate HA with L3 mobility enabled and the **auth-sta-roam** parameter disabled.
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 50: *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 revoking authentication. **Scenario:** This issue was observed when the switch revoked authentication for user entries with multiple IP addresses. This issue was not limited to any specific switch model or release version.

Remote AP

Table 51: *Remote AP Fixed Issues*

Bug ID	Description
97009	**Symptom:** A RAP failed to establish a PPPoE connection when the RAP's up-link 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 52: *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 53: *Voice Fixed Issues*

Bug ID	Description
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.

WebUI

Table 54: *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.
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**.**
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.

Resolved Issues in AOS-W 6.4.0.1

The following issues were resolved in AOS-W 6.4.0.1:

PhoneHome

Table 55: *PhoneHome Fixed Issues*

Bug ID	Description
96789	**Symptom**: Starting with AOS-W 6.4.0.1, PhoneHome automatic reporting is disabled by default. This is a change in behavior from AOS-W 6.4.0.0, as this feature was automatically enabled when the switch upgraded to AOS-W 6.4.0.0. **Scenario**: This change in behavior impacts switches upgrading to AOS-W 6.4.0.1.

Resolved Issues in AOS-W 6.4.0.0

The following issues were resolved in AOS-W 6.4.0.0.

802.1X

Table 56: *802.1X Fixed Issues*

Bug ID	Description
89106	**Symptom**: A configured CLASS attribute was missing from the accounting messages sent from the RADIUS server to clients when previously idle clients reconnected to the network. **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. This issue is resolved with the introduction of the **delete-keycache** parameter in the 802.1X authentication profile, which, when enabled, 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 are again be sent by the RADIUS servers.
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 57: *AirGroup Fixed Issues*

Bug ID	Description
88522 92368	**Symptom:** The multicast Domain Name System (mDNS) process of AirGroup crashed and restarted on 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 specified on a platform. This issue was observed in the switches except OAW-4306 Series switches running earlier versions of AOS-W 6.4.

Air Management-IDS

Table 58: *Air Management-IDS Fixed Issues*

Bug ID	Description
84148	**Symptom:** The **show wms client** command took a long time to return output. This issue is fixed by retrieving wms client information from the in-memory data structures, instead of sending queries to the database. **Scenario:** This issue occurred when the **show wms client** command was executed. This issue was not limited to any specific switch model or release version.
90330	**Symptom:** An adhoc AP was classified to be manually contained, but it would not be contained unless the **protect from adhoc** feature was also enabled. This issue is resolved by changes that ensure an adhoc AP marked for containment is correctly contained. **Scenario:** This issue was observed in switches running AOS-W 6.2 or later.
92070	**Symptom:** The age field in the Real-Time Location System (RTLS) station report sent by an AP was sometimes reset although the station was no longer being heard by the AP. **Scenario:** 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 could occur on a switch running AOS-W 6.1 or later.

Table 58: *Air Management-IDS Fixed Issues*

Bug ID	Description
93912	**Symptom:** Issuing the **show wms client probe** command did not return any output and instead it displayed the **WMS module busy** message after a timeout period. Executing the command with the MAC address of the client fixed this issue. **Scenario:** This issue is observed when there was a large number of entries in the WLAN Management System (WMS) table. This issue is not limited to any specific switch model or AOS-W version.

AP-Datapath

Table 59: *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:** The VLAN in the wired AP is different from the AP's native VLAN. **Scenario:** 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 60: *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.
86112	**Symptom**: The APs went to an inactive state. Changes in the internal code fixed this issue. **Scenario:** This issue was observed when the **named-vlan** parameter was configured in **wlan virtual-ap <name>** command and when all the VLAN IDs were greater than 4064. This issue was not limited to any specific switch model or AOS-W version.
87775	**Symptom:** A Remote AP (RAP) crashed due to incorrect watchdog feeding. The issue is resolved by ensuring that the hardware watchdog feeding is done periodically. **Scenario:** This issue was observed in OAW-RAP5WN and OAW-AP120 Series access points running AOS-W 6.3 or earlier versions when there was a high traffic flow in the network.
87857	**Symptom**: Fragmented configuration packets sent from the switch to the AP can cause the AP to come up with the “D:” (dirty) flag. Improvements to how AOS-W handles out-of-order packets resolve this issue. **Scenario**: This issue is triggered by network congestion or breaks in the connection between the switch and AP.
88288 88568 89040 89135 89137	**Symptom**: 802.11n-capable APs 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 occurred on OAW-AP125, OAW-AP135, and OAW-AP105 access points running AOS-W 6.3.0.1.

Table 60: *AP-Platform Fixed Issues*

Bug ID	Description
	Duplicate Bugs: The following bug IDs have reported similar issues: 89252, 89254 , 89255, 90021, 90028, 90495, 90604, 91016, 91392, 91393, 91755, 92585, 93336
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.
88504 92678	**Symptom:** No output was displayed when the **show ap config ap-group <ap-group>** command was executed. Increasing the buffer size of SAPM (an AP management module in STM) resolved this issue. **Scenario:** This issue was observed on switches running AOS-W 6.3.x.x.
88813 89594	**Symptom:** The **show ap allowed-max-EIRP** command displayed incorrect information for OAW-AP220 Series access points. This display issue is resolved by increasing the buffer size that stores Effective Isotropic Radiated Power (EIRP) information. **Scenario:** This issue was observed in OAW-4504 Series switches and OAW-4604 Series switches running AOS-W 6.3.x.
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 manage layer-2 roaming resolve this issue. **Scenario**: This issue was observed when clients roamed between APs running AOS-W 6.2.
89041	**Symptom:** A 802.11n-capable access point unexpectedly rebooted or failed to respond. This issue is 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. The log files for the event listed the reason for the crash as **kernel panic**. This issue is 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 is resolved by 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.
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 access point code resolved the issue. **Scenario:** This issue was observed on OAW-AP220 Series access points running AOS-W 6.3.x or later versions.
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.
90854	**Symptom:** On multiport APs (such the OAW-AP93H), the APs bridge priority was configured as 8000 by default. This caused the AP to become a root bridge, when connected to a switch, and the AP became slow. **Scenario:** Starting in AOS-W 6.4, the default value has been set to 61440 (0xF000), which avoids this issue.
91803	**Symptom:** An OAW-AP120 Series switch failed unexpectedly.

Table 60: *AP-Platform Fixed Issues*

Bug ID	Description
	Scenario: This issue occurred on an OAW-AP120 Series switch running on AOS-W 6.3.10. It was due to the AP's memory is low due to heavy traffic or many clients.
88793 91804 92194 92195 92700	**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 resolved this issue. **Scenario:** This issue was observed in AOS-W 6.2 and later versions, but was not limited to a specific switch model. **Duplicate Bugs:** The following bug IDs have reported similar issues: 92749, 93080, 93140, 93695, 93798, 93845, 93997
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 the OAW-AP92 and OAW-AP93 access points with 16 MB flash are 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 another. 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 current the LMS. **Scenario:** This issue occurred after a failover of an AP from one switch to another, 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 an LMS and a backup LMS configured.
92245	**Symptom:** An AP did not respond with "**aruba_valid_rx_sig: Freed packet on list at ath_rx_tasklet+0x138/0x2880……**" message and needed a manual power cycle to restore the normal status. This issue is resolved by improvements to the wireless drivers in AOS-W 6.4. **Scenario:** This issue occurred when the buffer was corrupted in wireless driver. This issue was observed in OAW-AP125 model access points associated to switches running AOS-W 6.3.1.
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.
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 is not specific to any switch model.
93012 95172	**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.

Table 60: *AP-Platform Fixed Issues*

Bug ID	Description
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.
93715 93380 93494 93687 93744	**Symptom:** An unexpected reboot of an OAW-AP220 Series AP occurred due to a kernel panic. Internal software changes resolved this issue. **Scenario:** This reboot was triggered by VAP deletion and can occur upon mode change when all VAPs are deleted. The crash was caused because the PCI device is put to sleep when all the VAPs are deleted but AOS-W accessed the PCI device before it woke up. This issue was limited to OAW-AP220 Series APs running any version of AOS-W. **Duplicate Bugs:** The following bug IDs have reported similar issues: 93780, 93904, 94068, 94102, 94124, 94146, 94166, 94192, 94193, 94196, 94258, 94371, 94373, 94422, 94455, 94540, 94564, 94763, 94843, 94864, 94893, 94917, 94918, 94927, 94937, 94956, 94988, 95010, 95011, 95144, 95189, 95259, 95293, 95619
94189	**Symptom:** The enet1 interface of OAW-AP135 did not power up when connected to a data switch. Starting with AOS-W 6.4, the OAW-AP130 Series supports full functionality when powered by an 802.3af Power over Ethernet (PoE) power source. **Scenario:** The issue was observed when the AP was connected to an 802.3af PoE power source. This issue was observed in OAW-AP135 access points, but is not specific to any version of AOS-W.
94279 94720	**Symptom:** A regulatory mismatch was observed on non-US switches after an IAP was converted to a switch based AP. This issue is resolved by adding a new rule to verify the 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 before Ethernet 1 is bonded even when it is UP. **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, and AOS-W release version.

AP Regulatory

Table 61: *AP Regulatory Fixed Issues*

Bug ID	Description
86764	**Symptom:** The output of the **show ap allowed channels** command incorrectly displayed that 5 GHZ channels were supported on OAW-AP68 and OAW-AP68P. This issue is resolved by modifying the allowed channel list for OAW-AP68 and OAW-AP68P. **Scenario:** This issue was observed in OAW-AP68 and OAW-AP68P running AOS-W versions 6.1.x, 6.2.x, or 6.3.
90995	**Symptom:** The Effective Isotropic Radiated Power (EIRP) was inconsistent and in some instances greater than the MaxEIRP, for HT20 and W52. This issue is resolved by updating the algorithm to consider the maximum EIRP for all modulation schemes. **Scenario:** This issue was observed in OAW-S3 switches running AOS-W 6.1.3.6.

AP-Wireless

Table 62: *AP-Wireless Fixed Issues*

Bug ID	Description
67847 69062 69346 71530 74352	**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 OAW-AP120 Series and OAW-AP68P devices connected to switches running AOS-W 6.3.1.2. **Duplicate Bugs:** The following bug IDs have reported similar issues: 74687, 74792, 75212, 75792, 75944, 76142, 76217, 76715, 77273, 77275, 78118, 80735, 82147, 83242, 83243, 83244, 83624, 83833, 84170, 84339, 84511, 85015, 85054, 85086, 85367, 85959, 88515, 89136, 89253, 89256, 89816, 90603, 91084, 92871, 92877, 92878, 92879, 93923
69424 71334 74646 75248 75874	**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 upgrading to AOS-W 6.2 from AOS-W 6.1.3.2 and later in any deployment with an OAW-AP125. **Duplicate Bugs:** The following bug IDs have reported similar issues: 78978, 78981, 79891, 80054, 85753, 87250, 87360, 88619, 88620, 88989, 89537, 91689, 92641, 92975, 93079, 93455, 93811, 91689
86398	**Symptom**: The output of the **show ap debug system-status** command showed an unexpectedly large increase in the buffers in use for queue 8. Changes in how unfinished frames are queued prevents an error that allowed this counter to increment more than once per frame. **Scenario**: This occurred in OAW-AP135 and OAW-AP115 access points running AOS-W 6.3.x.x, and managing multicast traffic without Dynamic Multicast Optimization (DMO).
86456	**Symptom**: A switch running AOS-W 6.3 with an OAW-AP125 running as a RAP rebooted unexpectedly. This was caused when the AP received a BC/MC auth frame and failed. **Scenario**: This issue occurred on an OAW-AP125 access point running AOS-W 6.3.
86584	**Symptom:** The OAW-AP225 did not support prioritization for multicast traffic. **Scenario:** This issue was observed on theOAW-AP220 Series running AOS-W 6.3.x.
88282	**Symptom**: OAW-AP220 Series access points 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**. AOS-W memory improvements resolve this issue. **Scenario**: This issue occurred in a master-local OAW-4x50 Series switch topology where the OAW-AP220 Series AP terminated on both the switches in campus mode.
88328	**Symptom:** Wireless clients experienced packet loss when connecting to remote AP that was in bridge mode. The fix ensures that some buffer is reserved for transmitting unicast traffic. **Scenario:** This issue was observed in OAW-AP105 running AOS-W 6.1.3.8 when there was a huge multicast or broadcast traffic in the network.
88385 94033	**Symptom**: Bridge mode users (802.1x and PSK) are randomly unable to associate to a 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 was observed in switches running AOS-W 6.3.0.1 or later.
88741	**Symptom:** Throughput degradation was observed on the OAW-AP225. **Scenario:** This issue was caused by an internal AOS-W malfunction and was observed only in OAW-AP225.
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.

Table 62: *AP-Wireless Fixed Issues*

Bug ID	Description
88827 93771	Symptom: An AP stopped responding and reset. Log files listed the reason for the event as **ath_bstuck_ tasklet: Radio 1 stuck beacon; resetting**. Changes in the AOS-W 6.4 channel change and radio reset routines prevent this error. **Scenario**: This issue occurred in an OAW-AP125 running AOS-W 6.2.1.3, and was not associated with any switch model.
89442 93804	**Symptom:** The OAW-AP220 Series switches crashed frequently. Log files listed the reason for the event as **Kernel Panic: Unable to handle kernel paging request**. **Scenario:** This issue occurred when the radio mode was altered between Monitor and Infrastructure. This issue was observed only in OAW-AP220 Series switches running AOS-W 6.3.1.2.
88631 88044 88569 88843 89044	**Symptom:** An access point stopped responding and continuously rebooted. Improvements in the wireless driver of the AP fixed this issue. **Scenario:** This issue was observed in OAW-AP220 Series running AOS-W 6.3.0.1 when clients disconnected from the network. **Duplicate Bugs:** The following bug IDs have reported similar issues: 89046, 89053, 89058, 89325, 89326 , 89811 , 89901 , 90890, 92076, 92336, 92786, 93335
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 an 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	**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 access points running AOS-W 6.3.1.0 and later versions. **Duplicate Bugs:** The following bug IDs have reported similar issues: 91620, 92017, 92428, 93373
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.
91192	**Symptom**: Poor performance was observed in clients connecting to an AP due to non-WiFi interference. Implementing the Cell-Size-Reduction feature in OAW-AP220 Series along with deauthorizing clients when they are about to go 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.
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**: Latency issues occur when clients are connected to a single AP. **Scenario:** This issue occurred on an OAW-AP225 access point on a switch running AOS-W 6.3.1 and later. This occurred when clients go into PS mode.
91379 91449 91454	**Symptom:** An OAW-AP220 Series device unexpectedly crashed. Using the correct structure to fill the information in the outgoing response frame resolved this issue.

Table 62: *AP-Wireless Fixed Issues*

Bug ID	Description
91480 94171	**Scenario:** The 802.11k enabled client that sent a Neighbor Report Request frame caused the OAW-AP220 Series device to crash when the packet was freed. This issue was observed in switches running AOS-W 6.3.x or later. **Duplicate Bugs:** The following bug IDs have reported similar issues: 94238, 94413
91856	**Symptom:** Certain 802.11b clients did not communicate with 802.11n-capable access points. Improvements in the wireless driver of 802.11n-capable access points resolved this 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.
91770 91802 91805 91946 92052	**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 running AOS-W 6.3.1.0. **Duplicate Bugs:** The following bug IDs have reported similar issues: 92102, 92260, 92550, 92552, 92554, 92555, 92557, 92559, 92561, 92562, 92736, 92788, 92790, 92873, 92976, 92977, 93756, 93757, 93963
92346	**Symptom**: When the 80 MHz option is enabled in the RF arm-profile, HT Capabilities in beacon only show 20 MHz support. **Scenario:** This issue occurred on switches with OAW-AP225 access points running AOS-W6.3.1 and later.
92626	**Symptom:** An AP crashed and the log files for the event listed the reason for the crash as **kernel panic**. This issue is fixed by referencing the valid memory. **Scenario:** This issue occurred when an invalid memory was referenced. This issue occurred in OAW-AP225 access points running AOS-W 6.3.1.1.
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 seen 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**.
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.
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 are about to go 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.
93476	**Symptom:** Sporadic input/output control errors were seen in the logs of many APs. Changes in the internal code resolved this issue. **Scenario:** This issue was observed when the authentication manager tries to set the keys for previous association, then station sends deauthentication, or the AP disconnects the station.
93710 94370	**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.

Table 62: *AP-Wireless Fixed Issues*

Bug ID	Description
	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.
93996	**Symptom:** An OAW-AP120 Series access point rebooted unexpectedly. This issue is resolved by making changes to the internal code to avoid a potential condition that causes an infinite loop and NMI watchdog condition which causes the AP to reboot. **Scenario:** This issue occurred on OAW-AP120 Series devices connected to switches running AOS-W 6.3.1.0.
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.
94117	**Symptom**: Clients are unable to connect to a SSID when the **Local Probe Request Threshold** setting in the SSID profile (which defines the SNR threshold below which incoming probe requests are ignored) is set to a value of 25 dB. This issue is resolved by 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 because when the Local Probe Request Threshold setting had a value of 25 dB in this setting, the AP did not respond to probe requests with 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.
94155 94249	**Symptom:** An OAW-AP225 device rebooted unexpectedly when connected to a PoE. This issue is 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.
94164 94534	**Symptom:** Wireless clients were unable to connect to an AP through the G band when the WPA2 authentication scheme was used. This issue is resolved by changing the initial value of VHT (Very High Throughput) to **0**. **Scenario:** This issue was observed in OAW-AP225 connected to switches running AOS-W 6.3.1.1.
94198	**Symptom:** An AP rebooted unexpectedly with the log error message out of memory. **Scenario:** This issue occurred on the OAW-AP120 Series running AOS-W 6.3.1.0.
95006	**Symptom:** IOS devices faced connectivity issues 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 handoff 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.

ARM

Table 63: *ARM Fixed Issues*

Bug ID	Description
93312	**Symptom:** When location server was configured on the switch, a connected Air Monitor (AM) mode AP did not generate a probe report unless the location-feed flag was manually set through the AP console. **Scenario:** This issue occurred could occur on any model of AP operating in AM mode running AOS-W 6.3.x.x.

Authentication

Table 64: *Authentication Fixed Issues*

Bug ID	Description
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.
94964	**Symptom:** Captive Portal users were forced to re-authenticate every 5-10 minutes as users were not sending the IPv6 traffic. This issue is resolved by making code level changes in the authentication module. **Scenario:** This issue was observed when wired users connected to an AP and IPv6 was enabled on the switch. This issue was limited only to release versions that supported IPv6 features.

Base OS Security

Table 65: *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 Local Management Switch (LMS) list fixed the issue. **Scenario:** This issue was observed in a VRRP or master-local deployment where the master switch queried itself and the LMS list resulted in duplicate client information. This issue was observed in switches running AOS-W 6.3.X.0.
86867	**Symptom:** When a user-role and the ACL that have the same name and were configured as the ip access-group on the interface for APs/RAPs, the AP/RAP traffic was hitting the user-role ACL instead of the ip access-group ACL. **Scenario:** This issue was observed on switches running AOS-W 6.2.1.2.
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.
87742	**Symptom:** AP group information was not present in the RADIUS packet when the radio was disabled on the AP. The fix ensures that the AP group information is correctly populated in the RADIUS packet even when the radio is disabled. **Scenario:** This issue occurred when the wired clients were connected to the AP where BSSIDs were unavailable due to a disabled radio. This issue was not limited to any specific switch model or release version.
88271	**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.
89453	**Symptom**: The **show rights** command did not display all the user roles configured in the switch. The output of this command now displays all the user roles configured in the switch. **Scenario** This issue was observed when more than 50 user roles were configured on a switch running AOS-W 6.2.1.3.
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.

Table 65: *Base OS Security Fixed Issues*

Bug ID	Description
	Scenario: The issue was observed when users were already connected, and the 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. The log files for the event listed the reason as **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. This issue was not limited to a specific switch model and was observed in AOS-W 6.2.1.2.
90233	**Symptom:** Clients with a logon user role did not age out from the user-table after the logonlifetime AAA timer expired. Users are mpw aged out with the logon user role if the User Derivation Rule (UDR) is configured in the AAA profile. **Scenario**: This issue was observed when UDR was configured in the AAA profile with the logon defined as the default user role. This issue was observed on 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 SAs are added and older IPsec SAs are removed resolved this issue. **Scenario**: This issue occurred after a random IPsec rekey, and was triggered 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 preventing heartbeat responses from reaching the AP.
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:** The client information was not being sent correctly to through the switch and, therefore, not being displayed in the dashboard.
91548	**Symptom**: The error message **User licensed count error** appeared in the error log. However, the system functionality was not affected. **Scenario:** This issue occurred on switches running AOS-W 6.2.1.3 and later. This occurred when the VIA client connected to a RAP in split-tunnel or bridge-mode and the RAP was connected to the same switch from behind NAT.
92674	**Symptom:** Class attribute was missing in the 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 any 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 to 16 bits. **Scenario:** This issue was observed if 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.
93066 93868	**Symptom:** The MAPC module on the switch 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 switch fixed this issue. **Scenario:** This issue was observed when IF-MAP was configured on the switch to communicate with ClearPass Policy Manager (CPPM). This issue was observed on OAW-4x50 Series switches running AOS-W 6.3 or later versions.
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.

Table 65: *Base OS Security Fixed Issues*

Bug ID	Description
	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 AOS-W version.
93237	**Symptom:** An internal module (Authentication) crashed on the switch. Ignoring the usage of the **equivalentToMe** attribute, which was not used by the master switch resolved this issue. **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 AOS-W version.
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 ACL was configured with spaces in their names. This was not limited to any specific switch model or AOS-W version.

Configuration

Table 66: *Configuration Fixed Issues*

Bug ID	Description
73459 85136 86427 90081	**Symptom:** The output of the **show acl hits** CLI command and the **Firewall Hits** information on the **UI Monitoring** page of the switch WebUI showed inconsistent information. This issue is resolved by displaying consistent information. **Scenario:** This issue occurred because the formatting of the XML response from the switch to the WebUI was incorrect, when the output was beyond the specified limit. This issue was not limited to a specific switch model or release version.
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** do not correctly sort the AP entries in ascending or descending order by up time. Improvements to how the switch sorts APs by status and up time resolve this issue. **Scenario**: This issue was identified in switches running AOS-W 6.2.1.2
91903 93462 93631	**Symptom:** The switch's fpcli process crashed when executing the command **show ap tech-support ap-name <ap name>** with a non-existing or incorrect AP name. Now, when this command is executed with a non-existent AP, the CLI returns AP with name "X" not found. **Scenario:** This issue was observed on an OAW-S3 switch running AOS-W 6.1.3.10 but was not limited to a specific switch model.

Captive Portal

Table 67: *Captive Portal Fixed Issues*

Bug ID	Description
87294 87589 92575	**Symptom:** Captive Portal (CP) whitelist that was mapped to the user-role did not get 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 was not limited to any specific switch model.
88001	**Symptom:** The domain name whitelist could not be configured using wild card characters in the Captive Portal profile. The fix ensures that the wild card characters are supported while configuring the domain name whitelist. **Scenario:** This issue was not limited to any specific switch model or release version.
88116	**Symptom:** Captive Portal user was incorrectly redirected to the **User Authenticated** page even when the user provided a wrong username or password. The user now gets an **Invalid username or password** error message when providing wrong credentials. **Scenario:** This issue was observed if MSCHAPv2 was used for Captive Portal authentication. This issue was not limited to a specific switch model or release version.
88283	**Symptom:** The captive portal profile used https by default. For authentication, the user was redirected to the https://securelogin.example.com. But if this URL was manually changed to http://securelogin.example.com, then connection remained insecure from that point onwards. The switch now sends a redirect URL using the protocol configured on the switch. **Scenario:** This issue was observed when there was a mismatch between the protocol configured on the AAA profile and the protocol from the browser, This issue was not limited to a specific switch model or release version.
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-4x50 Series switch running AOS-W 6.3.0.0.
91442	**Symptom:** In the master switch's command line interface **Login** page, the question mark symbol was neither getting pushed nor getting added to the local switch. This issue is resolved by ensuring that the master switch's command line interface accepts the question mark symbol. **Scenario:** This issue was observed while synchronizing the configuration from the master switch to the local switch.
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 observed in switches running AOS-W 6.3.0.0 or later versions.
93674	**Symptom**: Clients were unable to access an external captive portal page after the switch reset. 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.
94167	**Symptom:** When client traffic was moving through an L3 GRE tunnel between a switch and a switch, the switch did not provide the captive portal page to the client. **Scenario:** This issue was observed after an 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.

Switch-Datapath

Table 68: *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.
82824	**Symptom**: In some cases, when there was a large number of users on the network (more than 16k), and the **Enforce DHCP** parameter was enabled in the AP group's AAA profile, a user was flagged as an IP spoofed user. Changes to how AOS-W manages route cache entries with the 'DHCP snooped' flag resolves this issue. **Scenario**: This issue was observed in switches running AOS-W 6.3.
83422 85600 87794 88311 88360	**Symptom:** An OAW-4x50 Series switch unexpectedly rebooted. The switch log files listed the reason for the event as a **datapath timeout**. Improvements in creating tunnels in the internal switch datapath resolved this issue. **Scenario:** This issue was observed in OAW-4x50 Series switches running AOS-W 6.2.1.x. **Duplicate Bugs:** The following bug IDs have reported similar issues: 88505, 88683, 88740, 88833, 88985, 89004, 89303, 89910, 90450, 90457, 90482, 90609, 90836, 91170, 91363, 91695, 92161, 92177, 92811, 93064, 93572, 93985, 94025, 94514
85398 85627	**Symptom:** A switch responded to the Domain Name System (DNS) queries even when the IP domain lookup was disabled. This issue is resolved by ensuring that the DNS service is completely stopped if the IP domain lookup is disabled. **Scenario:** This issue occurred when the switch responded to DNS requests with its own IP. This issue was observed in switches running AOS-W 6.1.3.6.
85685 85543 87406	**Symptom:** An OAW-S3 switch running AOS-W 6.1.3.8 stopped responding and rebooted. The log files for the event listed the reason for the crash as **fpapps: Segmentation fault**. Changes to the process that handles the VLAN interfaces fixed the issue. **Scenario:** This issue was observed when the VLAN interface on the switch constantly switched between an UP and DOWN state, resulting in VRRP status change. This issue was not limited to a specific switch model or AOS-W release version.
85796 88233 88731 90350 91310	**Symptom:** A switch crash was observed due to a session table entry corruption. This issue is resolved by modifying the method by which the IGMP query is handled over a port channel. **Scenario:** This issue occurred when an IGMP query was triggered on the port channel. This issue was observed in OAW-4x04 Series switches, OAW-4x50 Series switches, and OAW-S3 switches running AOS-W 6.2.x. **Duplicate Bugs:** The following bug IDs have reported similar issues: 93153, 93183
85843	**Symptom**: A switch unexpectedly rebooted. Log files for the event listed the reason for the reboot as **datapath exception**. Memory improvements resolve this issue in AOS-W 6.4. **Scenario**: This issue was observed in an OAW-4x50 Series switch running AOS-W 6.2.1.1.
87295	**Symptom:** A crash was observed in a switch when it received certain types of DNS packets. This issue is fixed by modifying the internal code to handle the DNS packets correctly. **Scenario:** This issue was observed when the **firewall-visibility** feature was enabled on a switch running AOS-W 6.2 or later.
88325	**Symptom**: Enabling support for jumbo frames on an uplink interface caused pings larger than 1472 bytes to fail. This issue is resolved by changes that ensure AOS-W uses the correct default MTU size when jumbo frames are disabled globally, while still enabled on a port. **Scenario**: This issue was observed in AOS-W 6.3.1.0, on a switch with jumbo frames disabled globally, but enabled on a port.

Table 68: *Switch-Datapath Fixed Issues*

Bug ID	Description
88469 90779	**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.
87417 87846 87949 88039 88226	**Symptom:** A master switch rebooted unexpectedly. The log files for the event listed the reason for the reboot as **datapath exception**. Enhancements to the Broadcom driver of the access point fixed this issue. **Scenario:** This issue was observed in OAW-4750 switch running AOS-W 6.3.1.1 in a master-local topology. **Duplicate Bugs:** The following bug IDs have reported similar issues: 88445, 89433, 89539, 89641, 90024, 90458, 90469, 90746, 90896, 91853, 92284, 92464, 92466, 92827, 92828, 92829, 92830, 92832, 94007, 95012
87949 88039 88226 88445 89433	**Symptom:** A switch stopped responding to network traffic and rebooted. The log file for the event listed the reason for the reboot as **datapath timeout**. This fix ensures that the CPU livelock does not recur. **Scenario:** This issue occurred on OAW-4x50 Series switches running AOS-W 6.3.0.1 and 6.2.x.x. **Duplicate Bugs:** The following bug IDs have reported similar issues: 89539, 89641, 90024, 90458, 90469, 90746, 90896, 91853, 92294, 92464, 92466, 92827, 92828, 92829, 92830, 92832, 92988, 93555
89906 92248 93423 94010 94682	**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 is not limited to any specific switch model or AOS-W release version. **Duplicate Bugs:** The following bug IDs have reported similar issues: 94989, 95215, 95958
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-4x50 Series switches. This issue occurred because the switch was using multiple replay counters, which the device did not support.
93466	**Symptom**: The OAW-4x50 Series switches rebooted and the log files for the event displayed the reason for the reboot as **datapath timeout**. This issue is fixed by not forwarding the mirrored packets to monitor port when the monitor port status 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 AOS-W version.
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.
95588	**Symptom:** GRE tunnel groups 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.

Switch-Platform

Table 69: *Switch-Platform Fixed Issues*

Bug ID	Description
70068 85684 87008	**Symptom**: An internal switch module stops responding when a user attempts to add or delete a large number of VRRP instances. This issue is resolved by internal work flow enhancements that prevent this issue from occurring. **Scenario**: This error can be triggered by a VRRP state change, enabling or disabling an interface, or adding or deleting a tunnel.
82402 84212 86636 87552 89437	**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**. Verifying the Process Application Programming Interface (PAPI) packet before processing it resolved the issue. **Scenario:** This issue was observed when the PAPI library used by all applications did not filter the broadcast traffic correctly prior to PAPI inspection that caused the applications to crash. This issue occurred in OAW-4604 switches running AOS-W 6.2.1.0. **Duplicate Bugs:** The following bug IDs have reported similar issues: 90466, 91280, 93591, 94721, 94727, 95074, 95624, 95643, 95644
82736 82875 83329 83762 84022	**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 were **soft watchdog reset** or user pushed reset. This issue was identified in AOS-W 6.1.x.x, and is not limited to any specific switch model. **Duplicate Bugs:** The following bug IDs have reported similar issues: 85355, 85370, 85628, 86005, 86029, 86031, 86572, 86589, 87410, 87505, 87587, 88005, 88332, 88351, 88434, 88921, 89636, 89818, 90909, 91269, 91308, 91370, 91517, 92823, 93294, 93770, 95946
83502 83762 85355 85370 86029	**Symptom**: A switch rebooted unexpectedly. Changes in the watchdog implementation on the switch resolved the issue. **Scenario**: Log files for the event indicated the reason for the reboot as **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:** The following bug IDs have reported similar issues: 86031, 88005, 89636, 92823
85685 92814	**Symptom:** An 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 the switch on which the static or default routes were not configured. This issue was observed in OAW-S3 switches running AOS-W version 6.2.1.3 or later.
86107 93279	**Symptom**: The switch stopped processing radius packets every three hours and then resumed after one minute. This issue was resolved by setting **aaa profile <aaa-profile-name>** to **no devtype-classification** for all aaa profiles in use. Then execute the **clear aaa device-id-cache all** command. **Scenario:** An internal process took a backup of the database every three hours, and during this time authentication tried to access information from the database and waited there until backup was complete. Authentication resumed after that. This issue was observed on switches running AOS-W 6.2 or earlier.
86216 85566 87090 87635 88321	**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:** The following bug IDs have reported similar issues: 88387, 88699, 89436, 89727, 89839, 89911, 90162, 90338, 90481, 91193, 91387, 91941, 92139, 92187, 92516, 92808,,93630, 93693, 93931, 94308
86266	**Symptom**: In rare cases, issuing commands through a telnet shell caused an internal switch process to stop responding, triggering an unexpected switch reboot. This issue is resolved by changes that prevent AOS-W from referencing null pointers within the software.

Table 69: *Switch-Platform Fixed Issues*

Bug ID	Description
	Scenario: This issue was triggered by varying sequences of commands issued via the telnet shell, and is not specific to a switch model or release version.
87498	**Symptom**: An internal process (FPAPPS) failed unexpectedly. **Scenario:** This issue occurred on an OAW-4504 switch running AOS-W 6.3.0.1 when the PPOE/PPP connection was established.
89155	**Symptom**: OAW-4306 Series switches experienced high levels of CPU usage while booting, triggering the warning messages **Resource 'Controlpath CPU' has exceeded 30% threshold.** This issue is resolved by changes to internal CPU thresholds that better reflect expected CPU usage levels. **Scenario**: This issue was observed in switches running AOS-W 6.1.2.3.
90751 90633 90863 91154 91138	**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. **Duplicate Bugs:** The following bug IDs have reported similar issues: 91474, 91656
90619 92250	**Symptom:** The switch WebUI stopped responding indefinitely. The fix ensures that the OV3600 query fails if there is no firewall visibility. **Scenario:** This issue occurred when OV3600 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 an 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.
91778	**Symptom**: A switch unexpectedly reboots, displaying the error message **Mobility Processor update**. **Scenario**: This issue was observed in a local OAW-S3 switch module running AOS-W 6.3.x.x in a master-local topology.
93990	**Symptom:** A few **Not Found** error messages appeared in the switch's console while performing initial configuration while booting. Modifying the make subsystem, and packaging the binary resolved this issue. **Scenario:** A certain binary was not built correctly due to changes in make or packaging script. This issue was observed in OAW-4306 Series switches running AOS-W 6.1.x.x or later.
94013 94045 95079	**Symptom:** A switch rebooted due to low memory. Changes in the internal code of the switch software fixed this issue. **Scenario:** This issue occurred when there was continuous high traffic 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.
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.

Control Plane Security

Table 70: *Control Plane Security Fixed Issues*

Bug ID	Description
85402	**Symptom:** When sending the RAP whitelist information to CPPM, AOS-W did not fill the Calling-Station-Id correctly. **Scenario:** The switch returned a Calling-Station-Id value of 000000000000 instead of the actual value. This issue was caused by a malfunction in an internal switch process (auth) and was observed on a switch running AOS-W 6.3.0.

DHCP

Table 71: *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 6.4. **Scenario:** This issue was triggered by a race condition that caused the DHCP wrapper process to crash with continuous restarts. This issue was not limited to a specific switch model or release version.
92438	**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.

Generic Routing Encapsulation

Table 72: *Generic Routing Encapsulation 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 in the forwarding pipeline. **Scenario:** This issue occurred when the GRE tunnel keep alive was 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 73: *GSM Fixed Issues*

Bug ID	Description
91870	**Symptom:** The output of the **show ap database** command indicated that an 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.

Guest Provisioning

Table 74: *Guest Provisioning Fixed Issues*

Bug ID	Description
87091	**Symptom:** The **Guest Provisioning** page of the WebUI showed incorrect alignment when it was printed from the Internet Explorer 8 or the Internet Explorer 9 Web browser. Improvements in the HTML styles resolved this issue. **Scenario:** This issue was first identified in AOS-W 5.0.4.0. This issue was not observed when users viewed the switch WebUI using older versions of Internet Explorer (version 6 and 7).

HA-Lite

Table 75: *HA-Lite Fixed Issues*

Bug ID	Description
80206	**Symptom:** The high availability: fast failover feature introduced in AOS-W 6.3 did not support VRRP-based LMS redundancy in a deployment with master-master redundancy. This topology is supported in AOS-W 6.4. **Scenario:** This issue occurred because the high availability: fast failover feature does not allow the APs to form standby tunnels to the standby master switch.

Hardware Management

Table 76: *Hardware Management Fixed Issues*

Bug ID	Description
87481	**Symptom:** OAW-4x50 Series switch returned an invalid value when an SNMP query was performed on the internal temperature details (OID .1.3.6.1.4.1.14823.2.2.1.2.1.10). The fix ensures that the SNMP attribute is set correctly for the temperature details. **Scenario:** This issue was limited to OAW-4x50 Series switches running AOS-W 6.3 or later versions.

IGMP Snooping

Table 77: *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 AOS-W version.

IPv6

Table 78: *IPv6 Fixed Issues*

Bug ID	Description
88814	**Symptom:** When clients connected to a switch, they received IPV6 router advertisements from VLANs with which they were not associated. This issue is resolved by updating the datapath with the 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 79: *Licensing Fixed Issues*

Bug ID	Description
87424	**Symptom:** The licenses were lost on a standby master switch due to which the configuration on the local switch was also 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 occurred in all master scenarios when running AOS-W 6.3 or later.
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 80: *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 into 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 version. This issue was not limited to any specific switch model or release version.

Master-Redundancy

Table 81: *Master-Redundancy Fixed Issues*

Bug ID	Description
80041 87032 87946 88067	**Symptom:** The show **database synchronize** command displayed a FAILED message and the standby switch was out of sync with the Master. Additionally, if there is a switchover at this time, the system is in an inconsistent state. This issue is resolved by ignoring any aborted database's 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 previous aborted database synchronization. **Scenario:** This issue occurred when a switch was upgraded from a previous version of AOS-W to 6.3 or later version. This issue was not limited to any specific switch model or release version.

Mesh

Table 82: *Mesh Fixed Issues*

Bug ID	Description
89458 91343 92614	**Symptom:** A Mesh Point rebooted frequently as it could not connect to a Mesh Portal. This issue is 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 with switches running AOS-W 6.1.x and later versions.

Mobility

Table 83: *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.

PPPoE

Table 84: *PPPoE Fixed Issues*

Bug ID	Description
86681	**Symptom**: A switch was not able to connect to the Internet. This issue is fixed by modifying the way Point-to-Point Protocol over Ethernet (PPPoE) handles user name that contains special characters. **Scenario:** The PPPoE connection was not established with an internet service provider (ISP) server when a PPPoE user name contained special characters (for example: #0001@t-online.de). This issue was observed on switches running AOS-W 6.1.3.7 or later.
94356	**Symptom:** PPPoE connection did not work with 'ip nat inside' configuration. 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 has 'ip nat inside' enabled.

Remote AP

Table 85: *Remote AP Fixed Issues*

Bug ID	Description
82015	**Symptom:** An AP associated with a switch did not age out as expected when you changed the heartbeat threshold and interval parameters. Changes in the internal code fixed this issue. **Scenario:** This issue occurred when you changed the heartbeat threshold and interval parameters in the AP's system profile while the AP's status is UP in the switch. This issue was not limited to any specific switch, AP model, or AOS-W release version.
85249	**Symptom:** A degradation of Transmission Control Protocol (TCP) throughput by 9 to 11 Mbps was observed on a RAP. This issue is resolved by optimizing driver code. **Scenario:** This issue occurred in RAPs with any forwarding mode and not specific to any AP model.
85970	**Symptom:** RAPs were rebooting or crashing with a reboot reason as **Kernel page fault at virtual address**. This issue is resolved by adding a check while processing packets with no session entry. **Scenario:** This issue was observed when the RAPs received some packets with no session entries from the IPSec tunnel. This issue was observed only in RAPs running AOS-W 6.2.x.
86650	**Symptom**: A switch sent continuous RADIUS requests for the clients connected behind the wired port of a remote AP (RAP). This issue is resolved by AOS-W enhancements that prevent memory corruption. **Scenario**: This issue was observed when a RAP used a PPPoE uplink and operated as a wired AP in split-tunnel or bridge mode. This issue occurred on AOS-W running 6.1.3.6, and was not limited to any specific switch model.
86934	**Symptom:** The AP failed during boot up when the Huawei® modem E1371 was used. Clearing an empty device descriptor of the modem fixed the issue. **Scenario:** This issue was caused by an internal code error when using this modem. This issue was observed in OAW-RAP108 and OAW-RAP109 running AOS-W 6.3.
88193	**Symptom:** BOSE WiFi products were not able to acquire an IP address through the internal built-in DHCP server in an OAW-RAP5WN. **Scenario:** This issue occurred on switches running AOS-W 6.1.3.9 and later. The DHCP client did not receive an DHCP offer or acknowledgment from the DHCP server.
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 6.3.x.x nd 6.2.x.x, when OAW-AP70 and OAW-RAP108 access points connected to a Huawei® E220 Modem.
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 fix this issue. **Scenario:** This issue was observed in Remote Access Points running AOS-W 6.1.x.x.
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 pre-emption enabled. This issue was observed in RAPs running AOS-W 6.3.1.0.

Table 85: *Remote AP Fixed Issues*

Bug ID	Description
93707	**Symptom:** The RAP rebootstraps every 6 minutes if the RAP's local gateway IP is 192.168.11.1. **Scenario:** This issue occurred on switches running AOS-W6.2.1.4 and 6.3.1.1. It was caused by the DHCP server net assignment conflicting with the RAP's local networks.
94140	**Symptom:** IAP whitelist database on the switch did not allow multiple APs in same branch to share a common remote IP. **Scenario:** Starting with AOS-W 6.4, this option is now supported. This issue was caused by a typecasting error that prevented smaller IP addresses from being allowed.
94703	**Symptom:** IAP-VPN connection disconnected intermittently. This issue is resolved by not allowing IAP database to store more than six subnets per branch. **Scenario:** This issue was observed when IAP database had more than six subnets-per-branch although a maximum of six subnets-per-branch is allowed. IAP-VPN branch with six subnets went down for more than idle timeout and came up with different DHCP profiles which led to more than six subnet entries for the branch in the IAP database.

Role/VLAN Derivation

Table 86: *Role/VLAN Derivation Fixed Issues*

Bug ID	Description
88508	**Symptom:** User derived roles were not considered for DHCP options. This issue is resolved by removing the ceiling limit set on the packet length. **Scenario:** This issue was observed when the DHCP packet length was greater than 1000 bytes in switches running AOS-W versions 6.3.x or earlier versions.

SNMP

Table 87: *SNMP Fixed Issues*

Bug ID	Description
85119	**Symptom:** The **wlsxNLowMemory** trap could not be triggered when the free memory of a switch was low. This issue is fixed by allowing a switch to send the **wlsxNLowMemory** trap, when the free memory of a switch reaches a threshold of 50 Mb. When the free memory of a switch reaches more than 50 Mb, the switch sends the **wlsxMemoryUsageOK** trap. **Scenario:** This issue occurred because the **wlsxNLowMemory** trap was not implemented. This issue was observed in switches running AOS-W 6.x.
83948 85146 87842	**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 OV3600 was used to monitor OAW-4306 and OAW-4704 switches running AOS-W 6.3.0.0.
90453	**Symptom:** The **wlsxStackTopologyChangeTrap** SNMP trap was seen on OV3600 from the switch OV3600 doesn't support. This issues is resolved by updating to the latest AOS-W MIBs on OV3600**.** **Scenario:** This issue was observed on switches running OV3600 7.7.4 and AOS-W 6.3.0.1.
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 88: *Station Management Fixed Issues*

Bug ID	Description
85662 84880 88009 88319 89321	**Symptom:** The state of APs were displayed as **down** on the master switch even if these APs 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 Local Management Switch (Primary-LMS) and master switch was configured as a backup Local Management Switch (Backup-LMS). This issue was not limited to any specific switch model and occurred in AOS-W 6.3 or later. **Duplicate Bugs:** The following bug IDs have reported similar issues: 91963, 92164, 93243, 93388, 93389, 93984
86357	**Symptom:** Station Down messages were not logged in the syslog messages. Changes to syslog messaging resolved this issue. **Scenario:** This issue was observed in switches running AOS-W 6.3.x.x.
88938 88999	**Symptom:** A switch's internal station management module stopped responding, causing the OAW-AP125 access points associated to that switch to rebootstrap. Improvements to the process that updates internal tables for the client match feature resolve this issue. **Scenario:** This issue occurred on switches running AOS-W 6.3.0.1 and using the client match feature.

TACACS

Table 89: *TACACS Fixed Issues*

Bug ID	Description
89676	**Symptom:** Users were not able to authenticate against a TACACS server. **Scenario:** This issue was observed in switches running AOS-W 6.1.3.7 and later. This was triggered when non-blocking sockets for TCP connect() were not polled long enough (at least 2-3 seconds are required) before closing the tcp socket.

VLAN

Table 90: *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.

Voice

Table 91: *Voice Fixed Issues*

Bug ID	Description
77716 88996 90000	**Symptom:** Incompatibility issues observed between an 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 an OAW-4704 switch running AOS-W 6.0 or later.
86224	**Symptom:** Calls dropped after 30 seconds when performing a blindly transferred SIP call. Ignoring the mid call re-invite message (by SIP ALG state machine) handling process resolves the issue. **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.
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 ensuring to handle the message appropriately for wired clients. **Scenario**: This issue was observed when Lync clients were identified as voice clients via media classification. This issue occurred on AOS-W running 6.2 and 6.3 versions, and not limited to any specific switch version.
93517	**Symptom:** Access point rebooted unexpectedly resulting in wireless clients losing 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 or later versions.

WebUI

Table 92: *WebUI Fixed Issues*

Bug ID	Description
73459	**Symptom:** The output of the **show acl hits** command and the firewall hits information on the **Monitoring** page of the switch WebUI shows inconsistent information. The issue is resolved by displaying consistent information in the CLI and WebUI. **Scenario:** This issue occurred because the formatting of the XML response from the switch to the WebUI was incorrect, when the output exceeded the specified limit. This issue was not limited to a specific switch model or release version.
76439	**Symptom**: The Spectrum Analysis section of the WebUI fails to respond when a connected spectrum monitor is in a DOWN state. Changes to how AOS-W manages popup error messages resolve this issue. **Scenario**: This issue occurred in AOS-W 6.2.0.0, when an OAW-AP105 access point in hybrid AP mode failed to appear as a connected spectrum monitor in the switch WebUI.
85225	**Symptom:** The following two issues were observed when adding an SNMPv3 user under the **Configuration** > **Management** > **SNMP** page of the WebUI: 1. **User Name** field was not editable. 2. **Privacy Protocol** value changed to null, when the **Authentication Protocol** was edited in SNMPv3 user entry. The first issue is an expected behavior for SNMPV3 users and the button caption is changed to **DONE** in the **Edit** mode. The second issue is fixed by avoiding the **Privacy Protocol** value changing to null. **Scenario:** This issue was not limited to any specific switch model or release version.

Table 92: *WebUI Fixed Issues*

Bug ID	Description
87457	**Symptom:** The **PKCS#12 Passphrase** field was incorrectly enabled while provisioning a regular remote AP in the WebUI (under the **Configuration** > **Wireless** > **AP Installation** > **Provision** page). The **PKCS#12 Passphrase** field is now enabled in the WebUI only for provisioning a certificate based remote AP. **Scenario:** This issue was not limited to a specific switch model or software version.
87078	**Symptom:** While accessing **AP Configuration** or **Authentication** options, the system displayed **show aaa authentication mgmt: data null** error. This issue is resolved by restarting an internal process in the switch. **Scenario:** This issue was observed in OAW-4504 Series switches running AOS-W 6.1.3.5.
87720	**Symptom:** The **Reset** button on the **Monitoring** page was not functioning correctly. The **Reset** button now resets all Air Monitors correctly. **Scenario:** This issue was not limited to a specific switch model or release version.
88066	**Symptom:** Users were unable to generate Certificate Signing Request (CSR) with a comma in the **Organization** field in the WebUI and displayed a message **Invalid Character(s) Input for Organization**. This issue is fixed by GUI updates to allow comma in the **Organization** field. **Scenario:** This issue occurred only in the WebUI and there was no impact in the Command Line Interface (CLI). This issue was not limited to any specific switch model or release version.
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 select 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 WebUI, 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 only in OAW-4306 Series switches running AOS-W 6.3.x.
89092	**Symptom:** When an administrator added bulk VLANs under **Configuration > Network > VLAN > VLAN ID**, the switch did not add the bulk VLANs and the web page displayed a JavaScript error. Correction in the formatting of the XML response from the switch to the WebUI fixed this issue. **Scenario:** This issue was observed in switches running AOS-W 6.4.
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 an OAW-4306G switch running AOS-W 6.2.1.3, but could impact any switch model.
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.

Table 92: *WebUI Fixed Issues*

Bug ID	Description
92340 92649	**Symptom:** The WebUI of a switch failed to load in 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 the new standards in Internet Explorer 11. **Scenario:** This issue was caused by changes in Internet Explorer 11 from Internet Explorer 10. This issue was observed in Internet Explorer 11 and not limited to any specific switch model or release version.
92620	**Symptom:** When TPM Initialization failed, the following error message was displayed: **TPM Initialization or Certificate Initialization failed. For debug information see /tmp/deviceCertLib.log**. The fix ensures that the error message points to the **show tpm errorlog** command. **Scenario:** This issue was observed when the Trusted Platform Module (TPM) Initialization or Certificate Initialization failed. This issue was not limited to a specific switch model.
93606	**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.

WLAN Management System

Table 93: *WLAN Management System Fixed Issues*

Bug ID	Description
84146	**Symptom:** WLAN Management System (WMS) slowed down with redundant database queries in a switch. This issue is fixed by ignoring queries to the database that determine if there are more Virtual APs (VAPs) present on the probe. Now, the information on VAP presence can be retrieved from the in-memory data structures. **Scenario:** This issue occurred when many APs rebooted, WMS marked them as down. This caused the WMS to slow down by generating redundant database queries. This issue was not limited to any specific switch model or release version.

XML API

Table 94: *XML API Fixed Issues*

Bug ID	Description
84801	**Symptom:** Clients connected to the local switch were unable to access the Captive Portal (CP) page from an external server. This issue is resolved by configuring the **default-xml-api** parameter in the AAA profile. **Scenario:** This issue was observed when the **default-xml-api** was not configured. This issue was not limited to any specific switch or AP model.

This chapter describes the known and outstanding issues identified in AOS-W 6.4.x release versions.

Known Issues and Limitations in AOS-W 6.4.1.0

The following are the known issues and limitations found in AOS-W 6.4.1.0. Applicable Bug IDs and workarounds are included.

AP Regulatory

Table 95: *AP Regulatory Known Issues*

Bug ID	Description
99290	**Symptom:** 80 MHz channels in the Hong Kong regulatory domain are disabled on the OAW-AP220 Series. **Scenario:** 80 MHz channels are not supported on the OAW-AP220 Series within the Hong Kong regulatory domain. **Workaround:** Download and activate the latest regulatory file from the Alcatel-Lucent support site.
102555	**Symptom:** The Puerto Rico regulatory domain is disabled on the OAW-AP270 Series. **Scenario:** The OAW-AP270 Series is not currently supported in the Puerto Rico regulatory domain. **Workaround:** Enable the US regulatory domain or download and activate the latest regulatory file from the Alcatel-Lucent support site.

BaseOS Security

Table 96: *BaseOS Security Known Issues*

Bug ID	Description
101355	**Symptom:** The switch is not completely compliant with the RFC3576 as the state attribute is not processed and send back to the server. **Scenario:** This issue occurs when the Change of authorization (CoA) request packet sent contains a state attribute but the switch is not placing that state attribute in the CoA-Ack. This issue is not limited to a specific switch model or release version. **Workaround:** None

Captive Portal

Table 97: *Captive Portal Known Issues*

Bug ID	Description
95922	**Symptom:** Captive portal log out does not work. **Scenario:** This issue is observed when you configure a captive portal profile with an external log in page and custom captive portal certificate. This issue is not limited to any specific switch model or release version. **Workaround:** None.

Switch-Datapath

Table 98: *Switch-Datapath Known Issues*

Bug ID	Description
88629	**Symptom:** ACL enforcement for Microsoft® Skype doesn't work consistently. **Scenario:** This issue occurs on OAW-4x50 Series switches running AOS-W 6.4 when Deep Packet Inspection (DPI) is enabled on the switch. **Workaround:** None.
89722	**Symptom:** Facebook® application traffic is not getting classified correctly. **Scenario:** This issue occurs on OAW-4x50 Series switches running AOS-W 6.4 when DPI is enabled on the switch. **Workaround:** None.
92955	**Symptom:** When sending small sized data packets at high speed data rate through IPSec tunnel, the switch crashes due to **datapath timeout**. **Scenario:** This issue is observed when the switch sends IPSec traffic at 400 Mbps with 64 bytes packet size. This causes the switch's ingress queue run out of buffer. This issue is not limited to a specific switch model or software release version. **Workaround:** None.
93327	**Symptom:** World of Warcraft® online game sessions are not getting classified correctly. **Scenario**: This issue occurs on OAW-4x50 Series switches running AOS-W 6.4 when AppRF is enabled on the switch. **Workaround:** None
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. **Workaround:** None.
101010	**Symptom:** When both DMO and broadcast-filter-all is enabled and port-channel is used for uplink port, incoming known multicast traffic from uplink is dropped in the switch. **Scenario:** This issue occurs in switches running AOS-W 6.3.x.0 and 6.4.x.0. **Workaround**: None.

Switch-Platform

Table 99: *Switch-Platform Known Issues*

Bug ID	Description
99197 99198	**Symptom:** WMS and DBSTART processes crash frequently. **Scenario:** This issue is observed when the MYSQL database crashes, and system reloads after AOS-W upgrade This issue is observed in AOS-W 6.3.x and later versions. **Workaround:** Listed below are the upgrade recommendations: • A flash backup is recommended before proceeding with the AOS upgrade. • When the issue is observed, clear the WMS database and run the **wms reinit-db** command to restore database from the flash backup.
97789 98763	**Symptom:** Switches running AOS-W 6.4 or later versions fail to copy an AOS-W image using Windows TFTP. **Scenario:** This issue is seen when you copy an AOS-W image onto the non-boot partition of the switch using TFTP. The following error message is displayed: • In CLI: **Error determining image version** • In WebUI: **Error determining new default boot partition version** This issue is not limited to any specific switch model and observed in switches running AOS-W 6.4 or later versions. **Workaround:** Use FTP or SCP to copy an AOS-W image onto the non-boot partition.

LLDP

Table 100: *LLDP Known Issues*

Bug ID	Description
94647	**Symptom:** In rare cases, a **lldp GSM PORT_INFO Lookup failed at Function: sm_handle_lldp_info_events** error message appears in the log. **Scenario:** This issue occurs when the script to shut or open the interface is executed multiple times. This issue is not limited to any specific switch model and occurs on AOS-W running 6.4. **Workaround:** None.

Remote AP

Table 101: *Remote AP Known Issues*

Bug ID	Description
101962	**Symptom:** Remote AP (RAP) shows the status as down on the switch when custom certificate is configured on the RAP. **Scenario:** A USB containing a pfx file is connected to the RAP. During boot up, the RAP searches for the pfx file and loads the key/certificates from the pfx file. The key/certificates are used in IKEv2 tunnel establishment. When the USB has more than one pfx file in different directories having a same file name such as **<mac-address>.p12**, the RAP fails to upload the pfx files and hence cannot establish an IKEv2 tunnel. This issue is not specific to any switch model or AOS-W release version. **Workaround:** On the USB connected to the RAP, delete any duplicate pfx file. Only one pfx file must be present with the RAP MAC address i.e., **<mac-address>.p12**.

Voice

Table 102: *Voice Known Issues*

Bug ID	Description
87316	**Symptom:** The Call Detailed Record (CDR) for a VoIP client goes into **ABORTED** state due to session age out. **Scenario:** This issue is observed in an L3 mobility deployment when the Real-time Transport Protocol (RTP) packets do not get tunneled to the Home Agent (HA), when a client that has roamed to the Foreign agent (FA) initiates a Lync call. This issue is observed in switches running AOS-W 6.3 or later versions. **Workaround:** None.

WebUI

Table 103: *WebUI Known Issues*

Bug ID	Description
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 WebUI. **Scenario:** This issue is not limited to any specific switch model. **Workaround:** Clear the browser cache after the image is upgraded.
101390	**Symptom:** Using the switch's WebUI, a user cannot copy files to a USB drive connected to slot 1 of the switch. **Scenario:** There are two USB slots in OAW-4010 switch. This issue is observed in OAW-4010 switch running AOS-W 6.4.1.0. **Workaround:** Use the CLI to copy files to a USB drive connected to slot 1 of the switch. Or To copy files, connect the USB drive to slot 0 of the OAW-4010 switch.

Known Issues and Limitations in AOS-W 6.4.0.2

The following are the known issues and limitations in AOS-W 6.4.0.2. Applicable Bug IDs and workarounds are included.

AP-Wireless

Table 104: *AP-Wireless Known Issues*

Bug ID	Description
88940	**Symptom:** A crash is observed on APs when the status of the channel is set inappropriately by the process handling the AP management. **Scenario:** This issue is observed when a standard RAP or CAP is 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. **Workaround:** Set the AP channel to No DFS before rebooting the AP.
97333	**Symptom:** All clients associated with an AP disassociates when more than 48 users start FTP downloads. **Scenario:** This issue is observed on switches running AOS-W 6.4.0.1. **Workaround:** None.

Base OS Security

Table 105: *Base OS Security Known Issues*

Bug ID	Description
93550	**Symptom:** Running the **aaa test-server** command for a TACACS authentication server displays **AAA server timeout** in spite of successful authentication. **Scenario:** This issue is not limited to a specific switch model or release version. **Workaround:** Issue the **aaa test-server** command twice.
95479	**Symptom:** A switch stops responding and reboots. The log files for the event listed the reason as **Nanny rebooted machine - sshd process died**. **Scenario:** This issue is observed in OAW-4x50 Series switch running AOS-W 6.3.1.2. **Workaround:** None.

Switch-Datapath

Table 106: *Switch-Datapath Known Issues*

Bug ID	Description
91085	**Symptom:** Google® hangout sessions are classified as Google. **Scenario:** This issue occurs on OAW-4x50 Series switches running AOS-W 6.4 when AppRF is enabled on the switch. **Workaround:** None.

Switch-Platform

Table 107: *Switch-Platform Known Issues*

Bug ID	Description
94615	**Symptom:** The switch may get into an **OutOfMemory** or **kernel panic** state during an AOS-W image upgrade. **Scenario:** This issue is seen when you issue the **tar logs tech-support** command repetitively on the switch. This depletes the kernel **LowFree** memory. This issue is observed in OAW-4306 Series switch running AOS-W 6.4 or later versions. **Workaround:** Do not issue the **tar logs tech-support** command repetitively before upgrading an AOS-W software image.

LLDP

Table 108: *LLDP Known Issues*

Bug ID	Description
94302	**Symptom:** In rare cases, issuing some of the LLDP show commands display the **<ERRS> |lldp| Invalid Physical Port 0 passed at Function: li_get_handle** error message in the log. This issue does not impact any functionality. **Scenario:** This issue is not specific to any switch model and occurs on AOS-W running 6.4. **Workaround:** None.

Startup Wizard

Table 109: *Startup Wizard Known Issues*

Bug ID	Description
98110	**Symptom:** Mobility Switch **Setup Wizard** page gets stuck with Java script error when you click **Next** on the **VLANs and IP Interfaces** tab of the switch's WebUI. **Scenario:** This issue is not limited to any specific switch model and is observed in AOS-W 6.4.0.2. **Workaround:** Use Mozilla® Firefox browser to access the **VLANs and IP Interfaces** tab of the **Setup Wizard** page.
98159	**Symptom: Campus WLAN Wizard** page gets stuck in **Role Assignment** step when you click **Next** on the **Authentication Server** step of the switch's WebUI using Microsoft® Internet Explorer 10 or Internet Explorer 11. **Scenario:** This issue is not limited to any specific switch model and is observed in AOS-W 6.4.0.2. **Workaround:** Use any browser other than Internet Explorer 10 and Internet Explorer 11 to access the **Role Assignment** tab under the **Setup Wizard** page.

Known Issues and Limitations in AOS-W 6.4.0.0

The following are known issues and limitations in AOS-W 6.4.0.0. Applicable Bug IDs and workarounds are included.

AirGroup

Table 110: *AirGroup Known Issues*

Bug ID	Description
91690	**Symptom**: Clients were unable to use AirGroup services to connect to other iChat clients. **Scenario**: This issue was observed in AOS-W 6.3.0.1, and is triggered because AirGroup does not support unsolicited advertisements required by iChat. As a result, clients are unable to immediately discover each other when they log in to the network using Bonjour. **Workaround**: None.
94208	**Symptom:** Wireless Clients such as iPad and iPhone running the SONOS® Switch application do not discover the SONOS music system. **Scenario:** This issue is observed when AirGroup is enabled on a switch with the SONOS music system connected. **Workaround:** None.

AP-Platform

Table 111: *AP-Platform Known Issues*

Bug ID	Description
91172	**Symptom:** A switch crashes occasionally during freeing some corrupted memory packets. **Scenario:** This issue is not limited to any specific switch model or release version. **Workaround:** None.
93876	**Symptom:** Occasionally, the CPSEC CAPs unexpectedly reboot. **Scenario:** This issue occurs on all AP platforms with CPESEC and CAPs and may be caused by IKEv2 timing out. **Workaround:** None.
91805 93963	**Symptom:** An AP reboots occasionally without reboot reason or crash information. **Scenario:** This issue occurs on the OAW-AP125 running AOS-W 6.3.0.1. **Workaround:** None.
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. **Workaround:** None.
95260	**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. **Workaround:** None.
95764	**Symptom:** An 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. **Workaround:** None.

AP-Wireless

Table 112: *AP-Wireless Known Issues*

Bug ID	Description
69424 71334 74646 75248 75874	**Symptom:** When upgraded to AOS-W 6.2, OAW-AP125 crashes and reboots. **Scenario:** This issue is observed when upgrading to AOS-W 6.2 from AOS-W 6.1.3.2 and later in any deployment with an OAW-AP125. **Workaround:** None. **Duplicate Bugs:** The following bug IDs have reported similar issues: 78978, 78981, 79891, 80054, 85753, 87250, 87360, 88619, 88620, 88989, 89537, 91689, 92641, 92975, 93079, 93455, 93811, 91689
86184	**Symptom:** Wireless clients are unable to associate to an access point on the 5GHz radio. **Scenario:** This issue is observed when a channel change in an access point fails after a Dynamic Frequency Selection (DFS) radar signature detection. This issue is observed in OAW-AP125 running AOS-W 6.1.x, 6.2.x, 6.3.x, and 6.4.x. **Workaround:** None.
91510	**Symptom**: An access point reboots occasionally without reboot reason or crash information. **Scenario**: This issue occurs on OAW-AP134 and OAW-AP135 connected to switches running AOS-W 6.3.0.1. **Workaround**: None.
93380	**Symptom:** Occasionally, an AP stops responding and reboots.

Table 112: *AP-Wireless Known Issues*

Bug ID	Description
93494 93687 93744	**Scenario:** This issue is observed because of the Ethernet connectivity problem leading to loss of connectivity between the AP and switch. This issue occurs on OAW-AP224 and OAW-AP225 models and is not limited to a specific AOS-W version. **Workaround**: Ensure that the Ethernet connection issue does not lead to loss of connectivity between the AP and the switch.
93511 93953	**Symptom:** The user gets error **Could not read cached limits** and **License number mismatch in cached limits** messages in a switch with master-local topology. **Scenario:** This issue is not limited to any specific switch model and is observed in switches running AOS-W 6.3 or later. **Workaround**: None.
95113 95086 95088 95111 95114	**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.x.x. **Workaround**: Disable **Multiple Tx Replay Counters** parameter under SSID profile. **Duplicate Bugs:** The following bug IDs have reported similar issues: 95115, 95116, 95117, 95123, 95124

Base OS Security

Table 113: *Base OS Security Known Issues*

Bug ID	Description
93550	**Symptom:** Running the **aaa test-server** command for a TACACS authentication server displays **AAA server timeout** in spite of successful authentication. **Scenario:** This issue is not limited to a specific switch model or software release version. **Workaround:** Issue the **aaa test-server** command twice.
95449	**Symptom:** A switch reboots and displays the message **Reboot Cause: Nanny rebooted machine - fpapps process died**. **Scenario:** This issue may occur in OAW-S3 switches running AOS-W 6.3 in a master-local topology. **Workaround:** None.

Captive Portal

Table 114: *Captive Portal Known Issues*

Bug ID	Description
92927	**Symptom:** When Apple® clients try to access a web page using captive portal, the switch displays **error occurred** message on the client's browser. **Scenario:** This issue is observed in a Virtual AP (VAP)-SSID enabled network with external captive portal authentication. Further investigation suggested that the backslash (\) character is not URL-encoded. As a result, external captive portal stops working for Apple clients. **Workaround:** None.

Configuration

Table 115: *Configuration Known Issues*

Bug ID	Description
93922	**Symptom:** A custom banner with the **#** delimiter gets added as part of the **show running-config** command output. **Scenario:** The 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 or later versions. **Workaround:** None.
95535	**Symptom:** The ACL configuration on the local switches goes out of sync intermittently with the master switch. **Scenario:** This issue may occur if there is a change in licenses. This issue is observed in switches running AOS-W 6.3 in a master-local topology. **Workaround:** Use the **clear master-local-session <local IP>** command on the master switch to sync the ACL configuration.

Switch-Datapath

Table 116: *Switch-Datapath Known Issues*

Bug ID	Description
91085	**Symptom:** Google hangout sessions are classified as Google when AppRFv2 is enabled. **Scenario:** This issue occurs on OAW-4x50 Series switches running AOS-W 6.4. **Workaround:** None.
92248	**Symptom:** A crash occurs on a master switch and the log files for the event listed the reason for the crash as **datapath timeout**. **Scenario:** The trigger of this issue is not known and this issue is observed in OAW-4604switches running AOS-W 6.3.1.0 in a master-local topology. **Workaround:** None.
92477	**Symptom:** Bittorrent sessions are not denied only when the deny rule is added in the middle of a bittorrent file download. **Scenario:** This issue occurs because the bittorrent control session information is deleted once the traffic is classified. This issue occurs on OAW-4x50 Series switcheswhen DPI is set to On. **Workaround**: Creating a bittorrent rule in the user role before a bittorrent file download denies the bittorrent traffic.
93285	**Symptom:** An OAW-S3 switch reboots unexpectedly. The log files for the event listed the reason as **datapath timeout**. **Scenario**: This issue occurs in OAW-S3 switches running AOS-W 6.3.X.X. **Workaround:** None.
93582	**Symptom:** An OAW-4550 switch crashes. The logs for this error listed the reason for the crash as **datapath timeout**. **Scenario:** This issue is observed in OAW-4550 switches running AOS-W 6.3.1.0. **Workaround:** None.
93817	**Symptom:** The master switch throws an internal error while provisioning APs that belong to a specific local switch. **Scenario:** This issue occurs on OAW-4504 switches running AOS-W 6.3.1.1 in a master-local topology. **Workaround:** None.

Table 116: *Switch-Datapath Known Issues*

Bug ID	Description
94143	**Symptom:** An OAW-4504 switch reboots unexpectedly. The log files for the event listed the reason as **datapath timeout**. **Scenario:** This issue is observed on an OAW-4504 switch running AOS-W 6.3.1.1. **Workaround:** None.
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. **Workaround:** None.
94267	**Symptom**: After an upgrade to AOS-W 6.3.1.x, clients unexpectedly disconnected from the network, or were unable to pass traffic for 2-3 minutes after roaming between APs. **Scenario**: This issue was observed in Psion Omni handheld scanners roaming between OAW-AP175 and OAW-AP120 Series APs running AOS-W 6.3.1.1. **Workaround**: None.
94636	**Symptom:** A crash occurs on a local switch and the log files for the event listed the reason for the crash as **datapath timeout**. **Scenario:** The trigger of this issue is not known and this issue is observed in OAW-4550 switches running AOS-W 6.3.0.1. **Workaround:** None.
93203 94965 95719	**Symptom:** An OAW-4550 switch crashes. The logs for this error listed the reason for the crash as **datapath timeout**. **Scenario:** The trigger of this issue is not known and this issue is observed in OAW-4550 switches running AOS-W 6.3.1.1 in a master-local topology. **Workaround:** None.
95286	**Symptom:** A master switch crashes with log message **datapath timeout**. **Scenario:** The trigger of this issue is unknown and is observed in OAW-4650 switches running AOS-W 6.3.1.1. **Workaround:** None.

Switch-Platform

Table 117: *Switch-Platform Known Issues*

Bug ID	Description
80200 81225 81752 81930 84672	**Symptom:** The OAW-4306 Series and OAW-4x04 Series switches reboots with kernel panic. **Scenario:** This issue is observed because of high traffic in control plane for a sustained period. This issue occurs on OAW-4306 Series and OAW-4x04 Series switches running AOS-W 6.3.0.0 or later. **Workaround:** Configure bandwidth contracts depending on the incoming traffic. **Duplicate Bugs:** The following bug IDs have reported similar issues: 85422, 87079, 89014, 89243, 89726
92968	**Symptom:** Generating the **tech-support.log** file from the WebUI of the switch gets truncated at times. **Scenario:** This issue is not limited to a specific switch model and is observed in AOS-W 6.2.1.3, AOS-W 6.3.1.0 or later versions. **Workaround:** Issue the **tar logs tech-support** command from the CLI to download the **tech-support.log** file.
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.

Table 117: *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-4x50 Series switches with OAW-AP225 APs following an upgrade to AOS-W 6.4. **Workaround:** None.
95071	**Symptom**: Issuing a show command from the CLI of a standby switch running AOS-W 6.3.1.1 triggers the error "Module Configuration Manager is Busy" **Scenario**: This issue was observed in a standby OAW-4704 switch in a master-standby topology, **Workaround**: None.

DHCP

Table 118: *DHCP Known Issues*

Bug ID	Description
94345	**Symptom:** The Symbol N410 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.
95166	**Symptom:** When a switch is configured as a DHCP server,by default it attempts Dynamic DNS updates and the following log message appears: "dhcpd: if CU-iPad-2-64-GB.aspect.com IN A rrset doesn't exist add CU-iPad-2-64-GB.aspect.com 10800 IN A 169.136.135.108: destination address required." **Scenario:** This issue is observed on switches running AOS-W 6.3 and later. It is caused when the DHPCD server issues a DHCP address and then attempts a DDNS update. **Workaround:** None.

Hardware-Management

Table 119: *Hardware-Management Known Issues*

Bug ID	Description
87191 87808	**Symptom:** A switch unexpectedly stops responding and reboots. **Scenario:** This issue is observed when a module (hwMon) crashes on the switch. This issue occurs on OAW-S3 series switches running AOS-W 6.3.0.1 or later. **Workaround:** None.

IPSec

Table 120: *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 limit when IKEv2 with GCM256-EC384 encryption algorithm configured. **Scenario:** This issue is observed on OAW-4306 Series, OAW-4x04 Series, and OAW-S3 switches and occurs when the IKE session is established to a standby unit in a failover deployment. **Workaround:** None.
95634	**Symptom:** Site-to-Site IPsec VPN tunnels randomly lose connectivity on an OAW-4550 switch. **Scenario:** This issue is observed where there are 500 or more remote sites terminating IPsec VPN tunnels on an OAW-4550 switch. This issue is observed on an OAW-4550 switch running AOS-W 6.3.1.2. **Workaround:** None.

Local Database

Table 121: *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.

LLDP

Table 122: *LLDP Known Issues*

Bug ID	Description
92998	**Symptom:** The remote interface name appears as **Not received** while issuing the **show lldp neighbor** command. **Scenario**: This issue occurs when Link Layer Discovery Protocol (LLDP) is enabled on the switch and if the neighbor is a third-party device such as Arista or Alcatel. This issue is not specific to any switch model and occurs on AOS-W running 6.4. **Workaround:** None.

Master-Local

Table 123: *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 or later versions. **Scenario:** This issue is observed on an OAW-4x50 Series switch running AOS-W 6.3.1 or later versions. **Workaround:** Disabling the configuration snapshot by executing the **cfgm set sync-type complete** command on master and standby switches prevents partial configuration loss. Wait at least five (5) minutes after the upgraded master and standby have rebooted before reloading the upgraded local switch.
88919	**Symptom:** Global configuration like user-role on the master switch does not synchronize with the local switch after issuing the **write memory** command. **Scenario:** This issue is observed in a master-local topology. This issue is observed in OAW-4x50 Series switch running AOS-W 6.3.0.0 or later versions. **Workaround:** On the master switch, issue the **cfgm set sync-type complete** command, followed by the **write memory** command to send the complete configuration file to the local switch.

RADIUS

Table 124: *RADIUS Known Issues*

Bug ID	Description
94081	**Symptom:** Multiple authentication failures are observed in the switches. **Scenario:** This issue is observed when external LDAP server is used for authentication. This issue is not limited to a specific switch models and occurs in AOS-W running 6.3.x versions. **Workaround:** Reduce LDAP timeout parameter value to 3 seconds for LDAP servers.

Remote AP

Table 125: *Remote AP Known Issues*

Bug ID	Description
95572	**Symptom:** Wired clients are unable to access the internet when connected to a Remote AP (RAP). **Scenario:** This issue is observed when wired clients cannot pass traffic locally with source NAT in split-tunnel forwarding mode. This issues is observed when the OAW-4504 switch is upgraded from AOS-W 6.1.3.6 to AOS-W 6.3.1.2. **Workaround:** None.
95658	**Symptom:** Cisco® Unified IP Phone 7945G reboots randomly during an active voice call. **Scenario:** This issue is observed when a Cisco Unified IP Phone 7945G is connected to a Power over Ethernet (PoE) port of an OAW-RAP3WNP remote AP. This issues is observed in AOS-W 6.3.0.1. **Workaround:** None.

Station Management

Table 126: *Station Management Known Issues*

Bug ID	Description
85662 84880 88009 88319 89321	**Symptom:** The state of APs are displayed as **down** on the master switch even if these APs are connected and UP. **Scenario**: This issue is observed when AP's system profile has a local switch as the primary Local Management Switch (Primary-LMS) and master switch is configured as a backup Local Management Switch (Backup-LMS). This issue is not limited to any specific switch model and occurs in AOS-W running 6.3 or later. **Workaround:** Remove master switch as backup LMS during initial phase. **Duplicate Bugs:** The following bug IDs have reported similar issues: 92164, 93243, 93388, 93389, 93984
91758	**Symptom**: Stationary Apple® MacBook laptops unexpectedly disassociated from APs, and were temporarily unable to pass traffic for 3-5 minutes during a period when many users on the network were roaming between APs. **Scenario**: This issue occurs on a network with a switch running AOS-W 6.3.1.1 with ARM channel assignment and scanning features enabled. **Workaround**: Disable ARM channel assignment and scanning features.

Voice

Table 127: *Voice Known Issues*

Bug ID	Description
90888	**Symptom:** The **show voice real-time-analysis** command does not display any result for voice calls between Microsoft® Lync clients. **Scenario:** This issue is observed when Microsoft Lync clients are connected to the same Remote AP (RAP) in split-tunnel forwarding mode. In such a case, the voice packets are locally routed through the RAP without forwarding it to the switch. As a result, the switch does not display any Real-time Transport Analysis (RTPA) report. This issue is observed in switches running AOS-W 6.4. **Workaround:** None.

WebUI

Table 128: *WebUI Known Issues*

Bug ID	Description
90026	**Symptom:** When a user attempts to access the switch WebUI, the WebUI returns the **Session Invalid** error message. **Scenario:** The user is forced to attempt to access the WebUI two to three times before successfully logging in. Each failed attempt returns the **Session Invalid** error message. This error occurs on switches running AOS-W 6.3.0.1. **Workaround:** None.
93454	**Symptom:** The **Dashboard** > **Spectrum** page of the WebUI is not loading and re-subscription fails frequently. **Scenario:** This issue is observed in OAW-AP105 access points associated to switches running AOS-W 6.3.0.1. **Workaround:** Use the **ap spectrum clear-webui-view-settings** command to avoid this issue.
95185	**Symptom:** Collecting the **logs.tar** and **tech-support** logs from the switch's WebUI fails with **Error running report… Error: receiving data from CLI, interrupted system call** error message. **Scenario:** This issue is not seen under the following cases: • Downloading the **logs.tar** without the **tech-support** log from the WebUI. • Downloading the **logs.tar** and **tech-support** logs from the CLI. This issue is observed in OAW-4650 switch running AOS-W 6.3.1.2. **Workaround:** Download the **logs.tar** and **tech-support** logs from the CLI.

Issues Under Investigation

The following issues have been reported in AOS-W 6.4.x and are being investigated.

Switch-Datapath

Table 129: *Switch -Datapath Issues Under Investigation*

Bug ID	Description
95532	**Symptom:** AnOAW-4550 switch running AOS-W 6.3.1.1 stopped responding and rebooted. The log files for the event listed the reason as **datapath timeout**.

Switch-Platform

Table 130: *Switch -Platform Issues Under Investigation*

Bug ID	Description
95125	**Symptom:** A switch unexpectedly reboots when upgrading to AOS-W 6.3.0.2.
101003	**Symptom:** Centralized image upgrade over TFTP does not work if the image file is in subdirectory. Centralized upgrade over TFTP works if the image file is in root directory.

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

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

Topics in this chapter include:

Upgrade Caveats

- If your switch is running AOS-W 6.4.0.0 or later versions, do not use Windows-based TFTP server to copy an AOS-W image onto the non-boot partition of the switch for upgrading or downgrading. Use FTP or SCP to copy the image. For more information, see bug ID 99197 on page 79.
- AP LLDP profile is not supported on OAW-AP120 Series in AOS-W 6.4.x.
- Starting from AOS-W 6.3.1.0, the local file upgrade option in the OAW-4306 and OAW-4306G switch WebUI has been disabled.
- The local file upgrade option in the OAW-4x50 Series switch WebUI does not work when upgrading from AOS-W 6.2. 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.
- AOS-W 6.4.x does not allow you to create redundant firewall rules in a single ACL. AOS-W will consider a rule redundant if the primary keys are the same. The primary key is made up of the following variables:
  - source IP/alias
  - destination IP/alias
  - proto-port/service

  If you are upgrading from AOS-W 6.1 or earlier and your configuration contains an ACL with redundant firewall rules, upon upgrading, only the last rule will remain.

  For example, in the below ACL, both ACE entries could not be configured in AOS-W 6.4.x. 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
```

- AOS-W 6.4.x is supported only on the newer MIPS switches (OAW-4x50 Series, OAW-S3, OAW-4504XM, OAW-4604, OAW-4704, and OAW-4306 Series). Legacy PPC switches (OAW-4302, OAW-4308, OAW-4324, SC1/SC2) and OAW-4504 switches are not supported. Do not upgrade to AOS-W 6.4.x if your deployment contains a mix of MIPS and PPC switches in a master-local setup.
- When upgrading the software in a multi-switch network (one that uses two or more Alcatel-Lucent switches), special care must be taken to upgrade all the switches in the network and to upgrade them in the proper sequence. (See Upgrading in a Multi-Switch Network on page 97.)

Peer Switch Upgrade Requirement

If you are running an L2 and L3 GRE tunnel between two or more Alcatel-Lucent switches with **keepalive** enabled, all peer switches must be upgraded to AOS-W 6.4.1.0. This is not a requirement if **keepalive** is disabled on the peer switches.

During the upgrade procedure, if one switch is upgraded and the other end point switch is yet to be upgraded, the GRE tunnel goes down. It is recommended to schedule a maintenance window to upgrade the peer switches.

Points to Remember

- AOS-W 6.4.1.0 continues to support L2 GRE tunnel type zero, but it is recommended to use a non-zero tunnel type.
- If both L2 and L3 tunnels are configured between end point devices, you must use a non-zero tunnel type for L2 GRE tunnels.

Installing the FIPS Version on AOS-W 6.4.1.0

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 will not be able to 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.
- Always upgrade the non-boot partition first. If problems occur during the upgrade, you can restore the flash, and switch back to the boot partition. Upgrading the non-boot partition gives you a smoother downgrade path should it be required.
- Before you upgrade to this version of AOS-W, assess your software license requirements and load any new or expanded licenses you require. For a detailed description of these new license modules, refer to the “Software Licenses” chapter in the user guide.

Memory Requirements

All Alcatel-Lucent switches store critical configuration data on an onboard compact flash memory module. Ensure that there is always free flash space on the switch. Loading multiple large files such as JPEG images for RF Plan can consume flash space quickly. To maintain the reliability of your WLAN network, Alcatel-Lucent recommends the following compact memory best practices:

- 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 96 to copy the **crash.tar** file to an external server, then issue the command **tar clean crash** to delete the file from the switch.
- **Flash Backups:** Use the procedures described in Backing up Critical Data on page 96 to back up the flash directory to a file named **flash.tar.gz**, then issue the command **tar clean flash** 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 96 to copy the **logs.tar** file to an external server, then issue the command **tar clean logs** to delete the file from the switch.

Backing up Critical Data

It is important to frequently backup 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

Backup and Restore Compact Flash in the WebUI

The WebUI provides the easiest way to backup and restore the entire compact flash file system. The following steps describe how to backup and restore the compact flash file system using the WebUI on the switch:

1. Click on the **Configuration** tab.
2. Click **Save Configuration** at the top of the page.
3. Navigate to the **Maintenance > File > Backup Flash** page.
4. Click **Create Backup** to backup 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**.

Backup 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 backup 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 Alcatel-Lucent switches), special care must be taken to upgrade all switches based on the switch type (master or local). Be sure to back up all switches being upgraded, as described in Backing up Critical Data on page 96.

NOTE

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

To upgrade an existing multi-switch system to this version of AOS-W:

1. Load the software image onto all switches (including redundant master switches).
2. If all the switches cannot be upgraded with the same software image and rebooted simultaneously, use the following guidelines:
   a. Upgrade the software image on all the switches. Reboot the master switch. Once the master switch completes rebooting, you can reboot the local switches simultaneously.
   b. Verify that the master and all local switches are upgraded properly.

Upgrading to AOS-W 6.4.1.0

Install Using the WebUI

CAUTION

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 95

NOTE

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 AOS-W 6.4.1.0.

- 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 and install the latest version of AOS-W 5.0.4.x.
- For AOS-W 6.0.0.0 or 6.0.0.1 versions, download and install the latest version of AOS-W 6.0.1.x.

Follow step 2 to step 11 of the procedure described in Upgrading From a Recent version of AOS-W on page 98 to install the interim version of AOS-W, then repeat step 1 to step 11 of the procedure to download and install AOS-W 6.4.1.0.

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:

- 3.4.4.1 or later
- 5.0.3.1 or later 5.0.x (If you are running AOS-W 5.0.3.1 or the latest 5.0.x.x, review Upgrading to AOS-W 6.4.1.0 on page 97 before proceeding further.)
- 6.0.1.0 or later 6.x

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 AOS-W 6.4.1.0 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 command **sha256sum <filename>** or use a suitable tool for your operating system that can generate a **SHA256** hash of a file.
   c. Verify that the output produced by this command matches the hash value found on the support site.

The AOS-W image file is digitally signed, and is verified using RSA2048 certificates pre-loaded on the switch at the factory. Therefore, even if you do not manually verify the SHA hash of a software image, the switch will not load a corrupted image.

4. Log in to the AOS-W WebUI from the PC or workstation.
5. Navigate to the **Maintenance > Switch > Image Management** page.
   a. Select the **Upload Local File** option.
   b. Click **Browse** to navigate to the saved image file on your PC or workstation.
6. Select the downloaded image file.
7. In the **partition to upgrade** field, select the non-boot partition.
8. In the **Reboot Switch After Upgrade** option field, best practices 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 will not take effect until you reboot the switch.

9. In the **Save Current Configuration Before Reboot** field, select **Yes**.
10. Click **Upgrade**.

    When the software image is uploaded to the switch, a popup window displays the message **Changes were written to flash successfully**.
11. Click **OK**.

    If you chose to automatically reboot the switch in step 8, the reboot process starts automatically within a few seconds (unless you cancel it).
12. When the reboot process is complete, log in to the WebUI and navigate to the **Monitoring > 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. Log in into 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 would expect.

4. Test a different type of client for each access method that you use and in different locations when possible.
5. Complete a back up 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 96 for information on creating a backup. If the flash (Provisioning/Backup) image version string shows the letters *rn*, for example, 3.3.2.11-rn-3.0, note those AP names and IP addresses. The OAW-RAP5/OAW-RAP5WN reboots to complete the provisioning image upgrade.

Install Using the CLI

Confirm that there is at least 40 MB of free memory and at least 60 MB of flash available for an upgrade using the CLI. For details, see Memory Requirements on page 95.

Upgrading From an Older Version of AOS-W

Before you begin, verify the version of AOS-W currently running on your switch. If you are running one of the following versions of AOS-W, you must download and upgrade to an interim version of AOS-W before upgrading to AOS-W 6.4.1.0.

- 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 RN-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 6.0.0.0 or 6.0.0.1 versions, 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 on page 99 to install the interim version of AOS-W, then repeat step 1 to step 7 of the procedure to download and install AOS-W 6.4.1.0.

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:

- 3.4.4.1 or later
- 5.0.3.1 or later 5.0.x (If you are running AOS-W 5.0.3.1 or the latest 5.0.x.x, review Upgrading to AOS-W 6.4.1.0 on page 97 before proceeding further.)
- 6.0.1.0 or later 6.x

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

1. Download AOS-W 6.4.1.0 from the customer support site.
2. Open a Secure Shell session (SSH) on your master (and local) switches.
3. Execute the **ping** command to verify the network connection from the target switch to the SCP/FTP/TFTP server:

   ```
   (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
   ---------------------------------
   Partition               : 0:0 (/dev/ha1)
   Software Version        : AOS-W 6.1.1.0 (Digitally Signed - Production Build)
   ```

```
Build number            : 28288
Label                   : 28288
Built on                : Thu Apr 21 12:09:15 PDT 2012
----------------------------------
Partition               : 0:1 (/dev/hda2) **Default boot**
Software Version        : AOS-W 6.1.3.2 (Digitally Signed - Production Build)
Build number            : 38319
Label                   : 38319
Built on                : Fri June 07 00:03:14 2013
```

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-4x50 Series switches.

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

```
(hostname)# show image version

----------------------------------
Partition               : 0:0 (/dev/hda1) **Default boot**
Software Version        : AOS-W 6.4.1.0 (Digitally Signed - Beta Build)
Build number            : 44233
Label                   : 44233
Built on                : Thu Jun 12 11:33:31 PDT 2014
----------------------------------
Partition               : 0:1 (/dev/hda2)
Software Version        : AOS-W 6.1.3.2 (Digitally Signed - Production Build)
Build number            : 38319
Label                   : 38319
Built on                : Fri June 07 00:03:14 2013
```

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. Log in into 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 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 96 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 AOS-W 6.4.1.0 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 6.4.1.0 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 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 96.
2. Verify that control plane security is disabled.
3. Set the switch to boot with the previously-saved pre-AOS-W 6.4.1.0 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-AOS-W 6.4.1.0 flash backup from the file stored on the switch. Do not restore the AOS-W 6.4.1.0 flash backup file.
   - You do not need to re-import the WMS database or RF Plan data. However, if you have added changes to RF Plan in AOS-W 6.4.1.0, the changes do not appear in RF Plan in the downgraded AOS-W version.
   - If you installed any certificates while running AOS-W 6.4.1.0, 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.

   ```
   (host) # boot config-file <backup configuration filename>
   ```

3. Execute the **show image version** command to view the partition on which your previous software image is stored. You cannot load a new image into the active system partition (the default boot).

   In the following example, partition 1, the backup system partition, contains the backup release AOS-W 6.1.3.2. Partition 0, the default boot partition, contains the AOS-W 6.4.1.0 image:

   ```
   #show image version
   ---------------------------------
   Partition               : 0:0 (/dev/hda1) **Default boot**
   Software Version        : AOS-W 6.4.1.0 (Digitally Signed - Beta Build)
   Build number            : 44233
   Label                   : 44233
   Built on                : Thu Jun 12 11:33:31 PDT 2014
   ---------------------------------
   Partition               : 0:1 (/dev/hda2)
   Software Version        : AOS-W 6.1.3.2 (Digitally Signed - Production Build)
   Build number            : 38319
   Label                   : 38319
   Built on                : Fri June 07 00:03:14 2013
   ```

4. Set the backup system partition as the new boot partition:

   ```
   (host) # boot system partition 1
   ```

5. Reboot the switch:

   ```
   (host) # reload
   ```

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

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

Before You Call Technical Support

Before you place a call to Technical Support, follow these steps:

1. Provide a detailed network topology (including all the devices in the network between the user and the Alcatel-Lucent switch with IP addresses and Interface numbers if possible).
2. Provide the wireless device's make and model number, OS version (including any service packs or patches), wireless NIC make and model number, wireless NIC's driver date and version, and the wireless NIC's configuration.
3. Provide the switch logs and output of the **show tech-support** command via the WebUI Maintenance tab or via the CLI (**tar logs tech-support**).
4. Provide the syslog file of the switch at the time of the problem. Alcatel-Lucent strongly recommends that you consider adding a syslog server if you do not already have one to capture logs from the switch.
5. Let the support person know if this is a new or existing installation. This helps the support team to determine the troubleshooting approach, depending on whether you have an outage in a network that worked in the past, a network configuration that has never worked, or a brand new installation.
6. Let the support person know if there are any recent changes in your network (external to the Alcatel-Lucent switch) or any recent changes to your switch and/or AP configuration. If there was a configuration change, list the exact configuration steps and commands used.
7. Provide the date and time (if possible) 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.