AOS-W 6.5.0.0

Alcatel·Lucent

Release Notes

Copyright Information

Specifications in this manual are subject to change without notice.

Originated in the USA.

AOS-W, Alcatel 4302, Alcatel 4304, Alcatel 4306, Alcatel 4308, Alcatel 4324, Alcatel 4504, Alcatel 4604, Alcatel 4704, Alcatel 6000, OAW-AP41, OAW-AP68, OAW-AP60/61/65, OAW-AP70, OAW-AP80, OAW-AP92/93, OAW-AP105, OAW-AP120/121, OAW-AP124/125, OAW-AP175, OAW-IAP92/93/105, OAW-RAP2, OAW-RAP5, and Omnivista 3600 Air Manager are trademarks of Alcatel-Lucent in the United States and certain other countries.

Any other trademarks appearing in this manual are the property of their respective companies. Includes software from Litech Systems Design. The IF-MAP client library copyright 2011 Infoblox, Inc. All rights reserved. This product includes software developed by Lars Fenneberg et al.

Legal Notice

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

Copyright Information

Open Source Code

This product includes code licensed under the GNU General Public License, the GNU Lesser General Public License, and/or certain other open source licenses. A complete machine-readable copy of the source code corresponding to such code is available upon request. This offer is valid to anyone in receipt of this information and shall expire three years following the date of the final distribution of this product version by Hewlett Packard Enterprise Company. To obtain such source code, send a check or money order in the amount of US $10.00 to:

Hewlett Packard Enterprise Company
Attn: General Counsel
3000 Hanover Street
Palo Alto, CA 94304
USA

Revision History

The following table provides the revision history of this document.

Table 1: *Revision History*

Revision	Change Description
Revision 02	Updated the Supported Browser section with Microsoft Edge and Chrome. Added the following sections: ● New and Deprecated Hardware Platforms ● Huawei E3372 Modem Support
Revision 01	Initial release.

AOS-W 6.5.0.0 is a major software release that introduces several new features and fixes to the issues detected in previous releases.

NOTE

See the Upgrade Procedure on page 89 for instructions on how to upgrade your switch to this release.

Chapter Overview

- New Features provides a description of features and enhancements introduced in AOS-W 6.5.0.0.
- Regulatory Updates describes the regulatory updates in AOS-W 6.5.0.0.
- Resolved Issues describes the issues resolved in AOS-W 6.5.0.0.
- Known Issues describes the known and outstanding issues identified in AOS-W 6.5.0.0.
- Upgrade Procedure on page 89 describes the procedures for upgrading a switch to AOS-W 6.5.0.0.

NOTE

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

Supported Browsers

The following browsers are officially supported for use with AOS-W 6.5.0.0 Web User Interface (WebUI):

- Microsoft Internet Explorer 10.x and 11 on Windows 7 and Windows 8
- Mozilla Firefox 23 or later on Windows Vista, Windows 7, and Mac OS
- Apple Safari 5.1.7 or later on Mac OS
- Chrome 51.0.2704.103 m (64-bit)
- Microsoft Edge 25.10586.0.0 and Microsoft Edge HTML 13.10586

Contacting Support

Table 2: *Contact Information*

Contact Center Online	
Main Site	http://www.alcatel-lucent.com/enterprise
Support Site	https://service.esd.alcatel-lucent.com
Email	esd.support@alcatel-lucent.com
Service & Support Contact Center Telephone	
North America	1-800-995-2696
Latin America	1-877-919-9526
EMEA	+800 00200100 (Toll Free) or +1(650)385-2193
Asia Pacific	+65 6240 8484
Worldwide	1-818-878-4507

New Features in 6.5.0.0

This section describes the new features, enhancements, and hardware introduced in AOS-W 6.5.0.0. For more information about these features, refer to the *AOS-W 6.5.0.0 User Guide*.

New and Deprecated Hardware Platforms

Table 3 lists the new hardware platforms introduced in AOS-W 6.5.0.0. Table 4 lists the hardware platforms deprecated from AOS-W 6.5.0.0.

Table 3: *New Hardware Platforms in AOS-W 6.5.0.0*

Hardware	Description
OAW-AP310 Series	The OAW-AP310 Series (OAW-AP314 and OAW-AP315) wireless access points support IEEE 802.11ac standards for a high-performance WLAN. For more details, see section, Support for OAW-AP310 Series Access Points on page 11.
OAW-AP330 Series	The OAW-AP330 Series (OAW-AP334 and OAW-AP335) wireless access points support IEEE 802.11ac standards for high-performance WLAN. For more details, see section, Support for OAW-AP330 Series Access Points on page 11.

Table 4: *Deprecated Hardware Platforms in AOS-W 6.5.0.0*

Hardware	Hardware Models Not Supported from AOS-W 6.5.0.0	Last Supported Release
OAW-AP120 Series	OAW-AP120, OAW-AP121, OAW-AP124, and OAW-AP125 access points	AOS-W 6.4.4.x
OAW-4306 Series switches	OAW-4306, OAW-4306G, and OAW-4306G switches	AOS-W 6.4.4.x
OAW-4x04 Series switches	OAW-4504XM, OAW-4604, and OAW-4704 switches	AOS-W 6.4.4.x
OAW-S3 and OAW-6000 switches	OAW-S3 and OAW-6000 switches	AOS-W 6.4.4.x

For the complete list of end-of-life products, refer to http://www.arubanetworks.com/support-services/end-of-life/.

Adaptive Radio Management (ARM)

Cellular Handoff Assist is Configurable Per Virtual AP

The cellular handoff assist feature can help a dual-mode, 3G/4G-capable Wi-Fi device such as an iPhone, iPad, or Android client at the edge of Wi-Fi network coverage switch from Wi-Fi to an alternate 3G/4G radio that provides better network access. This setting can now be applied to individual virtual APs via the WLAN virtual-ap profile.

Dynamic Bandwidth Switch

ARM's dynamic bandwidth switch feature provides capability for ARM to detect the 20 MHz interferer by reading the Clear Channel Assessment (CCA) statistics and other radio statistics. Once the signatures are detected, ARM moves to another 80 MHz channel or downgrades to 40 MHz. This feature only works when **dynamic-bw** parameter is enabled and ARM is set to use 80 MHz assignment.

ARM Channel Planning Enhancements

Starting from AOS-W 6.5.0.0, the following enhancements have been made to resolve issues that occur with distributed channel/power algorithm:

- **Push random channel assignments to APs:** Random channels are pushed from the local switch Station Management (STM)/System AP Manager (SAMP) to APs that belong to a specific ap-group. This helps in replacing the dynamic channel change solution in a high-density environment, thereby overcoming the issue with convergence.
- **Reduce interference channel change:** To reduce the number of interference channel changes and to configure the weight of interfering APs when calculating the interference index, the **interfering-ap-weight** parameter has been introduced in the **rf-arm-profile** command.

Pending Client-Match Steers

The pending client match entries are no longer displayed in the output of the **show ap arm client-match history** command which now displays only the last 32 completed moves. A new parameter **pending** is introduced to the **show ap arm client-match** command. This parameter is introduced to filter and view only the pending client-match entries where the moves have not completed.

OV3600 Management

Clarity Synthetic

Clarity Synthetic enables the switch to select and convert any OAW-AP200 Series access point to client mode based on the instruction from a Network Management System (NMS). The converted AP acts like a Wi-Fi client and starts synthetic data transaction within the network to monitor and detect the network health.

AMON

AMON Packet Size

When upgrading from an existing AOS-W 6.4.x release, it is required to set AMON packet size manually to a desired value. However, the packet size is increased to 32K by default for fresh installations of AOS-W 6.5.0.0.

AP-Platform

AP Name in SNMP Traps

When an access point goes out of service, the SNMP traps list the name and IP address of the access point as identifiers.

Support for OAW-AP310 Series Access Points

The OAW-AP310 Series (OAW-AP314 and OAW-AP315) wireless access points support IEEE 802.11ac standards for a high-performance WLAN. This device is equipped with two single-band radios, which provide network access and monitor the network simultaneously. This access point can deliver high-performance 802.11n 2.4 GHz and 802.11ac 5 GHz functionality, while also supporting 802.11a/b/g wireless services. Multi-User Multiple-Input Multiple-Output (MU-MIMO) is enabled when operating in 5 GHz mode for optimal performance. The OAW-AP310 Series wireless access points work in conjunction with a switch.

The OAW-AP310 Series wireless access points provide the following capabilities:

- IEEE 802.11a/b/g/n/ac wireless access point
- IEEE 802.11a/b/g/n/ac wireless air monitor
- IEEE 802.11a/b/g/n/ac spectrum monitor
- Compatible with IEEE 802.3at and 802.3af PoE
- Support for MCS8 and MCS9
- Centralized management, configuration, and upgrades
- Integrated Bluetooth Low Energy (BLE) radio

For more information, see the *OAW-AP310 Series Wireless Access Point Installation Guide*.

Support for OAW-AP330 Series Access Points

The OAW-AP330 Series (OAW-AP334 and OAW-AP335) wireless access points support IEEE 802.11ac standards for high-performance WLAN. This device is equipped with two dual-band radios, which provide network access and monitor the network simultaneously. This access point delivers high-performance 802.11n 2.4 GHz and 802.11ac 5 GHz functionality, while also supporting 802.11a/b/g wireless services. Multi-User Multiple-Input Multiple-Output (MU-MIMO) is enabled when operating in 5 GHz mode for optimal performance. The OAW-AP330 Series wireless access points work in conjunction with a switch.

The OAW-AP330 Series wireless access points provides the following capabilities:

- IEEE 802.11a/b/g/n/ac wireless access point

- IEEE 802.11a/b/g/n/ac wireless air monitor
- IEEE 802.11a/b/g/n/ac spectrum monitor
- Compatible with IEEE 802.3at power sources
- Centralized management, configuration, and upgrades
- Integrated Bluetooth Low Energy (BLE) radio

For more information, see the *OAW-AP330 Series Wireless Access Point Installation Guide*.

USB Enhancement for OAW-AP335 Remote Access Points

For OAW-AP335 remote access points using AT power supply or Power over Ethernet (PoE), the USB port is shut down. If an OAW-AP335 remote access point (RAP) uses DC power supply, the USB port is enabled.

NOTE

By default, the USB port is enabled for all supported RAPs. The OAW-AP335 remote access point is an exception.

Novatel U620L Modem Support

AOS-W 6.5.0.0 introduces the support for the Novatel U620L 4G LTE USB modem for Verizon's LTE service on the OAW-RAP3WN, OAW-RAP108, OAW-RAP109, OAW-RAP155P, OAW-AP205H, OAW-AP210 Series, OAW-AP220 Series, OAW-AP310 Series, OAW-AP320 Series, and OAW-AP330 Series access points.

Huawei E3372 Modem Support

AOS-W 6.5.0.0 introduces the support for the Huawei E3372 4G LTE USB modem on the OAW-RAP3WN, OAW-RAP108, OAW-RAP109, OAW-RAP155P, OAW-AP205H, OAW-AP210 Series, OAW-AP220 Series, OAW-AP310 Series, OAW-AP320 Series, and OAW-AP330 Series access points.

Plug and Play 4G USB Modem

AOS-W 6.5.0.0 supports the USB modem Plug and Play. The switch auto-configures the 4G USB modem as soon as the user plugs in the modem into an AP or a RAP. The following 4G USB modems support Plug and Play:

- Netgear AirCard 340U (AT&T)
- Netgear AirCard 341U (Srpint)
- Franklin Wireless U770 (Sprint)
- Pantech UML290 (Verizon)
- Pantech UML295 (Verizon)
- Novatel MC551L (Verizon)
- Novatel U620L (Verizon)

NOTE

During a switch uplink failover from wired to cellular network, if a Netgear 340U Aircard modem switches to airplane mode unexpectedly, execute the switch console command **usb reclassify**. This command disconnects and reclassifies the USB device

Support for Secondary AP Master

Starting from AOS-W 6.5.0.0, seamless connectivity is provided even when the master switch fails, by allowing an access point to terminate on a secondary master switch.

PortFast Support for AP's Access Ethernet Port

In AOS-W 6.5.0.0, the PortFast feature has been enhanced to reduce the time taken for wired clients connected to an AP to detect the link before data traffic is sent.

Consolidated AP-Provisioned Information

Starting from AOS-W 6.5.0.0, a new feature that records the consolidated AP-provisioned information is introduced.

In situations where an AP does not come UP after a reboot, it would help troubleshooting when information about how the AP was provisioned is available. This new feature allows you maintain a consolidated record of AP-provisioned information, which will include the following details: static IP, dynamic IP, DHCP, DNS, Master information, previous local management switch (LMS) information, and more.

When an AP loses connection with the switch, you can retrieve the AP’s provisioning information by one of the following means:

- Executing a shell script after logging in to the AP through console or backup-SSID
- Executing appropriate CLI commands from the switch

Support for Viewing AP Power Monitoring Information

Starting from AOS-W 6.5.0.0, the output of the **show ap debug system-status** command displays the power monitoring information with real-time sensor values for the OAW-AP314, OAW-AP315, OAW-AP334, and OAW-AP335 access points.

Customizing AP Console Logging Level

Starting from AOS-W 6.5.0.0, switches provide support for customizing the level of driver log prints sent to the AP console. A new parameter, **console-log-lvl** is introduced under the **ap system-profile** command to set the AP console logging level.

AP-Wireless

VHT Bandwidth Signaling

Starting from AOS-W 6.5.0.0, the Very High Throughput (VHT) bandwidth signaling can be enabled or disabled. This parameter is supported only on OAW-AP320 Series access points. This setting appears only in the switch CLI.

Authentication

Support for IKE Fragmentation

AOS-W 6.5.0.0 supports the functionality where non-Aruba devices can fragment the large IKE_AUTH packets using the standards described in the **RFC 7383 – Internet Key Exchange Protocol Version 2 (IKEv2) message fragmentation** when the Alcatel-Lucent device acts as a responder and not as an initiator.

Device Name as Username

When a client is authenticated by non-802.1X method of authentication, the host name of the host device is used as the username (instead of the MAC address) of the host device.

Base OS Security

OCSP Configuration for AOS-W VIA

Starting from AOS-W 6.5.0.0, the following configuration parameters are removed to simplify the OCSP configuration for AOS-W VIA:

- ike url config: ocsp-responder ike-url
- eap url config: ocsp-responder eap-url
- ike cn name: ocsp-responder ike-cn
- eap cn name: ocsp-responder eap-cn

These parameters will be picked up directly from the certificate.

To enable OCSP certificate verification, the **ocsp-responder enable** subcommand is introduced in the **aaa authentication via connection profile** command. A corresponding option is available in the WebUI.

Branch Switches

WAN Health Check for Branch Switch Uplinks

The WAN health-check feature uses ping or User Datagram Protocol (UDP) probes to measure WAN availability and latency on selected uplinks. Based on the results of this health-check information, the switch can continue to use its primary uplink, or failover to a backup link. This feature can also measure the jitter while connecting to a remote host by sending and measuring packets at fixed intervals. If you enable this feature on a branch switch, jitter data appears in the **WAN** dashboard, in the **Dashboard** section of the WebUI.

App and App Category Visibility

Switches classify the traffic into multiple priorities and shape the egress traffic to match the actual upstream bandwidth. If there is any unused bandwidth in the downstream direction, switches allow the users to use the unused bandwidth although this bandwidth exceeds the allocation limit for the user. Switches ensure this by using an ingress scheduler with minimum-bandwidth guarantees. Minimum-bandwidth guarantees are provided on per traffic class basis. Additional classification is done on the traffic flows and these are assigned newer traffic classes. Use hardware assist or software scheduler to schedule these new traffic classes to achieve minimum-bandwidth guarantees. Maximum bandwidth is enforced with bandwidth contracts.

Captive Portal

Customizing Authentication Reply-Message to Captive Portal Users

AOS-W 6.5.0.0 introduces the support for customizing authentication Reply-Message to captive portal users in the log-in page for better user experience. The purpose behind the Reply-Message is to return appropriate information to the captive portal system.

IPv6 Address for Netdestination

The Captive Portal whitelist supports IPv6 addresses for netdestination.

Centralized Licensing

Multi-Version Licensing

AOS-W 6.5.0.0 supports multi-version licensing, which allows centralized licensing clients to run a different version of the license than that of the primary and backup licensing servers. If a license is introduced in a newer version of AOS-W, the primary and backup licensing servers set can still distribute licenses to licensing clients running an older version of AOS-W, even if the licensing client does not recognize the newer license type.

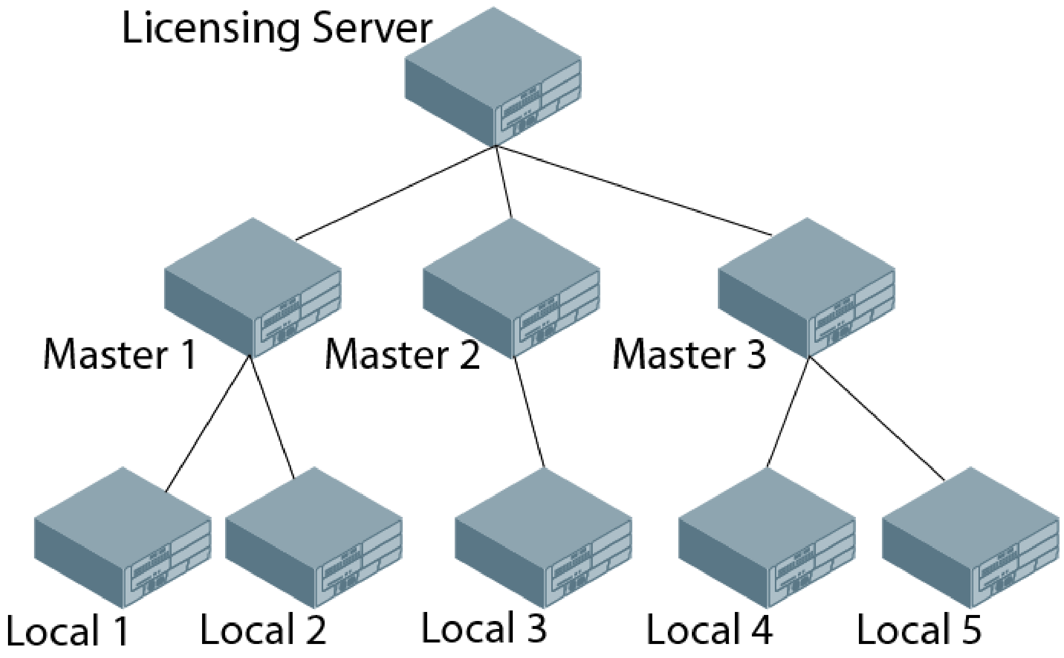
Support for Larger Switch Deployments

Improvements to the centralized licensing feature allow this feature to support very large deployments with up to 1600 switches.

Support for Multiple Master/Local Domains

A centralized licensing server now supports multiple master/local domains—topologies where multiple masters have one or more attached local switches. This topology requires that all local switches are able to access the licensing server. Previous releases of AOS-W only supported topologies with local if all local switches using centralized licensing were associated to a single master switch, or to a redundant master switch pair.

Figure 1 *Local Switches using Centralized Licensing in a Multi-Master Domain*



NOTE

All master switches should have the same advanced or enhanced security configuration. Mismatch in the security key will affect centralized licensing.

Switch-Platform

OAW-4008 Switch

The OAW-4008 switch is a wireless LAN switch that connects, controls, and intelligently integrates wireless APs and Air Monitors into a wired LAN system. The OAW-4008 switch includes the following specifications:

- 8 Ethernet ports
- 1 console port
- 1 USB 2.0 port

This switch supports up to 16 APs and 1024 users.

Disable Console Access

Starting from AOS-W 6.5.0.0, a new command, **mgmt-user console-block**, is introduced to disable the console-login. The purpose of this command is to introduce an ability to lock down all console ports, for example, micro USB, mini USB on the switch to enable high-level security. This also ensures that no Secure Shell (SSH) access is allowed at the remote branch office. The SSH is only allowed from the headquarters through the IPsec tunnel.

Remote Telnet or SSH Session from the Switch

Starting from AOS-W 6.5.0.0, an administrator can initiate a remote telnet or SSH session from the switch to a remote host. The host can be a switch or a non-Alcatel-Lucent host.

NTP Standalone

NTP standalone feature enables an Alcatel-Lucent switch to act as an NTP server so that the devices that do not have access to Internet can synchronize their clocks. Enabling this feature eliminates the need to provision and maintain another virtual machine on the network.

Switch Port-Security MAC Address Limitation

Starting from AOS-W 6.5.0.0, the MAC address limitation, a port-security feature, is enhanced for the OAW-40xx Series and OAW-4x50 Series switches. You can enable or disable this functionality using the WebUI or the CLI.

The **switchport port-security** command is enhanced to include parameters for setting the levels of security and autorecovery interval time. You can set appropriate values for the **level** parameter to log a warning message—**Max bridge entries limit hit on the port #**—in syslog and/or to shut down the port. For **level**, the default value is logging. You can set the autorecovery interval time (in seconds) in the range of 1–65,535.

When a port-security error occurs, the switch shuts down the port so that no traffic is received by the switch on this port. The **clear** command is modified to include the **port-security-error gigabitethernet <slot/module/port>** parameter to resolve the port-security error and bring UP the port.

Firewall

Geo-Location Filtering

Starting from AOS-W 6.5.0.0, to support IP-classification-based firewall, an IP reputation database containing a list of IP addresses with malicious activities is introduced. This helps in rejecting the traffic sent to or received from those IP addresses classified as malicious based on the policy configured. Using the geolocation IP database, the geographical location of the malicious IP address is also determined, and traffic is permitted or denied after scanning the geography-based rules configured by the administrator.

Routing Traffic Through Web Proxy

When the switch needs to access data on the cloud or the Internet, and if the Internet-bound traffic needs to pass through a proxy, execute the **web-proxy server** command. When the command is executed the switch routes web (HTTP/HTTPS) traffic through the proxy server.

Redirect User Session

The **block-redirect-url** command has been introduced to redirect a user session to an URL when it encounters a WebCC deny policy.

IPsec

HP Platform Interoperating with Alcatel-Lucent Switches

HP Trusted Platform Module (TPM) based switches can now interoperate with the Alcatel-Lucent switches and create the IKE/IPsec tunnels. These HP switches are running the software version k.16.02.

IPv6

Radius Accounting for IPv6 Clients

Starting from AOS-W 6.5.0.0, customers can monitor bandwidth usage by clients/hosts with IPv6 addresses over Remote Authentication Dial-In User Service (RADIUS) protocol. The **Framed-IPv6-Address** attribute is used in accounting start, stop, and interim packets. A host can have multiple IPv6 addresses and all of them are tracked to check the usage for billing purpose.

Subscription-Based Web Content Classification License

AOS-W 6.5.0.0 introduces support for the Web Content Classification (WebCC) license; a subscription-based, per-AP license that supports web content classification features on an AP for the duration of the subscription period (up to 10 years per license)

Virtual Private Network

Support for VIA-Published Subnets

Starting from AOS-W 6.5.0.0, a new feature is introduced to enable the switches accept the subnets published by AOS-W VIA clients. This is in conformation with section 3.15 of RFC 5996 applicable for route-based VPNs. You can enable or disable this feature using the WebUI or the CLI. This feature is disabled by default.

When you enable this feature, switches can accept CFG_SET message with the INTERNAL_IP4_SUBNET attribute type. When a switch receives this message, which consists of an IP address and netmask, it adds an entry to the IP route table that points to the AOS-W VIA's inner IP address as the next-hop. The datapath route-cache for the AOS-W VIA's inner IP will point to the tunnel endpoint associated with the AOS-W VIA.

NOTE

This feature is only applicable for IKEv2 and supports IPv4.

Voice and Video

Wi-Fi Calling

AOS-W 6.5.0.0 supports Wi-Fi Calling in the switch. Wi-Fi calling service allows cellular users to make or receive calls using a Wi-Fi network instead of using the carrier's cellular network.

WebUI

Cloud Management

AOS-W 6.5.0.0 enables the OAW-40xx Series switches to be managed by Aruba Central at a future date.

Smart Configuration

The smart config, which is used to manage branch switches, has been enhanced to allow a VLAN to get an IP address using DHCP. This setting appears only in the WebUI.

Traffic Analysis

Starting from AOS-W 6.5.0.0, the AppRF page in **Dashboard** has been renamed to **Traffic Analysis**.

Blocked Session

Starting from AOS-W 6.5.0.0, a new tab called **Blocked Sessions** is added in the **Traffic Analysis** page. The **Blocked Sessions** tab displays WebCC and AppRF sessions which are blocked by access control list (ACL) through system logging or that blocked on the WebUI interface.

Zero-Touch Provisioning

Static IP Management

Starting from AOS-W 6.5.0.0, the zero-touch provisioning (ZTP) feature is enhanced to support 16 VLANs per branch switch as against just four in the earlier versions of AOS-W.

The Bulk Edit template (in Excel sheet) on the branch switch allows you to specify the static IP assignment for individual branch switch devices. The static IP configuration is maintained in this Bulk Edit CSV file, with each line in the file representing the settings for a specific branch switch device. To support this enhancement, the Bulk Edit Excel sheet (.CSV format) is now expanded to allow for addition of up to 16 VLANs for each branch switch.

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 (CLI) and execute the **show ap allowed-channels country-code <country-code> ap-type <ap-model>** command.

Regulatory Updates in AOS-W 6.5.0.0

The following default Downloadable Regulatory Table (DRT) version is part of AOS-W 6.5.0.0:

- DRT-1.0_55384

For a complete list of countries certified with different AP models, refer to the DRT Release Notes at service.esd.alcatel-lucent.com.

NOTE

This software release supports the channel requirements described in *ALE Support Advisory SA-N0033*, available for download from the service.esd.alcatel-lucent.com site.

Resolved Issues in AOS-W 6.5.0.0

This release includes fixes for Network Time Protocol (NTP) vulnerabilities documented in CVE-2015-7704, CVE- 2015-7705, and CVE-2015-7871. Additionally, the following issues are resolved in this release of AOS-W.

Table 5: *Resolved Issues in 6.5.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
98884 99817 101260	**Symptom:** An application crashed. This issue is resolved by enabling checksum verification and dropping corrupt packets. **Scenario:** This issue occurred because a packet that the application received was corrupt and there was no validation done on the application. This issue was observed in switches running ArubaOS 6.2 or later versions.	Switch Datapath	All platforms	AOS-W 6.2.1.5	AOS-W 6.5.0.0
102055 102056 102059 102060 102061	**Symptom:** A switch crashed and rebooted. This issue is resolved by limiting the event list to 60 events per Call Detail Record (CDR) and adding a check on the statistics limit so that the old statistics is cleared when the threshold limit is reached. **Scenario:** A memory leak was observed in the **UCM** process because it recorded all client events for a CDR until the client went offline. Additionally, the event statistics and statistics list were also maintained. This issue was observed in OAW-4x50 Series switches running AOS-W 6.4.0.3.	Unified Communication and Collaboration (UCC)	OAW-4x50 Series switches	AOS-W 6.4.0.3	AOS-W 6.5.0.0
111799 129425	**Symptom:** The **SAPD** module in a switch did not send the Bluetooth Low Energy (BLE) configuration to the **BLE** process over a PAPI message. Instead, the SAPD module created temporary configuration files. The fix ensures that the **SAPD** module sends PAPI message to the **BLE** process with the BLE configuration. **Scenario:** This issue was observed in switches running AOS-W 6.4.3.6.	Bluetooth Low Energy	All platforms	AOS-W 6.4.3.6	AOS-W 6.5.0.0

Table 5: *Resolved Issues in 6.5.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
113132 113711 124010	**Symptom:** The switch module that manages IKE exchanges for remote and CPSec APs crashed repeatedly. This issue is resolved by avoiding stack corruption and logging it using counter. **Scenario:** This issue was observed with Mac OS clients connected to switches in a congested network and was caused by stack corruption. The crash was observed when Mac OS mode-config IKEv1 clients retried an Extended Authentication even after sending a response to the **config-mode** request.	IPSec	All platforms	AOS-W 6.3.1.12	AOS-W 6.5.0.0
114189	**Symptom:** The firewall visibility cache entries were not cleared in a switch. This issue is resolved by setting the correct DNS entry type. **Scenario:** This issue occurred because IPv4 DNS records of incorrect type set were populated as IPv6 records. This issue was observed in switches running AOS-W 6.4.3.0.	Firewall	All platforms	AOS-W 6.4.3.0	AOS-W 6.5.0.0
114606	**Symptom:** Clients failed to access the Captive Portal page. This issue is resolved by adding checks to prohibit IP snooping. **Scenario:** This issue was observed when a DHCP server was configured with a low DHCP lease time and the **no firewall prohibit-ip-spoofing** parameter was configured in a switch. The DHCP lease time of the IP address that was assigned to a client expired and it was re-assigned to another client. However, a copy of the old user entry remained in the switch. The MAC address mismatched between the new client and the old user entry and the client failed to access the Captive Portal page. This issue was observed in switches running AOS-W 6.3.1.2 or AOS-W 6.4.x.	Captive Portal	All platforms	AOS-W 6.3.1.2	AOS-W 6.5.0.0
116486 123621	**Symptom:** The number of clients displayed in the output of the **show-user-table** command was different from the number of clients displayed in the WebUI by navigating to **Monitoring > CONTROLLER > Clients**. The fix ensures that the same number of clients is displayed in the CLI and the WebUI. **Scenario:** This issue was observed in switches running AOS-W 6.4.2.10.	Base OS Security	All platforms	AOS-W 6.4.2.10	AOS-W 6.5.0.0

Table 5: *Resolved Issues in 6.5.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
116969	**Symptom:** The basic and beacon rates configuration for the VAPs of OAW-AP325 access points were not specific to each SSID. This issue is resolved by enabling the beacon rates separately for different VAPs. **Scenario:** This issue was observed in AP-325 access points connected to switches running AOS-W 6.4.4.0.	AP-Wireless	OAW-AP325 access points	AOS-W 6.4.4.0	AOS-W 6.5.0.0
117675	**Symptom:** After a client associated with a Virtual Access Point (VAP) in tunnel mode with dynamic WEP encryption, it did not send/receive traffic. This issue is resolved by setting null/dummy keys in all key IDs corresponding to WEP and setting cipher to none. **Scenario:** This issue was observed in OAW-AP320 Series access points connected to switches running AOS-W 6.4.4.0.	AP-Wireless	OAW-AP320 Series access points	AOS-W 6.4.4.0	AOS-W 6.5.0.0
117815	**Symptom:** A user could not change the maximum retries setting of an access point. The fix ensures that a user can change the maximum retries setting of access points. **Scenario:** This issue was observed in OAW-AP324 and OAW-AP325 access points connected to switches running AOS-W 6.4.4.0.	AP-Wireless	OAW-AP324 and OAW-AP325 access points	AOS-W 6.4.4.0	AOS-W 6.5.0.0
119884	**Symptom:** Clients were unable to pass traffic even though they were associated to an AP. Improvements to the wireless driver fixes the issue. **Scenario:** On executing the **show ap debug client-table** command, the AP association was displayed as present. However, on executing the **show ap remote debug association**, the **show ap remote debug mgmt-frames**, and the **show ap association** commands, the outputs displayed either stale information or no information for AP association in the Station Management (STM) table. This issue was observed in OAW-AP200 Series, OAW-AP210 Series, and OAW-AP220 Series access points running AOS-W 6.4.2.6.	AP-Wireless	OAW-AP200 Series, OAW-AP210 Series, and OAW-AP220 Series access points	AOS-W 6.4.2.6	AOS-W 6.5.0.0

Table 5: *Resolved Issues in 6.5.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
121020 124020	**Symptom:** Access points crashed with the error **Reboot caused by kernel panic: Fatal exception** message. This issue is resolved by limiting the number of in-transit broadcasts to 128 and the maximum length of the queues to 32 bits. **Scenario:** This issue occurred because the memory was exhausted from several queues with several broadcasts. This issue was observed in OAW-AP275 access points connected to switches running AOS-W 6.4.3.1.	AP-Wireless	OAW-AP275 access points	AOS-W 6.4.3.1	AOS-W 6.5.0.0
121389	**Symptom:** When the Captive Portal (CP) certificate was changed from one custom certificate to another, the default certificate was used instead of the new custom certificate. This issue is resolved by adding a sleep timer between changes to the custom certificate. **Scenario:** This issue was observed because of a timing mismatch between changes to the custom certificate. This issue was observed in switches running AOS-W 6.4.3.2.	Captive Portal	All platforms	AOS-W 6.4.3.2	AOS-W 6.5.0.0
122167	**Symptom:** An error message was displayed when calculating the authentication server response time. This issue is resolved by changing the log level of the error message from ERROR to DEBUG. **Scenario:** This issue was observed when an incorrect timestamp value was retrieved. This issue was observed in switches running AOS-W 6.4.2.8.	Switch-Platform	All platforms	AOS-W 6.4.2.8	AOS-W 6.5.0.0
122270	**Symptom:** The **write mem** command failed if there was a large number of DHCP pools in the switch. This issue is resolved by sending the configuration from the DHCP module to the CLI engine in multiple chunks that are smaller than 40 KB. **Scenario:** This issue was observed because a chunk of configuration exceeded 40 KB, the upper size limit of the message. This issue was observed in switches running AOS-W 6.4.2.8.	DHCP	All platforms	AOS-W 6.4.2.8	AOS-W 6.5.0.0

Table 5: *Resolved Issues in 6.5.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
122287	**Symptom:** A client acquired an incorrect IP address due to incorrect VLAN assignment . This issue is resolved by adding DHCP-based User Derivation Rule (UDR) support for IP mobility when mobility service is not provided to the client. **Scenario:** This issue occurred when DHCP-based VLAN derivation was configured with invalid L3 mobility Home Agent Table entries on the switch. This issue was observed in switches running AOS-W 6.4.4.x versions.	Mobility	All platforms	AOS-W 6.4.4.0	AOS-W 6.5.0.0
122695 128425 134457	**Symptom:** A Remote Access Point (RAP) failed to come online and displayed the **check_aruba_vid: STRAP License not available** error message. This issue is resolved by sending the RAP feature limit and bitmap updates to the applications. **Scenario:** This issue occurred after upgrading a switch to AOS-W 6.4.4.1 and converting a Campus Access Point (CAP) to a RAP.	Licensing	All platforms	AOS-W 6.4.4.1	AOS-W 6.5.0.0
122797	**Symptom:** On configuring a Pre-Shared Key (PSK) for a High Availability (HA) group profile with a plus character, the switch converted the plus character to a blank space. Encoding the values in the WebUI before sending them to the backend resolved this issue. **Scenario:** This issue occurred only when you configure a PSK using the WebUI. This issue was observed in switches running AOS-W 6.4.2.8 or later versions.	WebUI	All platforms	AOS-W 6.4.2.8	AOS-W 6.5.0.0
122814	**Symptom:** A type 9 RADAR was detected multiple times. This issue is resolved by removing the signal with first pulse interval. **Scenario:** This issue was observed in access points connected to switches running AOS-W 6.4.2.6.	AP-Wireless	All platforms	AOS-W 6.4.2.6	AOS-W 6.5.0.0
122939	**Symptom:** 802.11ac-capable access points experienced amplified packet loss during voice calls. This issue is resolved by changing the hybrid-mode spectrum monitoring to be voice-aware. **Scenario:** This issue was observed when spectrum monitoring was enabled on the AP. This issue was observed in 200 , OAW-AP210 Series, OAW-AP220 Series, and OAW-AP270 Series access points running AOS-W 6.4.2.x or AOS-W 6.4.3.x.	Switch-Datapath	OAW-AP200 Series, OAW-AP210 Series, OAW-AP220 Series, and OAW-AP270 Series access points	AOS-W 6.4.2.5	AOS-W 6.5.0.0

Table 5: *Resolved Issues in 6.5.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
123135	**Symptom:** An administrator was unable to configure the **Roaming Consortium entry 1/2/3 OI value and length** parameters with length 0. This issue is resolved by configuring the exact length of the entered string. **Scenario:** This issue occurred because an incorrect configuration design was selected. This issue was observed in switches running AOS-W 6.4.4.0.	Hotspot-11u	All platforms	AOS-W 6.4.4.0	AOS-W 6.5.0.0
123239	**Symptom:** The internal process that manages user authentication stopped responding and crashed in the master switch and logs listed the reason as **Control Processor Kernel** Panic. The fix ensures that the internal process does not crash. **Scenario:** This issue occurred during an Enhanced Client or Proxy (ECP) authentication when the user tried to access **user > l2role**, which is null.	Base OS Security	All platforms	AOS-W 6.3.1.15	AOS-W 6.5.0.0
123401	**Symptom:** During AP reprovisioning, the logs indicated that an internal error related to AP regulatory, was encountered. This issue is resolved by adding **AP-group** and **AP-name** in error log when a nonexisitent **AP-group** or **AP-name** without regulatory-profile is used. **Scenario:** This issue was observed when AP was reprovisioned from an older AP group (that may not exist on the switch) to a newer AP group. This issue was observed in switches running AOS-W 6.4.1.0 or later versions.	AP Regulatory	All platforms	AOS-W 6.4.2.6	AOS-W 6.5.0.0
123437	**Symptom:** A switch continued to display the **fpapps[3645]: <399816> <ERRS> |fpapps| hapiPortLinkStatus: Failed to read phy status on port 0/0/5** error message although the physical port of the switch was in service. The fix ensures that a switch does not generate such false alarms. **Scenario:** This issue was observed when Network Time Protocol (NTP) was configured in a switch. This issue was observed in OAW-40xx Series and OAW-4x50 Series switches running AOS-W 6.4.2.6.	Switch-Platform	OAW-40xx Series and OAW-4x50 Series switches	AOS-W 6.4.2.6	AOS-W 6.5.0.0

Table 5: *Resolved Issues in 6.5.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
123458	**Symptom:** Access points failed to send the Link Layer Discovery Protocol-Media Endpoint Discovery (LLDP-MED) Type-Length-Value (TLV) information after receiving an LLDP packet from a Cisco Voice over Internet Protocol (VoIP) phone. This issue is resolved by enabling the LLDP-MED flag when the downlink Ethernet port comes up if there are LLDP-MED neighbors. **Scenario:** This issue occurred when devices that supported LLDP-MED were connected to the downlink Ethernet port of access points. This issue was observed in access points connected to switches running AOS-W 6.4.3.3 or later versions.	AP-Platform	All platforms	AOS-W 6.4.3.3	AOS-W 6.5.0.0
123561	**Symptom:** Mac OS X client connected to OAW-AP130 Series access points displayed **NA** instead of **NG** for the Nigerian country code. The fix ensures that the correct country code is displayed. **Scenario:** This issue occurred in OAW-AP130 Series access points when 802.11d and 802.11h were enabled on the APs and were provisioned with a regulatory domain code.	AP-Platform	OAW-AP130 Series access points	AOS-W 6.4.2.6	AOS-W 6.5.0.0
123618 124086 125286 125301 125847 128413 128630 129193 129194 129831 130672 132529 138193 139459 143028	**Symptom:** Datapath crashed unexpectedly. This issue is resolved by using DMA channel distribution, avoiding station invalidation, and increasing page size. **Scenario:** This issue was observed when loading 8000 users on OAW-4450 switches running AOS-W 6.4.4.0.	Switch-Datapath	OAW-4450 switches	AOS-W 6.4.4.0	AOS-W 6.5.0.0
123677	**Symptom:** Type 5 and type 7 radars were detected multiple times. This issue is resolved by eliminating type 5 and type 6 radars from the country codes. **Scenario:** This issue was observed in OAW-AP214 access points connected to switches running AOS-W 6.4.2.6.	AP-Wireless	OAW-AP214 access points	AOS-W 6.4.2.6	AOS-W 6.5.0.0

Table 5: *Resolved Issues in 6.5.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
123707	**Symptom:** The **authentication** process on the switch stopped responding and crashed. This issue is resolved when the switch avoids a conflict while deleting an internally created net destination entry. **Scenario:** This issue was seen when a **write memory** command was executed on the master switch leading to a full configuration synchronization on the local switch. The **authentication** process crash was caused while deleting an internally created net destination entry from an Access Control List (ACL). This issue was observed in local switches running AOS-W 6.3.x or AOS-W 6.4.x.	BaseOS Security	All platforms	AOS-W 6.3.1.14	AOS-W 6.5.0.0
123866	**Symptom:** OAW-AP130 Series and OAW-RAP155 access points stopped responding and rebooted. The log files for the event listed the reason as **Reboot caused by kernel panic: Fatal exception**. Improvements in the kernel module resolved this issue. **Scenario:** The kernel panic issue was triggered due to corruption in the memory mapped buffer that was used to send Wi-Fi packets to ARM/WIDS process. This issue was observed in OAW-AP130 Series and OAW-RAP155 access points running AOS-W 6.4.2.x, AOS-W 6.4.3.x, or AOS-W 6.4.4.x.	AP-Wireless	OAW-AP130 Series and OAW-RAP155 access points	AOS-W 6.4.2.7	AOS-W 6.5.0.0
124136 138762	**Symptom:** Clients failed to connect to an SSID. The log files for the event listed the reason as **capability requested by STA unsupported by AP**. This issue is resolved by sending a VLAN discovery message (if required) during a High Availability (HA) failover. **Scenario:** This issue was observed during a failover in an HA set up, when no VLAN was assigned for the virtual AP profile that is configured in tunnel mode.	AP-Wireless	All platforms	AOS-W 6.4.2.5	AOS-W 6.5.0.0

Table 5: *Resolved Issues in 6.5.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
124211 126441 130639 132593 134424 135251 136274 136663 137195 137319 137409 137857 137959 138030 138213 138651 138759 139810 140116 140310 140758 140994 141654 141655 142507 142910	**Symptom:** Users noticed high memory utilization in the **Station Management Module** (STM) when a switch was upgraded to AOS-W 6.4.3.x. The fix ensures that monitoring and statistics related information is properly cleaned up when a station leaves the network. **Scenario:** A change to one of the station identifiers in the system led to some monitoring and statistics information not being cleaned up when a station moved. The issue was observed in switches running AOS-W 6.4.3.x and 6.4.4.x.	Station Management	All platforms	AOS-W 6.4.3.x and 6.4.4.x	AOS-W 6.5.0.0
124275	**Symptom:** All clients obtained IP addresses from the same Virtual Local Area Network (VLAN) even though a RADIUS server Vendor-Specific Attribute (VSA) specified a VLAN pool with multiple VLANs. This issue is resolved by updating the VLAN usage count in the **authorization** module. **Scenario:** This issue occurred when a RADIUS server VSA overwrote the Virtual Access Point (VAP) VLAN with a different VLAN pool that was configured with the **even** assignment type. This issue was observed in switches running AOS-W 6.4.2.6.	Station Management	All platforms	AOS-W 6.4.2.6	AOS-W 6.5.0.0

Table 5: *Resolved Issues in 6.5.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
124286 129845 131026	**Symptom:** The datapath module crashed in a switch. The fix ensures that the datapath module does not crash. **Scenario:** This issue was observed in switches running AOS-W 6.4.3.1.	Switch-Datapath	All platforms	AOS-W 6.4.3.1	AOS-W 6.5.0.0
124323	**Symptom:** The 802.11k neighbor table did not show any access points. This issue is resolved by enhancing the access point search to not have any dependency on the Virtual Access Point (VAP) order and by not checking if the neighbors of an access point are enabled or disabled. **Scenario:** This issue occurred when multi-VAP was configured in switches running AOS-W 6.3.1.5.	AP-Wireless	All platforms	AOS-W 6.3.1.5	AOS-W 6.5.0.0
124441	**Symptom:** Output modifiers were not allowed for the **show firewall dns-names** command. This issue is resolved by allowing the output modifiers for the command. **Scenario:** This issue was observed in switches running AOS-W 6.4.2.8.	Base OS Security	All platforms	AOS-W 6.4.2.8	AOS-W 6.5.0.0
124513 129297	**Symptom:** All switches in a network crashed and rebooted unexpectedly due to high memory consumption by the **isakmpd** process. This issue is resolved by freeing the temporary variable that is used for every tunnel. **Scenario:** This issue occurred when the **isakmpd** process did not free the temporary variable that was used for each tunnel, thereby causing memory leaks. This happened on the responder that was configured to use Fully Qualified Domain Name (FQDN) as the Internet Key Exchange (IKE) identity. This issue was observed on switches running AOS-W 6.4.2.9.	Switch-Platform	All platforms	AOS-W 6.4.2.9	AOS-W 6.5.0.0
124572	**Symptom:**Intel 7260 802.11ac clients that were connected to OAW-AP135 access points reached the default threshold limit of transmission retries, which caused an increase in the jitter, when voice calls were made. The fix ensures that the **jitter average value** is maintained within an acceptable threshold of 20 ms. **Scenario:** This issue was observed while sending data to Intel 7260 802.11ac clients downstream. This issue was observed in OAW-AP135 access point running AOS-W 6.4.2.6.	AP-Wireless	OAW-AP135 access points	AOS-W 6.4.2.6	AOS-W 6.5.0.0

Table 5: *Resolved Issues in 6.5.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
124682 126989	**Symptom:** A client or a switch relayed broadcast traffic when it was connected to a mesh point. This issue is resolved by removing eth0 from the bond0 interface. **Scenario:** This issue occurred when broadcast traffic from a switch to a mesh point's Ethernet 0 interface was sent back. This issue was observed when a client or a switch was connected to a mesh point's Ethernet 0 interface.	Mesh	All platforms	AOS-W 6.4.3.2	AOS-W 6.5.0.0
124886 125129 125567 126381 127879	**Symptom:** The **authentication** process spiked the CPU usage to 99%. This issue is resolved by redesigning the 802.1X reauthentication code to avoid using large lists of timers. **Scenario:** This issue was observed when reauthentication was enabled in the 802.1X authentication profile and there were large number of users in the reauthentication table. As the number of users for reauthentication increased, the authentication process slowed down. Although the 802.1X authentication throughput rate was low, the CPU load for the authentication process spiked above 90%. In systems that had multiple timers, it took many CPU cycles to maintain the timers. Hence, many clients did not pass the 802.1X authentication or user entries were not created for users who passed the 802.1X authentication, especially during busy hours. This issue was observed in switches running AOS-W 6.4.2.4.	BaseOS Security	All platforms	AOS-W 6.4.2.4	AOS-W 6.5.0.0
124917 129757	**Symptom:** OAW-AP205H access points crashed and rebooted. The fix ensures that OAW-AP205H access points do not reboot unexpectedly. **Scenario:** This issue was observed in OAW-AP205H access points connected to switches running AOS-W 6.4.3.3.	AP-Platform	OAW-AP205H access points	AOS-W 6.4.3.3	AOS-W 6.5.0.0
124944 137099	**Symptom:** OAW-AP200 Series access points failed to forward packets received on the up-link port. The fix ensures that the AP can forward packets received on the up-link port. **Scenario:** This issue was caused by the unwanted bytes in a packet during a Cyclic Redundancy Check (CRC). This issue was seen in tunnel forwarding mode only. This issue was observed in OAW-AP200 Series access points running AOS-W 6.4.2.x or AOS-W 6.4.3.x.	AP-Wireless	OAW-AP200 Series access points	AOS-W 6.4.2.6	AOS-W 6.5.0.0

Table 5: *Resolved Issues in 6.5.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
125093 125740 126416 127424 128656 129183 129878 129970 131805 131867 131868 132090	**Symptom:** A switch stopped responding and rebooted. The log files for the event listed the reason as **Reboot Cause: Datapath timeout (Intent:cause:register 56:86:50:2).** The fix ensures that switches do not experience any datapath timeout. **Scenario:** This issue was observed in OAW-4x50 Series switches running AOS-W 6.4.2.x or AOS-W 6.4.3.x.	Switch-Datapath	OAW-4x50 Series switches	AOS-W 6.4.2.6	AOS-W 6.5.0.0
125183 137806	**Symptom:** The **Station Management (STM)** process crashed in the switch. The fix ensures that the **STM** process does not crash while processing an AP whose system profile has not yet been created. **Scenario:** This issue was seen when the STM process was processing an AP whose system profile had not yet been created. This issue was observed in switches running AOS-W 6.4.2.x, AOS-W 6.4.3.x, or AOS-W 6.4.4.x.	Station Management	All platforms	AOS-W 6.4.4.4	AOS-W 6.5.0.0
125225 127492 136564	**Symptom:** A spike in the CPU utilization for the Distributed Data Store (DDS) process was observed in the switch. The fix ensures that the CPU utilization is normal for the DDS process. **Scenario:** This issue was observed in switches running AOS-W 6.4.2.x.	Distributed Data Store	All platforms	AOS-W 6.4.2.4	AOS-W 6.5.0.0
125232	**Symptom:** User-role and Access Control List (ACL)-related configuration were lost when a switch rebooted. This issue is resolved by reducing the number of time-ranges configured. **Scenario:** This issue occurred when switches with large time-range configuration rebooted and the user-role and ACL configuration were not saved. This issue was observed in switches running AOS-W 6.4.2.8.	Base OS Security	All platforms	AOS-W 6.4.2.8	AOS-W 6.5.0.0

Table 5: *Resolved Issues in 6.5.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
125261	**Symptom:** A spike in the CPU utilization for the datapath process was observed in a switch. This issue is resolved by restricting the flooding of unsolicited Neighbor Advertisement (NA) to Wi-Fi tunnels if the ingress port is a Wi-Fi tunnel or the source is not a router. **Scenario:** This issue was observed when a network was flooded with unsolicited NA packets. This issue was observed in switches running AOS-W 6.4.2.x.	IPv6	All platforms	AOS-W 6.4.3.3	AOS-W 6.5.0.0
125316	**Symptom:** On disabling an AP radio, unknown Wi-Fi packets were observed on channel 1. Improvements in the kernel module of the AP resolved this issue. **Scenario:** This issue was seen when an AP radio is disabled in either 2.4 GHz or 5 GHz. This issue was observed in OAW-AP320 Series access points running AOS-W 6.4.4.0.	AP-Wireless	OAW-AP320 Series access points	AOS-W 6.4.4.0	AOS-W 6.5.0.0
125346 127878	**Symptom:** A memory leak was observed in the **mDNS** process. This issue is resolved by removing the AP names that are assigned to all AP modes. **Scenario:** This issue was observed in network topologies with an AirGroup cluster and APs in "only BG mode" in the AP neighborhood. This issue was observed when mDNS queries with AP neighborhood information were sent from one switch to another (within a cluster). This issue was observed in switches running AOS-W version later than 6.4.3.0.	AirGroup	All platforms	AOS-W 6.4.4.0	AOS-W 6.5.0.0
125535	**Symptom:** On executing the **write memory** command on the master switch, few ACLs did not synchronize with the standby switch. The fix ensures that all ACLs synchronize with the standby switch. **Scenario:** This issue was observed in switches running AOS-W 6.4.2.x or 6.4.3.x. in a master-standby topology.	Captive Portal	All platforms	AOS-W 6.4.2.3	AOS-W 6.5.0.0

Table 5: *Resolved Issues in 6.5.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
125538	**Symptom:** OAW-AP105 access points did not send out a PPPoE Active Discovery Initiation (PADI) frame after the switch was upgraded to AOS-W 6.4.4.0. This issue is resolved by updating the Ethernet driver. **Scenario:** This issue was observed when setting up PPPoE on RAPs that were connected to switches running AOS-W 6.4.x and AOS-W 6.3.x. This issue occurred because the hardware setup did not happen until the interface was brought up explicitly. Hence, the **SAPD** process did not start the PPPoE connection because the link state was DOWN.	AP-Platform	OAW-AP105 access points	AOS-W 6.4.4.0	AOS-W 6.5.0.0
125572	**Symptom:** The **delete** command did not work for **Local Switch List For AP Whitelist Sync** and **Master Switch List For AP Whitelist Sync** under **Wireless > AP Installation > Whitelist > Campus AP** or **Remote AP**. The fix ensures that the **delete** command works as expected. **Scenario:** This issue was observed in switches running AOS-W 6.3.1.18.	WebUI	All platforms	AOS-W 6.3.1.18	AOS-W 6.5.0.0
125862	**Symptom:** Users were unable to edit a Virtual Local Area Network (VLAN) range in the port-channel using the WebUI. This issue is resolved by allowing changes to the VLAN range for port-channels. **Scenario:** This issue was observed in both master and local switches running AOS-W 6.4.x in a master-standby-local topology.	WebUI	All platforms	AOS-W 6.4.2.5	AOS-W 6.5.0.0
125889	**Symptom:** Pre-Shared Key (PSK) clients failed to associate to an AP. The log files for the event listed the reason as **Capability requested by STA unsupported by AP**. Sending a VLAN discovery message when there is a change in the Virtual AP (VAP) profile configuration resolved this issue. **Scenario:** This issue was seen when the administrator changed the VAP profile configuration in the switch. In addition, this issue was seen when the VAP profile did not have a VLAN assigned. This issue was observed in switches running AOS-W 6.4.2.x or AOS-W 6.4.3.x.	AP-Wireless	All platforms	AOS-W 6.4.2.9	AOS-W 6.5.0.0

Table 5: *Resolved Issues in 6.5.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
125987 137973 143187	**Symptom:** Switches running AOS-W 6.4.3.2 crashed on the authentication module. This issue is resolved by deriving aaa profile information for the ingress wired port from the correct hash table. **Scenario:** This issue occurred when the switch was processing a **STM_RAP_USER_AGENT_UPDATE** message for split tunnel wired users.	Base OS Security	All platforms	AOS-W 6.4.3.2	AOS-W 6.5.0.0
125997	**Symptom:** Multiple debugging messages were displayed repeatedly. The fix ensures that the number of debugging messages displayed are controlled. **Scenario:** This issue was caused by the **rdnssd** process. This issue was observed in switches running AOS-W 6.4.2.5.	AP-Platform	All platforms	AOS-W 6.4.2.5	AOS-W 6.5.0.0
126145 128293 128294 128295 128343 128369	**Symptom:** 802.11ac-capable access points broadcasted the maximum Equivalent Isotropically Radiated Power (EIRP) values instead of the ARM-configured values after each failover. This issue is resolved by implementing changes that allow the access points to broadcast the ARM-configured values after each failover. **Scenario:** This issue occurred during VRRP, master-to-local and local-to-master failover except High Availability (HA) failover. This issue was observed in OAW-AP200 Series, OAW-AP210 Series, and OAW-AP220 Series access points. This issue was observed after a switch was upgraded to AOS-W 6.4.2.11 or later versions.	AP-Platform	OAW-AP200 Series, OAW-AP210 Series, and OAW-AP220 Series access points	AOS-W 6.4.2.12	AOS-W 6.5.0.0
126237	**Symptom:** Clients failed to get an IP address from random APs, resulting in traffic failure. The fix ensures that the client gets an IP address when a split-tunnel Virtual AP (VAP) is added with the **BS** flag. **Scenario:** This issue was observed when a split-tunnel VAP was added with the **BS** flag which means that the VAP is in bridge and split-tunnel forwarding mode. This resulted in client failing to get an IP address. This issue was observed in switches running AOS-W 6.4.2.12 or later versions.	AP-Datapath	All platforms	AOS-W 6.4.2.12	AOS-W 6.5.0.0

Table 5: *Resolved Issues in 6.5.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
126385	**Symptom:** Clients could not connect to an SSID although the access points were connected to a switch. This issue is resolved by dropping the packets if the access point is not currently active. **Scenario:** This issue occurred when access points worked in active-backup mode with Virtual Access Point (VAP) in bridge mode. This issue was observed in access points connected to switches running AOS-W 6.4.2.12.	AP-Platform	All platforms	AOS-W 6.4.2.12	AOS-W 6.5.0.0
126418	**Symptom:** When the **show ap database flags D** command was executed on a master switch, the output incorrectly displayed a D flag (dirty or no configuration) for access points that had good configuration. This issue is resolved by checking if the **show ap database flags D** command is issued on a master switch and returning 0 when the access points are connected only to local switches. **Scenario:** This issue occurred when access points were connected on the local switches and not the master switch. This issue was observed in switches running AOS-W 6.4.x in a master-local topology.	AP-Platform	All platforms	AOS-W 6.4.2.10	AOS-W 6.5.0.0
126433	**Symptom:** The multicast DNS (mDNS) process crashed in the switch. This issue is resolved by correcting the timer ID immediately after a user is deleted. **Scenario:** This issue was observed when a shared user-list of an AirGroup policy was modified in ClearPass Policy Manager (CPPM) from one user to another and the earlier user was deleted within 5 seconds after changing the policy. This issue was observed in switches running AOS-W 6.4.2.10.	AirGroup	All platforms	AOS-W 6.4.3.1	AOS-W 6.5.0.0
126440 127145 140733	**Symptom:** Clients lost connectivity and were unable to pass traffic when debug log was enabled due to a crash in the process handling AP management and user association. The issue is resolved by removing the reason name mapping in the debug logs for the error codes received from the 802.11k beacon reports. **Scenario:** This issue occurred because the debug log did not have a proper reason name mapping for the error codes received from the 802.11k beacon reports. This issue was observed in switches running AOS-W 6.3.x or AOS-W 6.4.x.	Station Management	All platforms	AOS-W 6.3.1.14	AOS-W 6.5.0.0

Table 5: *Resolved Issues in 6.5.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
126484 130522 131584 131586	**Symptom:** The datapath process crashed in a switch. This issue is resolved by adding a check that avoids memory access beyond the buffer size. **Scenario:** This issue was observed when some attributes were absent in the STUN message for Apple Facetime calls which led to memory access beyond the buffer size. This issue was observed in switches running AOS-W 6.4.4.0.	UCC	All platforms	AOS-W 6.4.4.0	AOS-W 6.5.0.0
126572	**Symptom:** A master switch failed to send Simple Network Management Protocol (SNMP) traps for OAW-AP200 Series access points. The fix ensures that the master switch sends the correct SNMP traps when there is a change in the transmit power level of access points. **Scenario:** This issue occurred when the transmit power level of access points changed. This issue was observed in OAW-AP200 Series access points connected to switches running AOS-W 6.4.2.12.	ARM	OAW-AP200 Series access points	AOS-W 6.4.2.12	AOS-W 6.5.0.0
126589	**Symptom:** A switch stopped responding and rebooted repeatedly. This issue is resolved by preventing the Command Line Interface (CLI) from getting configured on the switch. **Scenario:** This issue was observed in Xsec opmode for WLAN. This issue was observed in OAW-4x50 Series switches running AOS-W 6.3.1.x.	Switch-Datapath	OAW-4x50 Series switches	AOS-W 6.3.1.18	AOS-W 6.5.0.0
126646	**Symptom:** The **mDNS** process crashed in a switch. This issue is resolved by checking for the existence of a cleanup service and ending a timer to free the cleanup service. **Scenario:** This issue was observed when a full configuration synchronization occurred in a switch after one minute of disabling any AirGroup service. This issue was observed in switches running AOS-W 6.4.4.0 in master-local or Virtual Router Redundancy Protocol (VRRP) topology.	AirGroup	All platforms	AOS-W 6.4.4.0	AOS-W 6.5.0.0

Table 5: *Resolved Issues in 6.5.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
126670	**Symptom:** When an ACL name was removed or added from an interface, the applied count of the ACLs were not updated. This issue is resolved by ensuring that ACLs on a physical interface are not changed when the system is powered on. **Scenario:** This issue was observed when ACLs were changed on a physical interface. This was observed in switches running AOS-W 6.3.1.5.	Configuration	All platforms	AOS-W 6.3.1.5	AOS-W 6.5.0.0
126690	**Symptom:** Certain Dell Latitude laptops with Dell Wireless 1501 wireless adapter failed to get an IP address when associating to OAW-AP200 Series, OAW-AP210 Series, OAW-AP220 Series, or OAW-AP270 Series access points. Improvements in the wireless driver of the AP resolved this issue. **Scenario:** This issue was caused by a wrong AP beacon. When High Throughput (HT) was disabled in **rf dot11g-radio-profile** and enabled in **rf ht-ssid-profile**, AP beacon advertised HT IE. Due to this, the Dell wireless 1501 wireless adapter failed to get an IP address. This issue was observed in OAW-AP200 Series, OAW-AP210 Series, OAW-AP220 Series, or OAW-AP270 Series access points running AOS-W 6.4.2.x or AOS-W 6.4.3.x.	AP-Wireless	OAW-AP200 Series, OAW-AP210 Series, OAW-AP220 Series, or OAW-AP270 Series access points	AOS-W 6.4.2.12	AOS-W 6.5.0.0
126713	**Symptom:** A switch sent authentication requests to an authentication server that was out of service. This issue is resolved by resetting the cache entries of the authentication server group. **Scenario:** This issue occurred when an authentication server went out of service after authenticating a user and the same server was reused for authentication in the next instance. The authentication server stored in the user context was reused even if the server was out of service. This issue was observed in switches running AOS-W 6.4.2.5.	Base OS Security	All platforms	AOS-W 6.4.2.5	AOS-W 6.5.0.0.
126736	**Symptom:** Home Agent/Foreign Agent configuration did not work with anchor table and clients that sent DHCP discover with unicast flag. This issue is resolved by making an exception for ARP/DHCP flood optimization when the mobility feature is enabled. **Scenario:** This issue occurred when the mobility feature was used with static IP and DHCP clients. This issue was observed in switches running AOS-W 6.4.3.4.	Switch-Datapath	All platforms	AOS-W 6.4.3.4	AOS-W 6.5.0.0

Table 5: *Resolved Issues in 6.5.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
126749	**Symptom:** Master-standy redundancy using VRRP did not work with untrusted ports when **firewall prohibit-IP spoofing** command was disabled. The fix ensures that VRRP works as expected when ports are set to untrusted. **Scenario:** When users upgraded to AOS-W 6.4.3.2, the **no firewall prohibit-ip-spoofing** command did not function as desired. As a result, master-standby redundancy using VRRP did not work with untrusted ports also stopped functioning. This issue was observed in switches running AOS-W 6.4.3.2.	Switch-Datapath	All platforms	AOS-W 6.4.3.2	AOS-W 6.5.0.0
126793 128230 131927 132149 132304 134889 137322 140746	**Symptom:** An AP crashed unexpectedly. The log file for the event listed the reason as **kernel panic: PC is at nss_core_handle_napi**. The fix ensures that the AP works as expected. **Scenario:** This issue occurred because of corrupted Network Switching Subsystem (NSS) descriptor. This issue was observed in OAW-AP324 access points running AOS-W 6.4.4.1.	AP-Wireless	OAW-AP324 access points	AOS-W 6.4.4.1	AOS-W 6.5.0.0
126905	**Symptom:** Only 99 user derivation rules were retained after a switch was rebooted. The fix ensures that all the user derivation rules are retained after the switch is reloaded. **Scenario:** When the **show aaa derivation-rules user** command was executed after the switch was rebooted, it was observed that only 99 rules were retained when 100 or more derivation rules were configured. This issue was not limited to any specific switch model or AOS-W release version.	Base OS Security	All platforms	AOS-W 6.4.2.8	AOS-W 6.5.0.0
126926	**Symptom:** Few Google Chromecast applications did not work when AirGroup was enabled on the switch. This issue is resolved by sending the wildcard query for unique service IDs that are not part of the **allowall** service. **Scenario:** This issue occurred because of a change in the Google cast support to application queries for Google Chromecast. This issue was observed in switches running AOS-W 6.4.x or later versions.	AirGroup	All platforms	AOS-W 6.4.2.10	AOS-W 6.5.0.0

Table 5: *Resolved Issues in 6.5.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
127210 128489	**Symptom:** The **Print Preview** page in a Google Chrome web browser was blank after logging in to a switch with the guest provisioning account. This issue is resolved by removing the reference to stylesheet. **Scenario:** This issue occurred because of a wrong reference to a stylesheet. This issue was observed after logging in to a switch using Google Chrome 46.0.2490.71m web browser and previewing the page to print the guest user credentials. This issue was observed in switches running AOS-W 6.3.1.x, AOS-W 6.4.3.x, or AOS-W 6.4.4.x.	WebUI	All platforms	AOS-W 6.4.3.4	AOS-W 6.5.0.0
127359 131197 131432 132495	**Symptom:** AP-228 and OAW-AP270 Series mesh portal and mesh points did not form a mesh link when they were connected to Cisco 3850 and 2960x Power Over Ethernet (POE) switches. This issue is resolved by adding a delay during the initial setup till the power profile changes to POE-AT. **Scenario:** This issue was observed in AP-228 and OAW-AP270 Series access points connected to switches running AOS-W 6.4.3.x or AOS-W 6.4.4.x.	Mesh	AP-228 and OAW-AP270 Series access points	AOS-W 6.4.3.5	AOS-W 6.5.0.0
127421	**Symptom:** The authentication process crashed in a switch. This issue is resolved by clearing the memory pointers whenever the memory is freed. **Scenario:** This issue was observed in switches with active Lightweight Directory Access Protocol (LDAP) server connections. This issue was observed in switches running AOS-W 6.4.3.x or later versions.	Base OS Security	All platforms	AOS-W 6.4.3.1	AOS-W 6.5.0.0
127460	**Symptom:** Multiple RADAR detections were observed on 80 MHz Dynamic Frequency Selection (DFS) channels. This issue is resolved by improving the detection algorithm for specific type of RADAR pulse. **Scenario:** This issue was observed in switches running AOS-W 6.4.3.3.	AP-Wireless	All platforms	AOS-W 6.4.3.3	AOS-W 6.5.0.0

Table 5: *Resolved Issues in 6.5.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
127489	**Symptom:** The sequence number of the heartbeats received from some access points were frozen at a particular number. This issue is resolved by: ● Deleting the IPsec tunnel with a Remote Access Point (RAP) based on MAC address when the RAP comes up. ● Including the ID field, which represents the destination NAT port in the lookup, tunnel addition, and tunnel deletion during outbound Security Association (SA). **Scenario:** This issue was observed in PSK-based RAP deployment behind Network Address Translation (NAT) servers. This issue was observed in RAPs connected to switches running AOS-W 6.4.0.3.	Switch-Datapath	All platforms	AOS-W 6.4.0.3	AOS-W 6.5.0.0
127848	**Symptom:** Access points did not reconnect their Point-to-Point Protocol over Ethernet (PPPoE) to the backup local management switch (LMS) when the primary LMS was not available. The fix ensures that access points reconnect their PPPoE to the backup LMS. **Scenario:** This issue was observed in OAW-AP205 and OAW-AP274 access points connected to switches running AOS-W 6.4.4.0.	Remote AP	OAW-AP205 and OAW-AP274 access points	AOS-W 6.4.4.0	AOS-W 6.5.0.0
127937 130815 131103 131239 133516 135969 139944	**Symptom:** A switch crashed because of datapath timeout after upgrading the switch to AOS-W 6.4.2.13. This issue is resolved by optimizing the inactive-user timeout logic. **Scenario:** This issue occurred when the fragmented untrusted traffic came from a client for an active session when the client user entry was not created in the switch.	Switch-Datapath	All platforms	AOS-W 6.4.2.13	AOS-W 6.5.0.0
127946	**Symptom:** OAW-AP325 access points rebooted with the reason **Reboot caused by kernel panic: Rebooting the AP because of FW ASSERT reason**. This issue is resolved by adding checks on the host side before sending WMI events. **Scenario:** This issue occurred when clients associated with access points and the host sent WMI event with incorrect Network Switching Subsystem (NSS) number. This issue was observed in OAW-AP325 access points connected to switches running AOS-W 6.4.4.1.	AP-Wireless	OAW-AP325 access points	AOS-W 6.4.4.1	AOS-W 6.5.0.0

Table 5: *Resolved Issues in 6.5.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
127971	**Symptom:** When user authentication failed, a switch did not update the syslog entry with the authentication method used. This issue is resolved by adding the authentication method to the log and by changing the log entry from USER to USER-DEBUG. **Scenario:** This issue occurred when replacing the old log entry 52,2042 with 52,2275. However, the new log entry did not include the authentication method. This issue was observed in switches running AOS-W 6.4.x.	Base OS Security	All platforms	AOS-W 6.4.2.12	AOS-W 6.5.0.0
127989	**Symptom:** OAW-AP325 access points rebooted at random times. The log file for the event listed the reason as **Failed over to standby**. This issue is resolved by not freeing a hardware crypto session when a tunnel using software encryption is destroyed. **Scenario:** This issue occurred when software encryption was used instead of hardware encryption for IPsec tunnels and an IPsec tunnel using software encryption was destroyed. This issue was observed in OAW-AP325 access points connected to switches running AOS-W 6.4.4.1.	AP-Platform	OAW-AP325 access points	AOS-W 6.4.4.1	AOS-W 6.5.0.0
128057	**Symptom:** In centralized licensing, the number of remaining licenses mismatched with the number of remaining AP capacity on the licensing master switch. This issue is resolved by not accounting the number of standby APs when calculating the remaining AP capacity. **Scenario:** This issue occurred when centralized licensing was enabled and standby APs were also accounted for while calculating the remaining AP capacity. Also, there were switches in HA mode in which backup APs were present. This issue was observed in switches running AOS-W 6.4.x or later versions.	AP-Platform	All platforms	AOS-W 6.4.2.8	AOS-W 6.5.0.0

Table 5: *Resolved Issues in 6.5.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
128170	**Symptom:** When an AirGroup service was deleted, the **mDNS** process crashed on the switch. The fix ensures that the **mDNS** process does not crash after deleting an AirGroup service. **Scenario:** This issue was observed because a list was created when an AirGroup service was disabled and a NULL value was not assigned to the list when the list was removed. Later, if the same AirGroup service was deleted, the **mDNS** process crashed when it tried to access a list which was removed but not assigned a NULL value. This issue was observed in switches running AOS-W 6.4.4.2.	AirGroup	All platforms	AOS-W 6.4.4.2	AOS-W 6.5.0.0
128348	**Symptom:** Intermittent high Noise Floor (NF) was observed in access points. This issue is resolved by increasing the NF calibration time on the home channel. **Scenario** This issue occurred when scanning was enabled and NF calibration parameters were not set correctly after returning to home channel. This issue was observed in access points connected to switches running AOS-W 6.4.4.1.	AP-Wireless	All platforms	AOS-W 6.4.4.1	AOS-W 6.5.0.0
128441	**Symptom:** Packet loss was seen during peak data traffic. This issue is resolved by increasing the platform limit for sessions from 32768 to 65536. **Scenario:** This issue was observed because system's session limit was reached. Session tables were full, so a new session entry could not be allocated due to which the associated packets dropped. This issue was observed in OAW-40xx Series series switches with session limit of 32k (32768) running AOS-W 6.4.x.	Switch-Datapath	OAW-40xx Series switches	AOS-W 6.4.2.13	AOS-W 6.5.0.0
128457	**Symptom:** The **wlsxMeshNodeEntryChanged** trap generated by a master switch due to a mesh link reset did not contain complete information about which mesh link was reset. This issue is resolved by incorporating a check for this trap while handling another trap for the table change type. **Scenario:** This issue occurred in a master switch running AOS-W 6.4.3.1. This issue was not limited to any specific switch model.	SNMP	All platforms	AOS-W 6.4.3.1	AOS-W 6.5.0.0

Table 5: *Resolved Issues in 6.5.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
128459	**Symptom:** The AirGroup user list showed IPv6 entries although the AirGroup IPv6 option was disabled. The fix ensures that IPv6 entries are not shown in the AirGroup user list when the AirGroup IPv6 option is disabled. **Scenario:** This issue occurred when the AirGroup IPv6 option was disabled. This issue was observed in switches running AOS-W 6.4.4.3.	AirGroup	All platforms	AOS-W 6.4.4.3	AOS-W 6.5.0.0
128460	**Symptom:** Users were not assigned the correct role-based VLAN after a full 802.1X authentication when the role was changed by Change of Authorization (CoA). This issue is resolved by allowing free role transitions to/from CoA/ESI roles without looking for priorities. **Scenario:** This issue occurred while conforming to a set of priorities when changing roles. This issue was observed in switches running AOS-W 6.4.3.4.	Base OS Security	All platforms	AOS-W 6.4.3.4	AOS-W 6.5.0.0
128461	**Symptom:** OAW-AP103H access points crashed with the **athr_gmac_recv_packets:1744: assertion failed** error message. This issue is resolved by emptying a pending received task before clearing an internal flag. **Scenario:** This issue occurred when a pending received tasklet was not emptied before clearing an internal flag. This issue was observed in OAW-AP103H access points connected to switches running AOS-W 6.4.2.5.	AP-Platform	OAW-AP103H access points	AOS-W 6.4.2.5	AOS-W 6.5.0.0
128466	**Symptom:** A switch displayed the **Invalid TLS version** error message in authentication trace buffer after uploading a new certificate for Extensible Authentication Protocol-Protected Extensible Authentication Protocol (EAP-PEAP) authentication. This resulted in user authentication failure. This issue is resolved by adding zeros to the private key so that it is 256 bytes in length. **Scenario:** This issue occurred while decrypting the pre-master secret key when a client attempted Transport Layer Security (TLS) for 802.1X authentication. This issue was observed in switches running AOS-W 6.4.2.x.	Base OS Security	All platforms	AOS-W 6.4.2.12	AOS-W 6.5.0.0

Table 5: *Resolved Issues in 6.5.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
128552	**Symptom:** A client that was connected to an AP lost connectivity for a short period of time on each day at the same time. This issue is resolved by resuming the normal operation when the client turns to active state from inactive state. **Scenario:** This issue was observed when a client was in hardware sleep mode and did not send a deauthentication request. This issue was observed in an OAW-AP215 access points running AOS-W 6.4.2.8.	AP-Platform	OAW-AP215 access points	AOS-W 6.4.2.8	AOS-W 6.5.0.0
128677	**Symptom:** An incorrect total number of access points was displayed in the WebUI under **WebUI > Monitoring**. This issue is resolved by calculating the total number of access points as the sum of wired AP and wireless AP and displaying the value in the WebUI. **Scenario:** This issue was observed in switches running AOS-W 6.3.1.15.	WebUI	All platforms	AOS-W 6.3.1.15	AOS-W 6.5.0.0
128800	**Symptom:** Guest users were not removed from the user table after the user idle timer value that was configured in the Captive Portal (CP) profile expired. This issue is resolved by ensuring that if **l3role** has **cp-profile**, then use it to get the idle timeout, else get the idle timeout from the **cp-profile** in **l2role**. **Scenario:** This issue occurred when the user idle timeout that was configured in the CP profile was not considered for guest users and the guest users were timed out after the global user idle timeout expired. This issue was observed in switches running AOS-W 6.4.3.4.	Base OS Security	All platforms	AOS-W 6.4.3.4	AOS-W 6.5.0.0
128916 132353 133884 138015	**Symptom:** Users were denied access by the switch and the **drop pkt as ip not assigned through dhcp** error message was displayed. The issue is fixed by enabling **enforce-dhcp**. **Scenario:** This issue occurred when the dhcp enforcement failed. This issue was observed in switches running AOS-W 6.3.1.16.	Switch-Datapath	All platforms	AOS-W 6.3.1.6	AOS-W 6.5.0.0

Table 5: *Resolved Issues in 6.5.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
128925	**Symptom:** The multicast DNS (**mDNS**) process crashed in a switch. The fix ensures that devices are not added to AirGroup when AirGroup is in disabled state. **Scenario:** This issue occurred when devices were added to an AirGroup device list and were not cleared as a global credit timer did not run when AirGroup was disabled. This resulted in exponential increase in memory usage in the **mDNS** process. This issue was observed in switches running AOS-W 6.4.2.6.	Switch-Platform	All platforms	AOS-W 6.4.2.6	AOS-W 6.5.0.0
128979	**Symptom:** An OAW-RAP109 access point rarely did not connect to the switch and could not recover by itself. The fix ensures that the remote access point (RAP) reboots and recovers even if the Wi-Fi Peripheral Component Interconnect (PCI) fails to initialize. **Scenario:** This issue occurred when the radio card was not detected and the RAP sent Hello request without the Wi-Fi1 MAC to the switch to which the switch could not respond. This issue was observed in OAW-RAP108 and OAW-RAP109 access points connected to switches running AOS-W 6.4.3.3 in a master-local topology.	AP-Platform	OAW-RAP108 and OAW-RAP109 access points	AOS-W 6.4.3.3	AOS-W 6.5.0.0
129043	**Symptom:** A switch rebooted. The log file for the event listed the reason as **datapath timeout**. This issue is resolved by adding AMSDU support for IPv6 access points and passing the fragments with forward opcode. **Scenario:** This issue occurred during reassembly of fragmented packets. This issue was observed in both master and local switches running AOS-W 6.4.3.4 in master-local topology.	Switch-Datapath	All platforms	AOS-W 6.4.3.4	AOS-W 6.5.0.0
129055 137138	**Symptom:** A switch stopped responding and rebooted unexpectedly. While collecting the crash logs, the switch crashed again and over-wrote the crash logs of the previous crash. This issue is resolved by removing the access to the device name for a given interrupt number in the crash path. **Scenario:** This issue occurred while collecting the crash logs in OAW-4650 switches running AOS-W 6.3.1.x, AOS-W 6.4.2.x, AOS-W 6.4.3.x, or AOS-W 6.4.4.x.	Switch-Platform	OAW-4650 switches	AOS-W 6.4.4.1	AOS-W 6.5.0.0

Table 5: *Resolved Issues in 6.5.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
129096	**Symptom:** The Lightweight Directory Access Protocol (LDAP) connection in a switch reset. The switch was unable to authenticate or query the users using the LDAP server. This issue is resolved by enabling the **chase-referrals** parameter in **LDAP-authentication--server-profile**. **Scenario:** This issue was observed when a search request from a switch to an LDAP server was redirected to another LDAP server that did not support anonymous queries. This issue was not limited to any specific switch model or AOS-W version.	LDAP	All platforms	AOS-W 6.4.2.12	AOS-W 6.5.0.0
129116 132900	**Symptom:** The AirGroup service configuration changed automatically on a standby switch after executing the **write memory** command on a master switch. This issue is resolved by restoring the status of AirGroup services after master-standby synchronization. **Scenario:** This issue occurred while synchronizing the configuration from a master switch to a standby switch. This issue was observed in switches running AOS-W 6.4.2.x, AOS-W 6.4.3.x, or 6.4.4.x in a master-local topology.	AirGroup	All platforms	AOS-W 6.4.2.13	AOS-W 6.5.0.0
129144	**Symptom:** Windows 10 clients running version 1511 were unable to connect to 802.1X SSID when termination was enabled on the switch. A workaround is added in the AOS-W code whereby the switch sends a HELLO message with TLS v1.0 when the Advanced Cryptography (ACR) license is not available in the switch for clients initiating a TLS v1.2 session. **Scenario:** AOS-W supports TLS v1.2 with Suite B which requires ACR license. Windows 10 clients with the new patch (OS Build 10586.3) seem to work with RSA certificates and TLS v1.2. This issue was observed in Windows 10 client with OS Build 10586.3 and switches running AOS-W 6.3.x or AOS-W 6.4.x.	RADIUS	All platforms	AOS-W 6.3.1.18	AOS-W 6.5.0.0
129223	**Symptom:** Clients failed to discover Amazon Fire TV even when AirGroup service was enabled in the switch. This issue is resolved by adding the Amazon Fire TV as part of the AirGroup services. **Scenario:** This issue occurred because the service ID was not listed under the AirGroup service in the switch. This issue was observed with Amazon Fire TV and switches running AOS-W 6.4.x.	AirGroup	All platforms	AOS-W 6.4.3.2	AOS-W 6.5.0.0

Table 5: *Resolved Issues in 6.5.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
129439 129652	**Symptom:** Duplicate subrecords were added under the allowall service for subrecord response packet. This issue is resolved by removing the sub part when adding the service ID under the allowall service. **Scenario:** This issue was observed in switches running AOS-W 6.4.4.3.	AirGroup	All platforms	AOS-W 6.4.4.3	AOS-W 6.5.0.0
129464	**Symptom:** Clients took long time to connect after High Availability (HA) failover. The log file for the event listed the reason as **Station Up Message to Controller Timed Out**. This issue is resolved by cleaning the deferred deauthentication list. **Scenario:** This issue occurred when the acknowledgment for the station up message arrived after the message list was moved to the deferred deauthentication list and the station up message was not processed normally. This issue was observed in switches running AOS-W 6.4.3.2.	AP-Wireless	All platforms	AOS-W 6.4.3.2	AOS-W 6.5.0.0
129535 134047	**Symptom:** Access points do not receive LLDP packets from LAN ports. This issue is resolved by adding the BRCM header before the Ethernet header. **Scenario:** This issue occurred because the BRCM header was positioned after the Ethernet header when the access points received the LLDP packets from the LAN ports of a switch. Hence, the access points dropped the LLDP packets. This issue was observed in access points connected to switches running AOS-W 6.4.3.x, AOS-W 6.4.4.x, or AOS-W 6.5.0.0.	AP-Platform	All platforms	AOS-W 6.4.3.3	AOS-W 6.5.0.0
129646	**Symptom:** Unsolicited mDNS response was not sent correctly across switches when the shared user list on the AirGroup server was modified in ClearPass Policy Manager (CPPM) policy. The fix ensures that the unsolicited mDNS response was sent correctly. **Scenario:** This issue was observed in switches running AOS-W 6.4.4.1.	AirGroup	All platforms	AOS-W 6.4.4.1	AOS-W 6.5.0.0

Table 5: *Resolved Issues in 6.5.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
129649	**Symptom:** When the AirGroup **allowall** service was enabled, wildcard queries were sent for subservices that were learnt by the **allowall** service. The fix ensures that wildcard queries are not sent for subservices that are learnt by the **allowall** service. **Scenario:** This issue was observed in switches running AOS-W 6.4.3.x or AOS-W 6.4.4.x.	AirGroup	All platforms	AOS-W 6.4.4.3	AOS-W 6.5.0.0
129698 132761	**Symptom:** A client experienced a one-way VoIP communication. The fix ensures that the SIP ALG uses the right datapath opcode to send the SIP 486 message so that the route cache entry for the client remains intact. **Scenario:** This issue was seen under the following circumstances: ● Call Admission Control (CAC) was enabled. ● The switch blocked the SIP-based call due to CAC. ● On clearing the CAC limitation, when a subsequent SIP-based call was made to or from the client, the switch dropped all RTP and RTCP packets to this client. This issue was seen because the route cache entry for the client was modified when SIP ALG sent a SIP 486 message to the client for blocking the call. This lead the switch to detect an IP spoofing because the route cache entry for the client indicated the wrong MAC address. This issue was observed in switches running AOS-W 6.4.x.	UCC	All platforms	AOS-W 6.4.2.5	AOS-W 6.5.0.0
130113 131652 131653	**Symptom:** RTP/RTCP packets were not prioritized in a Jabber voice conference call. This issue is resolved by adding a new IP address parameter in the media block to handle the video parameters. **Scenario:** This issue occurred when the connection details were overwritten because the IP address was common for different connections. This issue was observed in switches running AOS-W 6.5.0.0.	UCC	All platforms	AOS-W 6.5.0.0	AOS-W 6.5.0.0
130290	**Symptom:** The multicast DNS (**mDNS**) process crashed in a switch. This issue is resolved by allocating new memory instead of using the freed up memory. **Scenario:** This issue occurred when subrecord responses were sent for the **allowall** service. This issue was observed in switches running AOS-W 6.4.3.6.	AirGroup	All platforms	AOS-W 6.4.3.6	AOS-W 6.5.0.0

Table 5: *Resolved Issues in 6.5.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
130611	**Symptom:** An administrator failed to configure the **no spanning-tree** command for a port-channel. The fix ensures that the command can be set for a port-channel. **Scenario:** This issue was seen when the port-channel was changed to a trunk mode. This issue was observed in switches running AOS-W 6.4.4.x.	Port-Channel	All platforms	AOS-W 6.4.4.0	AOS-W 6.5.0.0
130917 136646 140035 142742	**Symptom:** When the **show running config** command was executed on the switch, the **Module AMAPI SNMP trap client is busy. Please try later** error message was displayed. The fix ensures that this error message is not displayed. **Scenario:** This issue occurred when bulk SNMP queries were executed on a switch. This issue was observed in switches running AOS-W 6.4.2.x, AOS-W 6.4.3.x, or AOS-W 6.4.4.x.	SNMP	All platforms	AOS-W 6.4.3.5	AOS-W 6.5.0.0
130965	**Symptom:** The switch WebUI defaulted the ACL queue priority value to **Low** even though it was set to **High**. However, the switch accepted the correct value when configured from the CLI. The fix ensures that the switch applies the queue priority correctly for an ACL when configured from the WebUI. **Scenario:** This issue occurred only when the queue priority for an ACL was set to **High** from the WebUI. This issue was observed in switches running AOS-W 6.4.2.3 or later versions.	WebUI	All platforms	AOS-W 6.4.2.3	AOS-W 6.5.0.0
130981	**Symptom:** A switch rebooted. The log file for the event listed the reason as **datapath timeout**. This issue is resolved by not parsing special characters. **Scenario:** This issue occurred when a **copy** command with \\ characters at the end of a command was executed. This issue was observed in switches running AOS-W 6.4.4.0.	Switch-Platform	All platforms	AOS-W 6.4.4.0	AOS-W 6.5.0.0
130983	**Symptom:** The Policy Based Routing (PBR) configuration in a standby switch was not retained after saving the configuration in a master switch. This issue is resolved by storing router ACL policies in a local table and not purging it during configuration push from the master switch. **Scenario:** This issue was observed in standby switches running AOS-W 6.4.4.1 in master-standby topology.	Switch-Datapath	All platforms	AOS-W 6.4.4.1	AOS-W 6.5.0.0

Table 5: *Resolved Issues in 6.5.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
131104 137024	**Symptom:** An incorrect AP interference statistic that was sent from a switch to an AP led to gaps in the channel utilization graph in OV3600. This issue is resolved by limiting the interference value of an AP in the range of 0-100. **Scenario:** This issue was observed in an OAW-AP135 access points running AOS-W 6.4.2.x, AOS-W 6.4.3.x, or AOS-W 6.4.4.x.	AP-Wireless	OAW-AP135 access points	AOS-W 6.3.1.5	AOS-W 6.5.0.0
131316	**Symptom:** A switch displayed the **AMP Alert - syslog: bad option at line 14 of /etc/dnsmasq.conf** error message. This issue is resolved by upgrading the dnsmasq to version 2.75. **Scenario:** This issue was observed in switches running AOS-W 6.4.2.12 in a master-standby topology.	Logging	All platforms	AOS-W 6.4.2.12	AOS-W 6.5.0.0
131401	**Symptom:** The **RC_ERROR_PEER_DELETE_SA** error message was displayed even for successful IKE negotiations. The fix ensures that the error is not displayed for successful negotiations. **Scenario:** This issue was observed in switches running AOS-W6.4.2.6.	Base OS Security	All platforms	AOS-W 6.4.2.6	AOS-W 6.5.0.0
131445	**Symptom:** When roaming using 802.11r fast handoff, a client got an IP address from a Virtual Local Area Network (VLAN) mapped in the Virtual Access Point (VAP) profile although it was supposed to get an IP address from a VLAN derived from Vendor Specified Attribute (VSA). This issue is resolved by updating the station management about the derived VLAN and avoiding key exchange when station management acknowledges the VLAN update. **Scenario:** This issue was observed in an 802.1X authenticated client when it roamed using 802.11r fast handoff. This issue was observed in switches running AOS-W 6.3.x or AOS-W 6.4.x.	Base OS Security	All platforms	AOS-W 6.4.3.4	AOS-W 6.5.0.0
131857	**Symptom:** The Type of Service (TOS) value of **0** did not take effect when it was set in the user-role. The fix ensures that the TOS value configured in the ACL takes effect. **Scenario:** This issue was observed in switches running AOS-W 6.4.3.3.	Switch-Datapath	All platforms	AOS-W 6.4.3.3	AOS-W 6.5.0.0

Table 5: *Resolved Issues in 6.5.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
131874 132843 133107	**Symptom:** The **Monitoring** page in the WebUI displayed incorrect count of active clients when searched with filters like ESSID. Additionally, the **show ipv4 user-table rows <starting-row-number> <number-of-rows>** command displayed more records than the pagination count. This issue is resolved by applying filters before selecting the rows on the filtered list. **Scenario:** This issue occurred because the rows were selected before the filters were applied on the user entries. This issue was observed in switches running AOS-W 6.4.2.14 or later versions.	WebUI	All platforms	AOS-W 6.4.2.14	AOS-W 6.5.0.0
131921 137958 138552 138581 138914 140744	**Symptom:** An AP rebooted unexpectedly. The log file for the event listed the reason as **memory corruption 0xAA**. The fix ensures that the AP does not reboot unexpectedly. **Scenario:** This issue was observed in OAW-AP325 access points running AOS-W 6.4.4.4.	AP-Platform	OAW-AP325 access points	AOS-W 6.4.4.4	AOS-W 6.5.0.0
131971 133165	**Symptom:** Wireless clients did not get IP address in DHCP-based derived VLAN and DHCP options based VLAN assignment did not work as expected. This issue is resolved by using station keys. **Scenario:** This issue occurred because of key mismatch in DHCP options based VLAN derivation. This issue was observed in switches running AOS-W 6.4.3.4.	Role/VLAN Derivation	All platforms	AOS-W 6.4.3.4	AOS-W 6.5.0.0
132148	**Symptom:** OAW-AP325 access points rebooted. The log files for the event listed the reason as **MSM HSL wait_for_xmitr is stuck**. This issue is resolved by resetting the UART and resuming the console. **Scenario:** This issue occurred because the UART was stuck. This issue was observed in OAW-AP325 access points connected to switches running AOS-W 6.4.4.2.	AP Datapath	OAW-AP325 access points	AOS-W 6.4.4.2	AOS-W 6.5.0.0

Table 5: *Resolved Issues in 6.5.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
132382	**Symptom:** Users could not add a user name with ' character (apostrophe) in the RAP whitelist database using the WebUI. The fix ensures that users can add user name with ' character (apostrophe). **Scenario:** This issue occurred because of a previous entry that was enclosed in ' character (apostrophe). This issue was observed in master switches running AOS-W 6.4.2.x in a master-standby topology.	WebUI	All platforms	AOS-W 6.4.2.3	AOS-W 6.5.0.0
132714	**Symptom:** An administrator failed to add a static ARP entry on the switch and the switch displayed the **Cannot add static ARP entry** message. The log files of the event listed the reason as **Static ARP: too many entries (ipMapArpStaticEntryAdd)**. This issue is resolved by not incrementing the static ARP counters for existing ARP entries when there is a change in the link status. **Scenario:** The static ARP counter continued to increment every time there was a change in the link status. This issue was observed in switches running AOS-W 6.4.3.4.	Switch-Platform	All platforms	AOS-W 6.4.3.4	AOS-W 6.5.0.0
132814	**Symptom:** An AP rebooted unexpectedly. The log file for the event listed the reason as **reboot reason: Reboot caused by kernel panic**. The fix ensures that the AP does not reboot unexpectedly without generating a crash information file. **Scenario:** This issue was observed in OAW-AP210 Series, OAW-AP220 Series, AP-228, or OAW-AP270 Series access points connected to switches running AOS-W 6.4.2.6.	AP-Wireless	OAW-AP210 Series, OAW-AP220 Series, AP-228, and OAW-AP270 Series access points	AOS-W 6.4.2.6	AOS-W 6.5.0.0
132838	**Symptom:** When using the search option in the WebUI, the pagination was incorrect and a user could not navigate to other pages. This issue is resolved by resetting the pagination counter to 0 when changing the filter **All**, **IPV4**, and **IPV6**. **Scenario:** This issue was observed in switches running AOS-W 6.4.4.3.	WebUI	All platforms	AOS-W 6.4.4.3	AOS-W 6.5.0.0

Table 5: *Resolved Issues in 6.5.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
132914	**Symptom:** A switch allowed the CLI option to configure qos-profile for user-role. This issue is resolved by removing the CLI option to configure the qos-profile for the user-role. **Scenario:** This issue was observed in switches running AOS-W 6.4.3.5.	Base OS Security	All platforms	AOS-W 6.4.3.5	AOS-W 6.5.0.0
133140	**Symptom:** OAW-AP205H access points did not complete 802.1X authentication when connected directly to a switch. This issue is resolved by configuring a rule in ARL to allow the EAPOL frames in OAW-AP205H access points. **Scenario:** This issue occurred because the OAW-AP205Haccess points dropped the EAPOL frames. This issue was observed whenOAW-AP205H access points were directly connected to untrusted ports of a switch running AOS-W 6.4.3.6 over an Ethernet cable.	AP-Platform	OAW-AP205H access points	AOS-W 6.4.3.6	AOS-W 6.5.0.0
133266	**Symptom:** A local switch rebooted unexpectedly. The log file for the event listed the reason as **Reboot Cause: Datapath timeout (Intent:cause:register 56:86:50:2)**. The fix ensures that a switch does not reboot unexpectedly. **Scenario:** This issue occurred because of memory corruption. This issue is observed in OAW-4650 switches running AOS-W 6.4.3.6.	Switch-Datapath	OAW-4650 switches	AOS-W 6.4.3.6	AOS-W 6.5.0.0
133366 139845	**Symptom:** The **station management** process frequently logged messages about tracing being on. The trace files were rotated and these logs could not be turned off through the logging level configuration. The fix ensures that logging level configuration is applied to these logs messages. **Scenario:** This issue was observed in access points that were logging station management trace-related log messages. This issue was observed in switches running AOS-W 6.4.3.5.	Station Management	All platforms	AOS-W 6.4.3.5	AOS-W 6.5.0.0

Table 5: *Resolved Issues in 6.5.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
133442	**Symptom:** The RAP's inner pool Layer 2 Protocol Tunneling (L2PT) traffic displayed clear-text traffic on the switch uplink with aged out sessions. The fix ensures that the switch is marked as DOWN until the WLAN Management Suite (WMS) acknowledges the inner IP change and updates its IP address to the inner IP of the RAP. **Scenario:** When RAPs rebootstrapped, the inner IP address of the RAP changed, but the WMS app was not updated immediately. The WMS was only updated during the next AP periodic update session. However, WMS did not acknowledge the periodic update as the IP address in the WMS was incorrect and so the AP sent a probe_ register that updated the IP address at the WMS. During this time, when the WMS had the incorrect inner IP of the RAP, if it sent a message to the AP, the message did not go through the IPsec tunnel. This issue was observed in switches running AOS-W 6.4.2.6.	Air Management - IDS	All platforms	AOS-W 6.4.2.6	AOS-W 6.5.0.0
133448	**Symptom:** IPsec association failed when IP NAT was configured outside on a branch switch. This issue is resolved by adding checks for destination port. **Scenario:** This issue occurred when IP NAT outside was applied to VLAN 4094 on a branch switch. A datapath session was created with a source network address translation rule and the IKE packets were source network address translated. As part of the network address translation, the source port in IKE packet was changed from 4500 to a different value and when route lookup was performed, the packet was not recognized as an IKE packet and the packet was not sent. This issue was observed in switches running AOS-W 6.4.3.2.	Switch-Datapath	All platforms	AOS-W 6.4.3.2	AOS-W 6.5.0.0
133562 133565 133566 133569 134162	**Symptom:** An Access Point (AP) crashed and rebooted unexpectedly. This issue is resolved by not copying the Virtual Memory Area (VMA) of the parent process. **Scenario:** This issue occurred when a child process was released. This issue was observed in an OAW-AP124 AP running AOS-W 6.4.4.3.	AP-Platform	OAW-AP124 access points	AOS-W 6.4.4.3	AOS-W 6.5.0.0

Table 5: *Resolved Issues in 6.5.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
133564	**Symptom:** An Access Point (AP) rebooted. The log files for the event listed the reason as **Reboot caused by kernel page fault at virtual address 0000000100000007, epc == ffffffff80268c20, ra == ffffffff80268ba8**. This issue is resolved by allocating memory pages from the cache and marking them as reserved. **Scenario:** This issue occurred because the memory pages were allocated from the freelist for polling. This issue is observed in OAW-AP135 and OAW-AP220 Series access points running AOS-W 6.4.4.3.	AP-Platform	OAW-AP135 and OAW-AP220 Series access points	AOS-W 6.4.4.3	AOS-W 6.5.0.0
133667 134471 135526	**Symptom:** Clients with Realtek chips experienced low throughput when the **g radio basic rates** or **g tx rates** included 802.11b rate. This issue is resolved by removing the ACK timeout configuration and using the default value in the wireless driver. **Scenario:** This issue occurred because a small ACK timeout value allowed an AP to ignore the Binding Acknowledgment (BA) message sent by a client with Realtek chip. This issue was observed in access points running AOS-W 6.4.4.3.	AP-Wireless	All platforms	AOS-W 6.4.4.3	AOS-W 6.5.0.0

Table 5: *Resolved Issues in 6.5.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
134147	**Symptom:** AirGroup did not send response for mDNS query. This issue is resolved by: ● Performing a full configuration synchronization without changing any state when there is no change in AirGroup. ● Retaining the status of services in the local switches when the AirGroup service is disabled in the master switch. ● Flushing the cache built for the service ID when a service ID is deleted. ● Adding a service ID and discovering the servers when a service ID is added. ● Not allowing the deletion of the default service ID on a master switch. ● Flushing the cache built for all service IDs under a service when a non-default service is deleted. ● Not adding the static service ID to the local switches when a static service ID is added to a master switch as part of static record configuration. ● Not adding the service ID to the local switches when a service ID is added to the master or backup switch as part of the allowall service. ● Synchronizing the disable enforce-registration to local switches. ● Synchronizing the changes to the CPPM server query interval to the local switches. **Scenario:** This issue was observed in switches running AOS-W 6.4.2.15.	AirGroup	All platforms	AOS-W 6.4.2.15	AOS-W 6.5.0.0

Table 5: *Resolved Issues in 6.5.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
134279	**Symptom:** The eth1 port of an OAW-AP225 access point displayed the link status as **UP** although the link status was **DOWN**. The fix ensures that the switch displays the correct physical link status of the AP. **Scenario:** This issue was observed under the following circumstances: OAW-AP225 detects POE+ power. On detecting POE+ power, the eth1 port on the AP is enabled with full functionality. The switch sends LLDP POE with 13.0W power. As the power is less, the periodic timer shuts the eth1 port on the AP. But the **show ap debug system-status** command displayed the link status as **UP** although the link status was **DOWN**. This issue was observed in OAW-AP225 access point running AOS-W 6.4.3.x or AOS-W 6.4.4.x.	AP-Platform	OAW-AP225 access points	AOS-W 6.4.3.5	AOS-W 6.5.0.0
134479	**Symptom:** A RAP rebooted continuously when a 340U USB modem was plugged into it. The RAP was provisioned with the 340U USB modem parameters. This issue is fixed by changing the USB driver. **Scenario:** This issue was observed in all remote access points supporting AT&T 340U USB modems. This issue was observed in switches running AOS-W 6.4.3.7.	Remote Access Point	All platforms	AOS-W 6.4.3.7	AOS-W 6.5.0.0
134507	**Symptom:** The call count remained even after a Session Initiation Protocol (SIP) session was terminated by a BYE request. This issue is resolved by not decrementing the call count if it is already 0. **Symptom:** This issue occurred when mobile IP was configured, a client roamed from a Home Agent to a Foreign Agent, received a SIP call while in Foreign Agent, and returned to the Home Agent. This issue was observed in switches running AOS-W 6.4.3.1.	Unified Communication and Collaboration	All platforms	AOS-W 6.4.3.1	AOS-W 6.5.0.0

Table 5: *Resolved Issues in 6.5.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
134534	**Symptom:** Real-time Transport Protocol (RTP) was sent to the wrong VLAN when a VOIP client roamed to Foreign Agent (FA) during an active session. This issue is resolved by redirecting packets from Home Agent (HA) to FA if an L3 user entry for the roamed user is not available at the FA. **Scenario:** This issue occurred when a VOIP client roamed from HA to FA and session entries were created without a redirect flag. This issue was observed in switches running AOS-W 6.4.3.1.	Mobility	All platforms	AOS-W 6.4.3.1	AOS-W 6.5.0.0
134646	**Symptom:** An **accounting-stop** message with wrong values was sent when posting XML user-add to a switch. The fix ensures that the **accounting-stop** on xml user-add has correct values. **Scenario:** This issue was observed when user-add is posted to an authenticated Captive Portal user. The **accounting-stop** contained all zeroes and the framed IP address is 0.0.0.0. This issue was observed in switches running AOS-W 6.4.2.12.	XML API	All platforms	AOS-W 6.4.2.12	AOS-W 6.5.0.0
134677	**Symptom:** When the user deleted an Access Control List (ACL) with attributes similar to the **Time Ranges** ACL, the ACL listed under the **Time Ranges** tab was also deleted. This issue is resolved by making code changes that restrict the generation of the **delete** command for ACLs that have attributes similar to the **Time Range** ACLs. **Scenario:** This issue was observed only when the ACL was deleted using the GUI. This issue was observed in switches running AOS-W 6.4.2.5.	WebUI	All platforms	AOS-W 6.4.2.5	AOS-W 6.5.0.0
134678	**Symptom:** High Throughput (HT) and Very High Throughout (VHT) capable clients failed to connect at HT and VHT rates. Improvements in the AP wireless driver ensure that HT and VHT capable clients connect at HT and VHT rates. **Scenario:** This issue occurred after a VRRP failover. This issue was observed in 802.11ac-capable access points connected to switches running AOS-W 6.4.2.15, AOS-W 6.4.3.x, or AOS-W 6.4.4.x.	AP-Wireless	OAW-AP200 Series, OAW-AP210 Series, and OAW-AP270 Series access points	AOS-W 6.4.2.15	AOS-W 6.5.0.0

Table 5: *Resolved Issues in 6.5.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
134723	**Symptom:** A wired client did not complete wired EAP authentication in bridge mode with an OAW-AP205H Access Point (AP). This issue is resolved by forwarding the packets to an internal port. **Scenario:** This issue occurred because an AP dropped the undersized EAPOL frames. This issue was observed in an OAW-AP205H AP running AOS-W 6.4.3.6.	AP-Platform	OAW-AP205H access points	AOS-W 6.4.3.6	AOS-W 6.5.0.0
134782 138446 138457 138513 138519 138536 138540 138542 138586	**Symptom:** An AP crashed unexpectedly. The log file for the event listed the reason as **activate_page+0x68/0x108**. This issue is resolved by preventing access to a memory page that is not on the inactive list. **Scenario:** This issue was observed in OAW-AP325 access points running AOS-W 6.4.4.4.	AP-Platform	OAW-AP325 access points	AOS-W 6.4.4.4	AOS-W 6.5.0.0
134789	**Symptom:** When the user selected an AP listed in the **Monitoring > Network > All Access Points** page, information related to multiple APs was displayed although only one AP was selected. This issue is resolved by making code level changes to the filter, so that only the AP queried for is fetched instead of fetching similar APs. **Scenario:** This issue was observed in access points connected to switches running AOS-W 6.4.3.4.	WebUI	All platforms	AOS-W 6.4.3.4	AOS-W 6.5.0.0
134884	**Symptom:** A difference in **AP Uptime** was observed when the AP was monitored from the **Dashboard > Access Points** and when the **show ap active ap-name** was executed. This issue is resolved by making code level changes to modify the up time in seconds to time-range conversion logic. **Scenario:** This issue was observed in OAW-4x50 Series switches running AOS-W 6.4.2.14.	WebUI	OAW-4x50 Series switches	AOS-W 6.4.2.14	AOS-W 6.5.0.0

Table 5: *Resolved Issues in 6.5.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
135029	**Symptom:** The **Monitoring > NETWORK > All Access Points** page of the WebUI displayed an incorrect user count. The fix ensures that the switch displays the correct user count in the WebUI. **Scenario:** There was a mismatch in the user count when seen in the **Monitoring** and **Dashboard** page of the WebUI. This issue was not seen in the CLI. This issue was observed in switches running AOS-W 6.4.2.12, AOS-W 6.4.3.x, or AOS-W 6.4.4.x.	WebUI	All platforms	AOS-W 6.4.2.12	AOS-W 6.5.0.0
135089	**Symptom:** Access points rebooted and the log files for the event listed the reason **Reboot caused by kernel panic: Fatal exception**. This issue is resolved by making internal code changes to prevent the kernel panic to re-occur. **Scenario:** This issue was observed in switches connected to OAW-AP325 access points running AOS-W 6.4.4.4.	AP-Platforms	OAW-AP324/OAW-AP325 access points	AOS-W 6.4.4.4	AOS-W 6.5.0.0
135090	**Symptom:** A client received a malformed Reset (RST) from a switch. This issue is resolved by adding the missing byte to the Transmission Control Protocol (TCP) RST. **Scenario:** This issue occurred when an Access Control Entry (ACE) in an Access Control List (ACL) was configured with send-deny-response and the switch responded to a client with an RST after dropping a matching packet. But the client received a malformed RST because of a missing byte in the RST response sent by the switch. This issue was observed in switches running AOS-W 6.4.2.3.	Switch-Datapath	All platforms	AOS-W 6.4.2.3	AOS-W 6.5.0.0
135097	**Symptom:** A switch rebooted unexpectedly. The log file for the event listed the reason as Datapath timeout **(Intent:cause:register 56:86:50:2)**. This issue is resolved by avoiding a race condition in aging sessions. **Scenario:** This issue occurred because of a race condition in aging session when a session had type 2 contract. This issue was observed in OAW-4650 switches running AOS-W 6.4.3.6.	Switch-Datapath	OAW-4650 switches	AOS-W 6.4.3.6	AOS-W 6.5.0.0

Table 5: *Resolved Issues in 6.5.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
135121	**Symptom:** A switch crashed and rebooted. The log file for the event listed the reason as **Datapath timeout (Intent:cause:register 56:86:50:2)**. This issue is resolved by enhancing the IPv6 firewall to drop packets with wrong application payload. **Scenario:** This issue occurred when unnecessary padding between the IPv6 and TCP header created wrong application payload. This issue was observed in switches running AOS-W 6.4.4.3.	Switch-Platform	All platforms	AOS-W 6.4.4.3	AOS-W 6.5.0.0
135131	**Symptom:** Clients randomly failed to send or receive traffic when associated to an SSID. This issue is resolved by eliminating a memory leak in the **authentication** process. **Scenario:** On further investigation, it was observed that the **authentication** process stopped responding due to an out of memory situation. This issue was observed in switches running AOS-W 6.4.4.4.	Base OS Security	All platforms	AOS-W 6.4.4.4	AOS-W 6.5.0.0
135132	**Symptom:** An OAW-AP105 access point stopped responding and rebooted. The fix ensures that the AP functions as expected. **Scenario:** This issue occurred when spectrum monitoring was enabled on the AP. When the AP radio changes from spectrum mode to normal mode on the home channel, it may experience a phenomenon called a stuck beacon. Stuck beacon is a driver-level error indicating that the chipset failed to complete a Tx function. This issue was observed in OAW-AP100 Series access points running AOS-W 6.4.3.6 or later versions.	AP-Wireless	OAW-AP100 Series access points	AOS-W 6.4.3.6	AOS-W 6.5.0.0
135284 137416	**Symptom:** The Signal to Noise Ratio (SNR) and RSSI columns in the output of the **show ap monitor ap-list** command displayed **0**. This issue is resolved by displaying the correct SNR and RSSI values in the output of the **show ap monitor ap-list** command. **Scenario:** This issue was observed in OAW-AP220 Series access points running AOS-W 6.4.4.0.	Air Management-IDS	OAW-AP220 Series access points	AOS-W 6.4.4.0	AOS-W 6.5.0.0

Table 5: *Resolved Issues in 6.5.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
135290	**Symptom:** The ARM history entries showed that a RADAR-contaminated channel was used within the non-occupancy period (30 minutes). This issue is resolved by adding a channel to the candidate list of channels only if it is not contaminated. **Scenario:** This issue occurred because a random channel was selected from a candidate list of channels without verifying if that channel was already under RADAR detection. This issue was observed in an OAW-AP274 access points running AOS-W 6.4.4.0.	AP-Wireless	OAW-AP274 access points	AOS-W 6.4.4.0	AOS-W 6.5.0.0
135411	**Symptom:** Some access points did not send frames in the 2.4 GHz channel. This issue is resolved by restoring timers with enable mask. **Scenario:** This issue occurred when quiet timers were enabled and a firmware cold reset was performed. The firmware restored the timer enable mask without restoring the next start time and period. Hence, the quiet timers were stuck. This issue was observed in access points connected to switches running AOS-W 6.4.4.x or AOS-W 6.5.0.0.	AP-Wireless	OAW-AP320 Series access points	AOS-W 6.4.4.4	AOS-W 6.5.0.0
135569	**Symptom:** An AP crashed and the log files listed the reason for the event as **Kernel panic - not syncing: Fatal exception in interrupt**. This issue is resolved by clearing the page index after removing the page index from page cache. **Scenario:** This issue was observed in OAW-AP135 access points connected to switches running AOS-W 6.4.4.4.	AP-Wireless	OAW-AP135 access points	AOS-W6.4.4.4	AOS-W 6.5.0.0
135678	**Symptom:** A switch randomly dropped **SIP INVITE** messages due to which users were unable to resume a Session Initiation Protocol (SIP) call which was placed on hold. This issue is resolved by sending the SIP signaling packets back to datapath after they are processed, irrespective of whether the processing succeeded or failed. **Scenario:** This issue occurred when SIP ALG failed due to which a switch dropped the subsequent SIP INVITE messages. This issue was observed in switches running AOS-W 6.4.3.x or AOS-W 6.4.4.x.	Unified Communication and Collaboration	All platforms	AOS-W 6.4.4.4	AOS-W 6.5.0.0

Table 5: *Resolved Issues in 6.5.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
135742	**Symptom:** The **authentication** process crashed in a local switch. The fix ensures that the **authentication** process does not crash. **Scenario:** This issue occurred because of a mismatch in the reference count of netdestination6 and more entries were added to netdestination6 alias. This issue was observed in switches AOS-W 6.4.2.x, AOS-W 6.4.3.x, or AOS-W 6.4.4.x.	Base OS Security	All platforms	AOS-W 6.4.2.14	AOS-W 6.5.0.0
135841	**Symptom:** A discrepancy in the month was observed when the user viewed the clock through the WebUI and the CLI. This issue is resolved by making code level changes to remove the addition of a month while retrieving data from the **show clock** command. **Scenario:** When the user navigated to **Monitoring > Controller > Uplink > Uplink Management** and **Monitoring > Controller > Universal Serial Bus > USB Devices** pages, the date displayed in the clock was a month ahead of what was displayed when the **show clock** command was executed in the CLI. This issue was observed in OAW-40xx Series switches running AOS-W 6.4.3.6.	WebUI	OAW-40xx Series	AOS-W 6.4.3.6	AOS-W 6.5.0.0
135855	**Symptom:** Authentication module crashed while updating netdestination on a switch. This issue is resolved by handling the netdestination update properly for app-based policies. **Scenario:** This issue was observed when the authentication module attempted to update the netdestination on the web-cc reference in the session ACL policy. This issue was observed in switches running AOS-W 6.4.2.12.	Base OS Security	All platforms	AOS-W 6.4.2.12	AOS-W 6.5.0.0
135862 141814	**Symptom:** After configuring the Maximum Transmission Unit (MTU) in **ap system-profile**, the **show ap bss-table** command displayed an incorrect MTU value. This issue is resolved by resending the MTU update message to a switch within 60 seconds if **switch_mtu** value is not equal to **gre_mtu** value and by setting **mtuhbt_pending** to null in the MTU discovery stop function. **Scenario:** This issue was observed when MTU update message wlost. This issue was observed in OAW-AP135 and OAW-AP225 access points running AOS-W 6.3.x.	AP-Datapath	OAW-AP135 and OAW-AP225 access points	AOS-W 6.3.1.9	AOS-W 6.5.0.0

Table 5: *Resolved Issues in 6.5.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
135949	**Symptom:** Bridge users were unable to pass traffic. The fix ensures that the bridge users are able to pass traffic. **Scenario:** This issue was observed when a vast number of users connected to d-tunnel VAP, then disconnected and the AP added L2 user entry for these d-tunnel user. The AP did not delete L2 user entry when the d-tunnel client was disconnected, which resulted in the user entry reaching the threshold. Therefore, when the client tried to connect to bridge VAP, the AP was unable to create user entry for bridge user. This issue was observed in switches running AOS-W 6.4.3.6.	AP-Datapath	All platforms	AOS-W 6.4.3.6	AOS-W 6.5.0.0
135959	**Symptom:** When **ip nat outside** command was executed the Smart Config was not pushed from the Master switch to the Branch switch. This issue is resolved by adding a check to restrict the execution of the **no ip ospf area** command for the specified vlan. **Scenario:** This issue was observed in OAW-40xx Series switches running AOS-W 6.4.4.4.	WebUI	OAW-40xx Series switches	AOS-W 6.4.4.4	AOS-W 6.5.0.0
136276	**Symptom:** The output of Very High Throughput (VHT) rates were similar when the **show ap ht-rates** and **show ap vht-rates** commands were executed. This issue is resolved by adding a check that ensures 80 MHz and 160 MHz columns are created only if VHT rates are requested. The Modulation and Coding (MCS) index displayed an incorrect value when the VHT-capable BSSID was added to the **show ap ht-rates** command. If the rate request is for ht-type, the fix ensures that the corresponding index for HT rates is printed. **Scenario:** This issue was observed in OAW-4x50 Series switches running AOS-W 6.4.4.4.	AP-Platform	OAW-4x50 Series switches	AOS-W 6.4.4.4	AOS-W 6.5.0.0
136349	**Symptom:** A switch sent the IP address in the port field and 0.0.0.0 as the remote address, resulting in security warnings. The fix ensures that a switch sends the same IP address in remote address field. **Scenario:** This issue was observed when TACACS+ accounting was enabled for command execution and the user logged in using Secure Shell (SSH). The authorization process sent the IP address in the port field and 0.0.0.0 as the remote address. This issue was observed in switches running AOS-W 6.4.3.6.	TACACS	All platforms	AOS-W 6.4.3.6	AOS-W 6.5.0.0

Table 5: *Resolved Issues in 6.5.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
136444	**Symptom:** Network Time Protocol (NTP) authentication keys when configured were not synchronizing from the master switch to the standby switch. The fix ensures that the configuration information is synchronized to the standby switch. **Scenario:** This issue was observed as the NTP authentication was enabled but the NTP authentication keys failed to synchronize with the standby switch. This issue was observed in switches running AOS-W 6.4.3.5.	Configuration	All platforms	AOS-W 6.4.3.5	AOS-W 6.5.0.0
136501	**Symptom:** A switch crashed unexpectedly. The log file for the event listed the reason as **Datapath timeout (Intent:cause:register 56:86:50:2)**. The fix ensures that a switch does not crash unexpectedly. **Scenario:** This issue occurred because of memory corruption. This issue is observed in switches running AOS-W 6.4.3.4.	Base OS Security	All platforms	AOS-W 6.4.3.4	AOS-W 6.5.0.0
136672 139929 142307	**Symptom:** An AP failed to come up when it was connected with a 4-wire Ethernet cable to a switch. This issue is resolved by ignoring the advised ability bit. **Scenario:** This issue occurred because the **sapd** process missed the advised ability bit. This issue was observed in OAW-AP105 access points running AOS-W 6.4.4.3.	AP-Platforms	OAW-AP105 access points	AOS-W 6.4.4.3	AOS-W 6.5.0.0
136724	**Symptom:** The **wlanAPRadioTransmitPower** decimal part was getting truncated when it was a floating value. This issue is resolved by representing **wlanAPRadioTransmitPower** multiplied by 2. **Scenario:** This issue was observed in switches running AOS-W 6.4.4.6.	Station Management	All platforms	AOS-W 6.4.4.6	AOS-W 6.5.0.0
136851	**Symptom:** An AP crashed and rebooted unexpectedly. The log file for the event listed the reason as **kernel panic: Fatal exception**. The fix ensures that an AP does not access wrong memory or reboot. **Scenario:** This issue occurred because of wrong memory access. This issue was observed in OAW-AP210 Series, OAW-AP220 Series, OAW-AP277, or OAW-AP320 Series access points running AOS-W 6.4.3.5.	AP-Platform	OAW-AP210 Series, OAW-AP220 Series, OAW-AP277, and OAW-AP320 Series access points	AOS-W 6.4.3.5	AOS-W 6.5.0.0

Table 5: *Resolved Issues in 6.5.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
137196	**Symptom:** A switch failed to respond and rebooted. The log file listed the reason for this event as **Reboot Cause: Datapath timeout**. This issue is resolved by adding sanity checks to avoid race conditions. **Scenario:** This issue occurred when Virtual Internet Access (AOS-W VIA) was used with Secure Socket Layer (SSL) fallback. This issue was not limited to any specific switch model or AOS-W release version.	Base OS Security	All platforms	AOS-W 6.4.0.3	AOS-W 6.5.0.0
137549	**Symptom:** The **no export-route** parameter under the **aaa authentication vpn** command did not work as expected. This issue is resolved by correcting the profile checking. **Scenario:** This issue occurred because the inner IP of IAP VPN was distributed over Open Shortest Path First (OSPF) after the **no export-route** parameter was configured under the **aaa authentication vpn** command. This issue was observed in a switch running AOS-W 6.4.2.13.	OSPF	All platforms	AOS-W 6.4.2.13	AOS-W 6.5.0.0
137641	**Symptom:** The **Port Status** LED in an OAW-4030 switch did not work. The fix ensures that the **Port Status** LED in a switch works as expected. **Scenario:** This issue was observed in OAW-4030 switches running cpboot version later than 43722.	Hardware Management	OAW-4030 switches	AOS-W 6.4.4.5	AOS-W 6.5.0.0
138014	**Symptom:** An AP crashed and rebooted frequently on a switch. The log files for the event listed the reason as **Reboot caused by kernel panic: Fatal exception in interrupt** or **Reboot due to out of Memory**. The fix ensures that the OAW-AP205H access points do not reboot unexpectedly. **Scenario:** This issue occurred because of a memory leak caused by the Jumbo frames. This issue was observed in OAW-AP205H access points running AOS-W 6.4.4.5.	AP-Platform	OAW-AP205H access points	AOS-W 6.4.4.5	AOS-W 6.5.0.0
138196 138482 138560 139345 140196 141406	**Symptom:** The **authentication** process stopped responding and crashed in a switch. The fix ensures that the **authentication** process does not crash in a switch. **Scenario:** This issue occurred because of memory corruption. This issue is observed in a local switch running AOS-W 6.4.3.6.	Base OS Security	All platforms	AOS-W 6.4.3.6	AOS-W 6.5.0.0

Table 5: *Resolved Issues in 6.5.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
138268	**Symptom:** OAW-AP277 access points displayed an I flag when connected to HP Layer 3 switch. The fix ensures that the power change detection is not mandated based on the AP state. **Scenario:** This issue occurred in OAW-AP277 access points connected to a Layer 3 HP switch with LLDP enabled on the switch port. This issue was observed in OAW-4x50 Series switches running AOS-W 6.4.3.4.	AP-Platform	OAW-4x50 Series switches	AOS-W 6.4.3.4	AOS-W 6.5.0.0
138271	**Symptom:** For High Throughput (HT) and Very High Throughput (VHT) 80 MHz channels, the switch sent the AMON messages with incorrect radio information to the OV3600 server. The fix ensures that the switch checks the channel type and populates the AMON messages with the correct radio information. **Scenario:** This issue was observed in switches running AOS-W 6.4.3.x or AOS-W 6.4.4.x.	Station Management	All platforms	AOS-W 6.4.4.4	AOS-W 6.5.0.0
138356	**Symptom:** AppRF did not block the desired traffic. This issue is resolved by blocking the desired traffic. **Scenario:** This issue occurred when DPI was classified but WebCC was not classified. The traffic did not go to Slow Path (SP) for DPI post ACL lookup for such session. Hence, DPI was not enforced. This issue was observed in switches running AOS-W 6.4.3.7.	Switch-Datapath	All platforms	AOS-W 6.4.3.7	AOS-W 6.5.0.0
138637	**Symptom:** Frames with VLAN 0 were dropped and not retransmitted over the air. The fix ensures that frames with VLAN ID 0 are not dropped. **Scenario:** This issue was observed in OAW-AP205 access points running AOS-W 6.4.3.4.	AP-Wireless	OAW-AP205 access points	AOS-W 6.4.3.4	AOS-W 6.5.0.0
138686	**Symptom:** The customer was intermittently unable to pass through traffic and the system displayed the **drop pkt as ip not assigned through dhcp** error message. This issue is resolved by manually clearing the route cache entry. **Scenario:** This issue was observed when the customer was present in the station table and the route cache entry for the station IP address had the OH flag. This issue is observed in OAW-4x50 Series switches running AOS-W 6.4.3.5.	Switch Datapath	OAW-4x50 Series switches	AOS-W 6.4.3.5	AOS-W 6.5.0.0

Table 5: *Resolved Issues in 6.5.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
138772	**Symptom:** An AP operated in the 802.3af mode. This issue is resolved by comparing the allocated power to the optimization power and enabling the Ethernet port when the allocated power is sufficient. **Scenario:** This issue occurred when AP power optimization option was enabled. This issue was observed in a OAW-AP225 or OAW-AP325 access points running AOS-W 6.4.4.5.	AP-Platform	OAW-AP225 and OAW-AP325 access points	AOS-W 6.4.4.5	AOS-W 6.5.0.0
138785	**Symptom:** On configuring the **Host Controller Name** and **Master Controller IP Address/DNS name** fields in the AP provisioning profile, the WebUI did not display the field values. The fix ensures that the correct field values are displayed. **Scenario:** This issue was not observed on executing the **show ap provisioning ap-name** command in the CLI. This issue was observed in switches running AOS-W 6.4.3.7.	WebUI	All platforms	AOS-W 6.4.3.7	AOS-W 6.5.0.0
139007	**Symptom:** The **WebCC** process stopped responding and crashed in a switch. This issue is resolved by using the value of 0 for an uncategorized Uniform Resource Locator (URL). **Scenario:** This issue occurred because the Webroot returned a value greater than the maximum category for an uncategorized URL. This issue was observed in a switch running AOS-W 6.4.2.x, AOS-W 6.4.3.x, or AOS-W 6.4.4.x.	WebUI	All platforms	AOS-W 6.4.3.5	AOS-W 6.5.0.0
139026	**Symptom:** When multiple clients (VM or physical clients) initiated the ICMP pings to the same destination IP-address almost simultaneously, the ICMP pings from only one client succeeded and those from the other clients did not. This issue is resolved by fixing the ICMP sequence of the Source Network Address Translation (SRC-NAT) in the datapath. **Scenario:** This issue was observed when SRC-NAT—that is, the **ip nat inside** option—was configured in the client VLANs and multiple clients started the ICMP pings to the same destination IP address simultaneously. This issue was not limited to any specific switch model or AOS-W version.	Switch Datapath	All platforms	AOS-W 6.4.3.7	AOS-W 6.5.0.0

Table 5: *Resolved Issues in 6.5.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
139061	**Symptom:** The switch rebooted with the reason as **RNGD reboot**. This issue is resolved by resetting the XLP CPU. **Scenario:** This issue was observed when the DRNG module reported error while booting and failed to generate random numbers. This issue was observed in OAW-40xx Series and OAW-4x50 Series switches running AOS-W 6.3.1.19.	Base OS Security	OAW-40xx Series and OAW-4x50 Series switches	AOS-W 6.3.1.19	AOS-W 6.5.0.0
139174	**Symptom:** On sending an SNMP message for a client, the 64-bit Rx/Tx rate fields were not populated by the AP. The fix ensures that the 64-bit Rx/Tx rate fields are sent as part of an SNMP message. **Scenario:** This issue was observed when clients were associated to OAW-AP320 Series access points running AOS-W 6.4.4.x.	Station Management	OAW-AP320 Series access points	AOS-W 6.4.4.3	AOS-W 6.5.0.0
139200	**Symptom:** Users were unable to decipher the ingress and egress interface values from the DHCP Debug logs as they were cryptic. The fix ensures that the DHCP debug logs are in user understandable format. **Scenario:** This issue occurred when DHCP debug logging was enabled. This issue was not specific to any switch model or release version.	DHCP	All platforms	AOS-W 6.3.1.16	AOS-W 6.5.0.0
139268 139351	**Symptom:** The **datapath** process in a switch crashed and the switch rebooted unexpectedly. The log file for the event listed the reason as **Datapath timeout**. This issue is resolved by dropping the packets that come over the mobility tunnel from the Home Agent to the Foreign Agent if they cause a bridge miss. **Scenario:** This issue occurred when packets coming over the mobility tunnel from the Home Agent to the Foreign Agent caused a bridge miss. This issue was observed in switches running AOS-W 6.4.3.6.	Switch-Datapath	All platforms	AOS-W 6.4.3.6	AOS-W 6.5.0.0

Table 5: *Resolved Issues in 6.5.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
139336 138868	**Symptom:** Traffic block was observed in switches when the customer tried to send an image using WhatsApp. The fix ensures that the WhatsApp message is classified so that the issue with sending an image using WhatsApp is resolved. **Scenario:** The WhatsApp traffic block was not functional as the latest version of WhatsApp was not classified as WhatsApp in the switch. This issue is observed in OAW-40xx Series and OAW-4x50 Series switches running AOS-W 6.4.3.7.	Switch-Datapath	OAW-40xx Series and OAW-4x50 Series switches	AOS-W 6.4.3.7	AOS-W 6.5.0.0
139341	**Symptom:** A branch switch ignored the branch configuration group **interface VLAN 4094** submode configuration including **ip nat outside**. This issue is resolved by moving the VLAN 4094 configuration prior to **interface VLAN 4094** submode configuration when a master switch generates the configuration to be pushed to the branch switch. **Scenario:** This issue occurred because VLAN 4094 was added after the **interface VLAN 4094** configuration was received when the configuration was pushed to the branch switch from a master switch, after the branch switch was reloaded. This issue was observed in branch switches running AOS-W 6.4.4.5.	Branch Switch	All platforms	AOS-W 6.4.4.5	AOS-W 6.5.0.0
139653	**Symptom:** An AP rebooted unexpectedly. The log file for the event listed the reason as **unknown**. This issue is resolved by disregarding the result of the pre-standard 802.3AT classification method based on the input voltage level measurement. Additionally, the power requested by the AP over LLDP is adjusted from 19.0 W to 20.2 W in normal mode and from 17.1 W to 17.2 W in reduced power mode. This allows an AP to operate during adverse conditions. **Scenario:** This issue occurred because the pre-standard 802.3AT classification created a false positive and an AP operated in full power mode when connected to a switch that was only 802.3AF-compliant. Thus, the AP exceeded the limits of the 802.3AF power budget of 12.9 W and consequently rebooted or was current limited by the switch and the log file for the event listed the reason as **unknown**. This issue was observed in OAW-AP220 Series access points running AOS-W 6.4.4.4.	AP-Platform	OAW-AP220 Series access points	AOS-W 6.4.4.4	AOS-W 6.5.0.0

Table 5: *Resolved Issues in 6.5.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
140057 142265	**Symptom:** An AP was unable to establish a Generic Route Encapsulation (GRE) tunnel with the switch. This issue is resolved by deauthenticating the client and cleaning up the VLAN ID array. **Scenario:** This issue occurred when the AP was not broadcasting the SSID but remote BSS-table was able to see the BSSID/SSID. This issue was observed when the STM received a VLAN delete message, and deleted all the VAPs with the same VLAN in the station VLAN array, which resulted in the switch bringing down the VAP without notifying the AP.	Station Management	All platforms	AOS-W 6.4.2.14	AOS-W 6.5.0.0
140121	**Symptom:** A user was unable to create an SNMPv3 community/user string with 6 characters. The fix ensures that an SNMPv3 community/user string can be created with a minimum of 6 characters. **Scenario:** This issue was observed in switches running AOS-W 6.4.3.x or later versions.	SNMP	All platforms	AOS-W 6.4.3.7-FIPS	AOS-W 6.5.0.0
140249	**Symptom:** OAW-AP204/OAW-AP205 access points were unable to modify the Maximum Segment Size (MSS) value. The fix ensures that the OAW-AP204/OAW-AP205 access points are able to set the value of Maximum Transmission Unit (MTU) correctly. **Scenario:** This issue was observed when the PPPoE server's MTU was set to a value lesser than 1492. This issue was observed in OAW-AP204 and OAW-AP205 access points connected to switches running AOS-W 6.4.4.6.	Remote Access Points	OAW-AP204 or OAW-AP205 access points	AOS-W 6.4.4.6	AOS-W 6.5.0.0
140290	**Symptom:** Tunneled-node clients failed to pass traffic when connected to a wired port of a Mobility Access Switch or a switch directly. The fix ensures that the switch initiates 802.1X authentication for tunneled-node clients. **Scenario:** This issue occurred because the switch did not trigger 802.1X authentication for wired users. This issue was observed in switches running AOS-W 6.4.1.0 or later versions.	Multiplexer	All platforms	AOS-W 6.4.2.15	AOS-W 6.5.0.0

Table 5: *Resolved Issues in 6.5.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
140383	**Symptom:** When the client upgraded an OAW-4550 switch from AOS-W 6.4.3.2 to AOS-W 6.4.3.7, there were multiple instances of **Authentication** module crash. The fix ensures that authentication is not performed on an AP wired port. **Scenario:** This issue occurred when authentication was performed on an AP wired port. This issue was observed in OAW-4x50 Series switches running AOS-W 6.4.3.7.	Base OS Security	OAW-4x50 Series switches	AOS-W 6.4.3.7	AOS-W 6.5.0.0
140386	**Symptom:** A switch did not allow the addition of multiple trap host with the same SNMPv3 user. The fix ensures that a switch allows the addition of multiple trap host with the same SNMPvV3 user. **Scenario:** This issue was observed in switches running AOS-W 6.4.3.7.	SNMP	All platforms	AOS-W 6.4.3.7	AOS-W 6.5.0.0
140507	**Symptom:** A user was unable to get the IP address post reconnection—after getting into the **power save** mode—if the user table entry was present. This issue is resolved by moving the user to **ready** state after MAC authentication was completed from cache. **Scenario:** This issue occurred when an existing user reconnected while **mac-auth** and **enforce-user-vlan** options were in enabled state. This issue was not limited to any specific switch platform or AOS-W version.	Base OS Security	All platforms	AOS-W 6.4.4.3	AOS-W 6.5.0.0
140731	**Symptom:** DHCP enforcement in the AAA profile failed on the switch for some clients connecting with static IP addresses. The fix ensures that the traffic from all the clients with static IP address is blocked when DHCP enforcement is enabled in the AAA profile. **Scenario:** This issue occurred when MAC-OS clients with static IP address connected to a switch on which the DHCP enforcement was enabled in the AAA profile. This issue was observed in switches running AOS-W 6.4.3.x.	Switch-Datapath	All platforms	AOS-W 6.4.3.7	AOS-W 6.5.0.0

Table 5: *Resolved Issues in 6.5.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
140923	**Symptom:** APs on a local switch went into inactive state randomly. The fix ensures that the **Packet** field representing information id length is within the ANQP Query Length value. **Scenario:** This issue occurred due to **Packet** field representing information ID length not getting checked against ANQP Query Length value. This issue was observed in switches running AOS-W 6.4.2.14.	Station Management	All platforms	AOS-W 6.4.2.14	AOS-W 6.5.0.0
141031	**Symptom:** Spare Ethernet ports got local IP address in bridge mode and were allowed Internet access even though the LAN connection was disconnected. The fix ensures that after an AP reboot, the Eth interface retains the Remote-AP Backup configuration. **Scenario:** This issue occurred when a RAP that had a LAN port (E1) setup for tunnel mode during switch configuration, reset the port to bridge mode when the RAP did not establish an IPsec VPN to the switch. This issue was observed as the tunnel node ports did not get disabled and were allowed access beyond RAP when the RAP was unable to connect to the switch.	Remote Access Points	All platforms	AOS-W 6.3.1.9	AOS-W 6.5.0.0
141221	**Symptom:** The **STM** process crashed in a switch. The fix ensures that the switch does not run out of memory and works as expected. **Scenario:** This issue occurred because the switch ran out of memory. This issue was observed in master switches running AOS-W 6.3.1.16 in a master-local topology.	Configuration	All platforms	AOS-W 6.3.1.16	AOS-W 6.5.0.0
141239	**Symptom:** Motorola MC75A0 handheld scanners were unable to associate to OAW-AP325 access points. This fix ensures that the device is able to connect to the OAW-AP325 access point. **Scenario:** This issue occurred when the client always sent a deauthentication message before sending the authentication message to the AP. Also, the AP sent deauthentication message to the client after receiving association request. This issue was observed in OAW-AP325 access points running AOS-W 6.4.4.5.	AP-Wireless	OAW-AP325 access points	AOS-W 6.4.4.5	AOS-W 6.5.0.0

Table 5: *Resolved Issues in 6.5.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
141272	**Symptom:** When the client tried to use USB as the backup uplink for the OAW-40xx Series switch, the switch was detected but the State was unreachable. The fix ensures that the USB modem is not in the Airplane mode when there is a new connection. If a USB modem goes into a bad state, execute the **usb reclassify** command or physically reconnect the USB modem. **Scenario:** This issue is observed in OAW-40xx Series switches running AOS-W 6.4.3.1.	Switch-Platform	OAW-40xx Series switch	AOS-W 6.4.3.1	AOS-W 6.5.0.0
141493	**Symptom:** OAW-AP335 access point rebooted unexpectedly. The log files for the event listed the reason as - **NS-TEST-4-RS-AP335-crash-54788-0509**. This issue is resolved by disabling the VGA driver. **Scenario:** This issue occurred when the VGA driver was enabled. This issue was observed in OAW-AP335 access points running AOS-W 6.5.0.0.	AP-Platform	OAW-AP335 access points	AOS-W 6.5.0.0	AOS-W 6.5.0.0
141646	**Symptom:** Campus access points (CAPs) responded to the Address Resolution Protocol (ARP) for the gateway IP address 192.168.11.1. This issue is resolved by using the correct process to program the br0 VLAN information when the AP's IP and the LMS IP lie in the range of 192.168.11.0/24. **Scenario:** This was caused due to an Endian issue when the AP's IP and the LMS IP belonged to the same range—that is, 192.168.11.0/24; the AP failed to use 172.16.11.0/24 as the DHCP server's IP address on the br0 interface and created a permanent ARP entry for 192.168.11.0/24. This issue was observed in OAW-AP204 and OAW-AP205 campus access points that were connected to switches running AOS-W 6.4.4.6.	AP Datapath	AP-20x Campus access points	AOS-W 6.4.4.6	AOS-W 6.5.0.0

Table 5: *Resolved Issues in 6.5.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
141678	**Symptom:** For the Session Initiation Protocol (SIP) clients with **VoIP CAC** enabled, when VoIP call admission control (CAC) threshold was reached, the SIP Invite to the called party was not blocked by the switch. This caused the called party to get call rings. This issue is resolved by successfully blocking the SIP Invite to the called party. **Scenario:** This issue occurred when the **send-sip-status-code** option to reject SIP calls with error codes was configured in the CAC profile. When the configured CAC threshold was reached, the newly initiated calls were blocked with the SIP error messages (SIP 486) being sent to the client or the server. But the switch did not block the SIP Invite being sent to the called party. This issue was observed in switches running AOS-W 6.4.x and AOS-W 6.5.x versions.	Unified Communication and Collaboration (UCC)	All platforms	AOS-W 6.4.4.6	AOS-W 6.5.0.0
141686	**Symptom:** Branch switch was unable to communicate with the master switch. This issue is fixed by avoiding network address translation of **ip nat outside** when the traffic is directed towards the master switch and flagging the master-ip route-cache entry as Permanent (P) and IPsec (I) in datapath. **Scenario:** This issue was observed when the **ip nat outside** option was enabled on the branch switch's uplink and the master switch’s IP is different from public IP. This issue occurred as the crypto SA between the Branch switch and the master switch was unstable and the cfgm packets from the Branch switch were Source-Network Address Translated (SRC-NATted).	Branch Switch	All platforms	AOS-W 6.4.4.0	AOS-W 6.5.0.0

Known Issues in AOS-W 6.5.0.0

This chapter describes the known and outstanding issues identified in AOS-W 6.5.0.0 release versions.

Table 6: *Known Issues in 6.5.0.0*

Bug ID	Description	Component	Platform	Reported Version
113049	**Symptom:** An internal error is sometimes observed when the user navigates to **Dashboard > Access Points** and tries to gather information about Goodput (bps) for wlan per AP. **Scenario:** This issue is observed in switches and access points running AOS-W 6.4.0.1 and above. **Workaround:** None.	Monitoring	All platforms	AOS-W 6.4.0.1
119293	**Symptom:** The switch fails to prioritize traffic based on the Wi-Fi Multimedia (WMM) traffic management profile. **Scenario:** The throughput bandwidth share across voice, video, best effort, and background is different from the bandwidth share configured in the WMM traffic management profile. This issue is observed in OAW-AP320 Series access points running AOS-W 6.4.4.0 or later versions. **Workaround:** None.	AP-Wireless	OAW-AP320 Series access points	AOS-W 6.4.4.0
119350	**Symptom:** The **Dashboard > Access Points** page of the switch WebUI displays an incorrect count of WLAN. **Scenario:** This issue occurs when Virtual APs (VAP) are configured through AP-specific configuration. This issue is not limited to any specific switch model or release version. **Workaround:** None.	Monitoring	All platforms	AOS-W 6.4.2.8
123601	**Symptom:** An AP stops responding and reboots. The log files for the event lists the reason as **SAPD module crash**. **Scenario:** After the AP reboots, the switch provisions it with the default AP group although it is provisioned with a custom AP group. This issue is observed in OAW-AP135 access points running AOS-W 6.4.2.10. **Workaround:** None.	AP-Datapath	OAW-AP135 access points	AOS-W 6.4.2.10

Table 6: *Known Issues in 6.5.0.0*

Bug ID	Description	Component	Platform	Reported Version
126244 133950 136632 136957	**Symptom:** An access point entry disappears from the local switch database and still displays as UP in the master switch. **Scenario:** This issue is observed in switches running AOS-W 6.4.3.5. **Workaround:** None.	AP-Platform	All platforms	AOS-W 6.4.3.5
126505	**Symptom:** An AP stops responding and reboots. The log files for the event lists the reason as **Reboot caused by kernel panic: Fatal exception in interrupt**. **Scenario:** This issue is observed in OAW-AP225 access points running AOS-W 6.4.2.3. **Workaround:** None.	AP-Platform	OAW-AP225 access points	AOS-W 6.4.2.3
127941	**Symptom:** OAW-AP225 access point misses DELBA (Delete BlockAck) from client randomly but continues to send TID (Terminal Identification), resulting in system lockups. **Scenario:** This issue is observed in OAW-AP225 access points running AOS-W 6.4.3.2. **Workaround:** None.	AP-Wireless	OAW-AP225 access points	AOS-W 6.4.3.2
128209	**Symptom:** When a user tries to hard reboot a switch, it fails to reboot with the following error: **not enough space on flash** **Scenario:** This issue occurs occasionally due to a database file corruption. This issue is observed in switches running AOS-W 6.4.2.x or later versions. **Workaround:** Contact Alcatel-Lucent Technical Support to remove the corrupted database file and recover the switch.	Switch-Platform	All platforms	AOS-W 6.4.2.12
128448	**Symptom:** A switch crashes and reboots unexpectedly. **Scenario:** After the switch is upgraded from 6.3.1.2 to 6.4.4.1, it crashes while running some SNMPv3 queries if configured with VRRP. This issue is observed in OAW-4750 switches running AOS-W 6.4.4.1. **Workaround:** None.	Switch-Datapath	OAW-4750 switches	AOS-W 6.4.4.1

Table 6: *Known Issues in 6.5.0.0*

Bug ID	Description	Component	Platform	Reported Version
129149	**Symptom:** The switch displays a non-configured WLAN SSID called **wired** in the **Dashboard > AppRF > WLAN > Details** section of the WebUI. **Scenario:** This issue occurs even when no WLAN SSID with the 'wired' name is configured in the switch. This issue is observed in switches running AOS-W 6.4.2.8 or AOS-W 6.4.3.7. **Workaround:** None.	Firewall Visibility	All platforms	AOS-W 6.4.2.8
130756	**Symptom:** After multiple reboots, there is a delay in access points connecting to the switch. **Scenario:** This issue is observed when an AP provisioned with uplink VLAN is not listed in trunk VLAN list of the uplink switch. The access point reverts to the native VLAN after rebooting multiple times. This issue is observed in access points running AOS-W 6.5.0.0. **Workaround:** Add access point's uplink VLAN to switch's trunk VLAN.	AP-Platform	All platforms	AOS-W 6.5
130840	**Symptom:** A wrong role is assigned to a user and a policy is wrongly applied to the traffic. **Scenario:** This issue is observed in switches running AOS-W 6.4.2.8. **Workaround:** None.	Base OS Security	All platforms	AOS-W 6.4.2.8
130983 136014 141304	**Symptom:** The Policy Based Routing (PBR) configuration in a standby switch is not retained after saving and reloading the standby switch. **Scenario:** This issue is observed in standby switches running AOS-W 6.4.4.1 in master-standby topology. **Workaround:** None.	Switch-Datapath	All platforms	AOS-W 6.4.4.1
131322	**Symptom:** An 802.1X machine authentication cache entry is created in a switch although a client does not perform machine authentication. **Scenario:** This issue is observed in switches running AOS-W 6.4.3.4 in master-standby-local topology. **Workaround:** None.	VLAN Derivation	All platforms	AOS-W 6.4.3.4
133036	**Symptom:** A switch encounters kernel panic. **Scenario:** This issue occurs when the USB reclassification happens many times, when a cellular modem—that is, modem models E3276 and E3372 (one that is not supported in AOS-W 6.5.0.0)— is connected as uplink to the switch in addition to the wired uplink. This issue is not limited to any specific switch model or AOS-W release version. **Workaround:** Either plug out and plug in the modem or reboot the switch.	Switch-Platform	All platforms	AOS-W 6.5.0.0

Table 6: *Known Issues in 6.5.0.0*

Bug ID	Description	Component	Platform	Reported Version
134232	**Symptom:** OAW-AP205 access points crashes and reboots when out of memory. **Scenario:** This issue is observed due to high slab memory allocation. This issue is observed in OAW-AP205 access points running AOS-W 6.4.2.6. **Workaround:** None.	AP-Platform	OAW-AP205 access points	AOS-W 6.4.2.6
135100	**Symptom:** When the persistent VAP feature is enabled on a VAP, the 802.1X wireless clients connected to the VAP lose connectivity if the AP loses connectivity to the switch. **Scenario:** When the AP loses connectivity to the switch and there are 802.1X clients connected to a persistent VAP, these clients lose their connectivity until the connectivity to the switch is restored. This issue is observed in OAW-AP200 Series, OAW-AP210 Series, and OAW-AP220 Series access points running AOS-W 6.4.3.6. **Workaround:** None.	Remote Access Points	OAW-AP200 Series, OAW-AP210 Series, and OAW-AP220 Series access points	AOS-W 6.4.3.6
135926	**Symptom:** After an Instant AP (IAP) or the VPN tunnel loses connectivity and returns to service, the nodes connected to VPN-NG centralized L2 VLANS behind IAPs becomes unreachable from behind the switch through the VPN tunnels. The switch shows L3 ARP entry for the node, but does not show L2 entry. **Scenario:** This issue is observed when an Instant AP is connected to a centralized switch through VPN-NG IPSEC tunnels configured for centralized L2 operations with Broadcast Multicast (BCMC) optimization configured on the VLAN. When the VPN tunnel is down, the switch deletes the learned L2 entries, but incorrectly keeps the L3 ARP entries. Once the VPN tunnel re-establishes, since the ARP entry exists, subsequent ARP frames are not flooded to the IAP and are not answered by the client allowing L2 re-learning. **Workaround:** Disable BCMC optimization on the affected VLAN by executing the following commands: **(host) (config) #interface vlan <VLAN>** **(host) (config-subif)#no bcmc-optimization**	RAP-NG	All platforms	AOS-W6.4.2.14

Table 6: *Known Issues in 6.5.0.0*

Bug ID	Description	Component	Platform	Reported Version
137031	**Symptom:** Clients are unable to associate to 2.4 GHz radio of the OAW-AP225 access points intermittently. **Scenario:** This issue occurs when the AP LACP profile is configured only on the master switch and not on the local switch. This issue is observed in OAW-AP225 access points connected to switches running AOS-W 6.4.2.0. **Workaround:** None.	AP-Platform	OAW-AP225 access points	AOS-W 6.4.2.0
138009	**Symptom:** An OAW-4650 switch (local) reboots because of datapath timeout. **Scenario:** This issue occurs after the local switch—supporting more than 1000 RAPs and 3000 wireless clients—is upgraded to AOS-W 6.4.2.15. This issue is observed in OAW-4650 switches running AOS-W 6.4.2.15 in a master-local topology. **Workaround:** None.	Switch-Datapath	OAW-4650 switches	AOS-W 6.4.2.15
138224	**Symptom:** A switch does not generate the syslog message 124821 when a Remote AP (RAP) has loop on Ethernet ports. **Scenario:** This issue is observed in switches running AOS-W 6.3.1.16. **Workaround:** None.	Remote Access Point	All platforms	AOS-W 6.3.1.16
138239 138240	**Symptom:** Clients are unable to pass traffic due to high CPU utilization. **Scenario:** This issue is observed in OAW-AP125 access points connected to switches running AOS-W 6.3.1.21. **Workaround:** None.	AP-Platform	OAW-AP125 access points	AOS-W 6.3.1.21
138684	**Symptom:** A switch crashes and reboots unexpectedly. The log files list the reason as **Datapath timeout (Intent:cause:register 56:86:50)**. **Scenario:** This issue is observed when provisioning an AP as a mesh point causing the switch to crash on a datapath module. This issue is observed in OAW-4604 switches running AOS-W 6.4.3.7. **Workaround:** None.	Switch-Datapath	OAW-4604 switches	AOS-W 6.4.37
139023	**Symptom:** Clients are unable to associate to G radio on OAW-AP103H access points. **Scenario:** This issue occurs when the OAW-AP103H access point terminates on an OAW-4750 switch. This issue is observed in OAW-AP103H access points connected to OAW-4750 switches running AOS-W 6.4.3.6. **Workaround:** None.	AP-Wireless	OAW-AP103H access points	AOS-W 6.4.3.6

Table 6: *Known Issues in 6.5.0.0*

Bug ID	Description	Component	Platform	Reported Version
139189	**Symptom:** An AP crashes and the log files list the reason for the event as **Reboot caused by kernel panic: Fatal exception**. **Scenario:** This issue occurs when multiple virtual access points are used in the bridge mode. This issues is observed in OAW-AP225 access points running AOS-W 6.5.0.0. **Workaround:** None.	AP-Platform	OAW-AP225 access points	AOS-W 6.5.0.0
139298 139371 140124 140918	**Symptom:** An AP crashes and the log files list the reason for the event as **Reboot caused by kernel panic: Fatal exception interrupt**. **Scenario:** This issue is observed in OAW-AP225 access points running AOS-W 6.4.2.5, AOS-W 6.4.2.12, or AOS-W 6.4.2.14. **Workaround:** None.	AP-Platform	OAW-AP225 access points	AOS-W 6.4.2.14
139416	**Symptom:** OAW-AP225 5 GHz radio is not functional after RADAR detect is triggered. **Scenario:** The customer receives a lot of random RADAR detections message on multiple APs. This issue is observed in OAW-AP225 access points running AOS-W 6.4.2.8. **Workaround:** Most the RADARs are detected on channel 116 triggering the switch to a Dynamic Frequency Selection (DFS) channel - 100/124/128/120. Remove the DFS channel.	AP-Wireless	OAW-AP225 access points	AOS-W 6.4.2.8
139424	**Symptom:** False RADAR events are detected on the DFS channel. **Scenario:** Access Points are moved to another channel, due to false RADAR detection. This issue is observed in OAW-AP320 Series access points running AOS-W 6.4.4.6. **Workaround:** None.	AP-Wireless	OAW-AP320 Series access points	AOS-W 6.4.4.6
139627	**Symptom:** Many APs randomly reboot without any reboot or bootstrap reason. **Scenario:** This issue is observed when upgrading the APs to AOS-W 6.4.4.5. **Workaround:** None.	AP-Wireless	All platforms	AOS-W 6.4.4.5
139913	**Symptom:** The noise floor value fluctuates to as much as 25 dB for certain APs. **Scenario:** This issue is observed in OAW-AP310 Series and OAW-AP330 Series access points running AOS-W 6.5.0.0. **Workaround:** None.	AP-Wireless	OAW-AP310 Series and OAW-AP330 Series access points	AOS-W 6.5.0.0

Table 6: *Known Issues in 6.5.0.0*

Bug ID	Description	Component	Platform	Reported Version
140154	**Symptom:** Frequent MAC authentication requests of devices that are not connected to the port are observed on the server. **Scenario:** This issue is observed in OAW-4x50 Series switches running AOS-W 6.4.3.6. **Workaround:** None.	Remote Access Point	OAW-4x50 Series switches	AOS-W 6.4.3.6
140175	**Symptom:** After a power cycle, the branch switch fails to establish isakmpd tunnel with the master switch. **Scenario:** This issue occurs after a power cycle, when uplink VLAN still points to the primary VLAN instead of the secondary VLAN. This issue is observed in OAW-40xx Series switches running AOS-W 6.5.0.0. **Workaround:** None.	Base OS Security	OAW-40xx Series switches	AOS-W 6.5.0.0
140327	**Symptom:** Memory usage of the **authentication** process in a switch increases gradually. **Scenario:** This issue occurs because of a memory leak. This issue is observed in switches running AOS-W 6.4.3.3. **Workaround:** None.	Base OS Security	All platforms	AOS-W 6.4.3.3
140721	**Symptom:** An OAW-AP103H access point reboots randomly without providing any reboot information. **Scenario:** This issue is observed in OAW-AP103H access points running AOS-W 6.4.4.4. **Workaround:** None.	AP-Platform	OAW-AP103H access points	AOS-W 6.4.4.4
140805	**Symptom:** Configuring multiple DHCP options in the DHCP pool using the navigation path **Configuration > Branch > Smart config > Routing > DHCP options** in the switch WebUI fails. **Scenario:** This issue is observed in switches running AOS-W 6.4.3.6. **Workaround:** None.	WebUI	All platforms	AOS-W 6.4.3.6
140984	**Symptom:** VOIP phones randomly stop passing traffic when connected to OAW-AP205 access points. **Scenario:** This issue is observed in access points running AOS-W 6.4.3.7. **Workaround:** None.	AP-Wireless	All platforms	AOS-W 6.4.3.7
141073	**Symptom: tacacs-accounting** configuration does not synchronize with the local switch that joins the network for the first time. **Scenario:** This issue is observed in switches running AOS-W 6.5.0.0. **Workaround:** None.	Base OS Security	All platforms	AOS-W 6.5

Table 6: *Known Issues in 6.5.0.0*

Bug ID	Description	Component	Platform	Reported Version
141213	**Symptom:** The **show ap debug radio-stats ap-name <ap-name> radio 1 advanced | include Busy** command displays the 2.4 GHz channels as busy although the Spectrum Analyzer displays the channels as free. **Scenario:** Initial investigation suggests that the TX timeout in the AP is significantly high although there is no heavy Tx traffic followed by a radio reset. This results in high utilization of the channel. This issue is observed in OAW-AP320 Series access points running AOS-W 6.4.4.5. **Workaround:** None.	AP-Wireless	OAW-AP320 Series access points	AOS-W 6.4.4.5
141285	**Symptom:** The ports on a switch moved to DOWN state unexpectedly. **Scenario:** This issue is observed in OAW-4x50 Series switches running AOS-W 6.5.0.0. **Workaround:** None.	Switch-Platform	OAW-4x50 Series switches	AOS-W 6.5.0.0
141455	**Symptom:** All access points connected to a switch reboot. The **LLDP**, **mDNS**, and **ARM** processes crash in the switch unexpectedly. The **STM** process in the switch uses more memory than usual. **Scenario:** This issue is observed in OAW-6000 switches running AOS-W 6.4.2.12. **Workaround:** None.	Switch-Platform	OAW-6000 switches	AOS-W 6.4.2.12
141558	**Symptom:** The Captive Portal redirection fails when using HTTP. **Scenario:** This issue occurs because the redirect URL from Captive Portal is appended with a string, **&arubalp**, when using HTTP. This issue is observed in switches running AOS-W 6.4.4.x or later versions. **Workaround:** Bypass the Captive Portal landing page to avoid this issue.	Captive Portal	All platforms	AOS-W 6.5.0.0
141684	**Symptom:** High latency is observed only when clients are connected to AirPlay, from a different subnet. **Scenario:** When a MacBook client is connected to a WLAN network, it works seamlessly and the speed reaches up to 300 Mbps; but, as soon as the screen is mirrored on an Apple TV, the speed drastically reduces to 10-30 Mbps. When the device is disconnected from AirPlay, it is back to normal working condition. This issue is observed in OAW-40xx Series switches running AOS-W 6.4.2.5. **Workaround:** None.	AP-Wireless	OAW-40xx Series switches	AOS-W 6.4.2.5

Table 6: *Known Issues in 6.5.0.0*

Bug ID	Description	Component	Platform	Reported Version
141938	**Symptom: fw_visibility** process stops responding and crashes on the switch. **Scenario:** This issue is observed due to a fault in segmentation. This issue is observed in OAW-4010 switches running AOS-W 6.4.4.8. **Workaround:** None.	Firewall	OAW-4010 switches	AOS-W 6.4.4.8
142121	**Symptom:** High CPU usage is observed in the **Station Management** module. **Scenario:** This issue is observed after upgrading the switch to AOS-W 6.4.3.7 in a master-local topology. **Workaround:** None.	Station Management	All platforms	AOS-W 6.4.3.7
142157	**Symptom:** The 5 GHz radio of an AP running in spectrum mode stops responding. **Scenario:** This issue is observed in OAW-AP315 access points running AOS-W 6.5.0.0. **Workaround:** Reboot the AP.	Spectrum	OAW-AP315 access points	AOS-W 6.5.0.0
142197	**Symptom:** An issue with client connectivity is observed as access points switch channels randomly due to false RADAR detection. **Scenario:** After upgrading to AOS-W 6.4.2.14, the following issues are observed: ● Multiple OAW-AP225 access points do not have wireless association for a long duration. ● Excessive channel switching is observed due to RADAR detect trigger. ● 5 GHz radio does not accept associations and transmission of frames is stalled until the AP is rebooted. This issue is observed in OAW-AP225 access points running AOS-W 6.4.2.14. **Workaround:** Rebooting the AP and forcing channel change by manually triggering a configuration commit from the AP fixes the issue with the radio.	AP-Wireless	OAW-AP225 access points	AOS-W 6.4.2.14
142383	**Symptom:** An AP intermittently does not transmit beacons. **Scenario:** This issue is observed when the AP is put in an RF shield box or cage, and scanning is enabled. This issue is observed in OAW-AP335 access points running AOS-W 6.5.0.0. **Workaround:** Disable scanning. To disable scanning, in the RF ARM profile, execute the **no scanning** command.	AP-Wireless	OAW-AP335 access points	AOS-W 6.5.0.0

Table 6: *Known Issues in 6.5.0.0*

Bug ID	Description	Component	Platform	Reported Version
142397	**Symptom:** IPv4 syslog messages are interpreted incorrectly due to invalid timestamp format. **Scenario:** This issue occurs because the timestamp in the syslog message for IPv4 address includes the year at the end, which is not according to the standards. This issue is not limited to any specific switch model or release version. **Workaround:** None.	Logging	All platforms	AOS-W 6.4.4.6
142498	**Symptom:** An AP crashes and the log files listed the reason for the event as **Reboot caused by kernel panic: Rebooting the AP because of FW ASSERT**. **Scenario:** This issue is observed in OAW-AP320 Series access points running AOS-W 6.4.4.4. **Workaround:** None.	AP-Platform	OAW-AP320 Series access points	AOS-W 6.4.4.4
142620	**Symptom:** The system user-roles are missing from a switch. **Scenario:** This issue occurs after a switch reboots due to power cycle failure. This issue is not limited to any specific switch model or release version. **Workaround:** None.	Licensing	All platforms	AOS-W 6.4.2.15
142663	**Symptom:** The command-line interface does not prompt for a reboot the first time a license is installed on a switch using centralized licensing. **Scenario:** When you install a license on a switch, you must reboot that device before the license is activated. An issue is observed where the command-line interface fails to display a reminder to prompt the user to reboot the switch. **Workaround:** None.	Licensing	OAW-4x50 Series and OAW-40xx Series switches	AOS-W 6.3.2.0
142678	**Symptom:** Adding a Network Translation Protocol (NTP) server to the switch causes all the Instant AP VPN /RAP to reconnect without notification. Many Instant AP VPNs cannot recover as well. **Scenario:** This issue occurs when the NTP server tries to correct the time difference in the switch. This issue is not limited to any specific switch model or release version. **Workaround:** Reboot the switch after configuring the NTP server.	IPsec	All platforms	AOS-W 6.4.2.13

Table 6: *Known Issues in 6.5.0.0*

Bug ID	Description	Component	Platform	Reported Version
142679	**Symptom:** An yellow exclamation mark is displayed on the wireless Network Interface Card (NIC) and the wireless users are unable to pass traffic. **Scenario:** This issue is observed as the client is unable to resolve the Address Resolution Protocol (ARP) for its default gateway. This issue is observed in switches running AOS-W 6.4.3.7. **Workaround:** Disable the **Allow the computer to turn off this device to save power** under the adapter properties of the computer.	AP-Wireless	All platforms	AOS-W 6.4.3.7
142728	**Symptom:** An AP fails to accept the antenna gain value when configured from the **apboot** prompt. **Scenario:** This issue is observed when the **setenv a_ant_gain <value>** command is executed form the **apboot** prompt of the AP. This issue is observed in OAW-AP224 access points running AOS-W 6.4.2.12. **Workaround:** Configure the antenna gain value from the WebUI.	AP-Platform	OAW-AP224 access points	AOS-W 6.4.2.12
142800	**Symptom:** A radio operating on 80+80 channel width operates the secondary 80 MHz channel on a different channel than the one reported on the switch. **Scenario:** This issue occurs because the RADAR detection happens on the secondary 80 MHz channel. This issue is observed when the 802.11a radio is configured for 80+80 operation and the secondary 80 MHz channel uses DFS channels. This issue is observed in OAW-AP315 and OAW-AP335 access points connected to switches running AOS-W 6.5.0.0. **Workaround:** Do not use DFS channels for the secondary 80 MHz channel in 80+80 operation.	ARM	OAW-AP315 and OAW-AP335 access points	AOS-W 6.5.0.0

Chapter 6 Upgrade Procedure

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

CAUTION

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

Topics in this chapter include:

Upgrade Caveats

- OAW-AP120 Series access points, OAW-4306 Series, OAW-4x04 Series, OAW-S3, and OAW-6000 switches are not supported from AOS-W 6.5.x. Do not upgrade to AOS-W 6.5.x if your deployment contains a mix of these switches in a master-local setup.
- If your switch is running AOS-W 6.4.0.0 or later versions, do not use a Windows-based TFTP server to copy the AOS-W image to the nonboot partition of the switch for upgrading or downgrading. Use FTP or SCP to copy the image.
- Starting from AOS-W 6.4.x, you cannot 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 following ACL, both ACE entries could not be configured in AOS-W 6.4.x. When the second ACE is added, it overwrites the first.

```
(host)(config) #ip access-list session allowall-laptop
(host)(config-sess-allowall-laptop) #any any any permit time-range test_range
(host)(config-sess-allowall-laptop) #any any any deny
(host)(config-sess-allowall-laptop) #!
(host)(config) #end
(host) #show ip access-list allowall-laptop

ip access-list session allowall-laptop
allowall-laptop
---------------
Priority        Source  Destination     Service Action  TimeRange
--------        ------  -----------     ------- ------  ---------
1               any     any             any     deny
```

- When upgrading the software in a multiswitch network (one that uses two or more Alcatel-Lucent switches), special care must be taken to upgrade all the switches in the network and to upgrade them in the proper sequence. (See Upgrading in a Multiswitch Network on page 93.)

GRE Tunnel-Type Requirements

This section describes the important points to remember when configuring an L2 GRE tunnel with respect to tunnel type:

- AOS-W 6.5.0.0 continues to support L2 GRE tunnel type zero, but it is recommended to use a non-zero tunnel type.
- If both L2 and L3 tunnels are configured between endpoint devices, you must use a non-zero tunnel type for L2 GRE tunnels.

Important Points to Remember and Best Practices

Ensure a successful upgrade and optimize your upgrade procedure by taking the recommended actions provided in the following list. You should save this list for future use.

- Schedule the upgrade during a maintenance window and notify your community of the planned upgrade. This prevents users from being surprised by a brief wireless network outage during the upgrade.
- Avoid making any other changes to your network, such as configuration changes, hardware upgrades, or changes to the rest of the network during the upgrade. This simplifies troubleshooting.
- Know your network and verify the state of your network by answering the following questions:
  - How many APs are assigned to each switch? Verify this information by navigating to the **Monitoring > NETWORK > All Access Points** section of the WebUI, or by executing the **show ap active** and **show ap database** CLI commands.
  - How are those APs discovering the switch (DNS, DHCP Option, Broadcast)?

  - What version of AOS-W is currently on the switch?
  - Are all switches in a master-local cluster running the same version of software?
  - Which services are used on the switches (employee wireless, guest access, remote AP, wireless voice)?
- Resolve any existing issues (consistent or intermittent) before you upgrade.
- If possible, use FTP to load software images to the switch. FTP is faster than TFTP and offers more resilience over slow links. If you must use TFTP, ensure the TFTP server can send over 30 MB of data.
- Always upgrade the non-boot partition first. If problems occur during the upgrade, you can restore the flash, and switch back to the boot partition. Upgrading the non-boot partition gives you a smoother downgrade path should it be required.
- Before you upgrade to this version of AOS-W, assess your software license requirements and load any new or expanded licenses you may require. For a detailed description of these new license modules, refer to the “Software Licenses” chapter in the *AOS-W 6.5.x User Guide*.

Memory Requirements

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

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

CAUTION

In certain situations, a reboot or a shutdown could cause the switch to lose the information stored in its compact flash card. To avoid such issues, it is recommended that you execute the **halt** command before power cycling.

If the output of the **show storage** command indicates that there is insufficient flash memory space, you must free up some used memory. Any switch logs, crash data, or flash backups should be copied to a location off the switch, then deleted from the switch to free up flash space. You can delete the following files from the switch to free up some memory before upgrading:

- **Crash Data:** Execute the **tar crash** command to compress crash files to a file named **crash.tar**. Use the procedures described in Backing up Critical Data on page 92 to copy the **crash.tar** file to an external server, and then execute the **tar clean crash** command to delete the file from the switch.
- **Flash Backups:** Use the procedures described in Backing up Critical Data on page 92 to back up the flash directory to a file named **flash.tar.gz**, and then execute the **tar clean flash** command to delete the file from the switch.
- **Log files:** Execute the **tar logs** command to compress log files to a file named **logs.tar**. Use the procedures described in Backing up Critical Data on page 92 to copy the **logs.tar** file to an external server, and then execute the **tar clean logs** command to delete the file from the switch.

Backing up Critical Data

It is important to frequently back up all critical configuration data and files on the compact flash file system to an external server or mass storage device. At the very least, you should include the following files in these frequent backups:

- Configuration data
- WMS database
- Local user database
- Licensing database
- Floor plan JPEGs
- Custom captive portal pages
- X.509 certificates
- Switch Logs

Backing up and Restoring Compact Flash in the WebUI

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

1. Click the **Configuration** tab.
2. Click **Save Configuration** at the top of the page.
3. Navigate to the **Maintenance > File > Backup Flash** page.
4. Click **Create Backup** to back up the contents of the compact flash file system to the **flashbackup.tar.gz** file.
5. Click **Copy Backup** to copy the file to an external server.

   You can later copy the backup file from the external server to the compact flash file system using the file utility in the **Maintenance > File > Copy Files** page.
6. To restore the backup file to the Compact Flash file system, navigate to the **Maintenance > File > Restore Flash** page and click **Restore**.

Backing up and Restoring Compact Flash in the CLI

The following steps describe the backup and restore procedure for the entire compact flash file system using the switch's command line:

1. Make sure you are in the **enable** mode in the switch CLI, and execute the following command:

   ```
    (host) # write memory
   ```
2. Execute the **backup** command to back up the contents of the compact flash file system to the **flashbackup.tar.gz** file.

   ```
    (host) # backup flash
   Please wait while we tar relevant files from flash...
   Please wait while we compress the tar file...
   Checking for free space on flash...
   ```

```
Copying file to flash...
File flashbackup.tar.gz created successfully on flash.
```

3. Execute the **copy** command to transfer the backup flash file to an external server or storage device.

   ```
   (host) copy flash: flashbackup.tar.gz ftp: <ftphost> <ftpusername> <ftpuserpassword> <remote directory>
   (host) copy flash: flashbackup.tar.gz usb: partition <partition-number>
   ```

   You can later transfer the backup flash file from the external server or storage device to the compact flash file system by executing the **copy** command.

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

4. Execute the **restore** command to untar and extract the **flashbackup.tar.gz** file to the compact flash file system.

   ```
   (host) # restore flash
   ```

Upgrading in a Multiswitch Network

In a multiswitch network (a network with two or more Alcatel-Lucent switches), special care must be taken to upgrade all switches based on the switch type (master or local). Be sure to back up all switches being upgraded, as described in Backing up Critical Data on page 92.

NOTE

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

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

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

Installing the FIPS Version of AOS-W 6.5.0.0

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

Instructions on Installing FIPS Software

NOTE

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

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

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

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

Upgrading to AOS-W 6.5.0.0

The following sections provide the procedures for upgrading the switch to AOS-W 6.5.0.0 by using the WebUI and the CLI.

Install Using the WebUI

CAUTION

Confirm that there is at least 60 MB of free memory and at least 75 MB of flash space available for an upgrade using the WebUI. For details, see Memory Requirements on page 91.

NOTE

When you navigate to the **Configuration** tab of the switch's WebUI, the switch may display the **Error getting information: command is not supported on this platform** message. This error occurs when you upgrade the switch from the WebUI and navigate to the **Configuration** tab as soon as the switch completes rebooting. This error is expected and disappears after clearing the Web browser cache.

Upgrading From an Older Version of AOS-W

NOTE

When upgrading from an existing AOS-W 6.4.x release, it is required to set AMON packet size manually to a desired value. However, the packet size is increased to 32K by default for fresh installations of AOS-W 6.4.3.9.

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 6.5.0.0.

- For switches running 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 switches running AOS-W 3.x or those running AOS-W 5.0.x versions earlier than AOS-W 5.0.3.1, download and install the latest version of AOS-W 5.0.4.x.
- For switches running AOS-W 6.0.0.0 or 6.0.0.1 versions, download and install the latest version of AOS-W 6.0.1.x.

Follow step 2 to step 11 of the procedure described in Upgrading From a Recent Version of AOS-W on page 94 to install the interim version of AOS-W, and then repeat steps 1 through 11 of the procedure to download and install AOS-W 6.5.0.0.

Upgrading From a Recent Version of AOS-W

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

- AOS-W 3.4.4.1 or later
- AOS-W5.0.3.1 or the latest version of AOS-W 5.0.x
- AOS-W 6.0.1.0 or later version of AOS-W 6.x

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

1. Download AOS-W 6.5.0.0 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 **Alcatel.sha256** file from the download directory.
   b. To verify the image, load the image onto a Linux system and execute the **sha256sum <filename>** command or use a suitable tool for your operating system that can generate a **SHA256** hash of a file.
   c. Verify that the output produced by this command matches the hash value found on the support site.

NOTE

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

4. Log in to the AOS-W WebUI from the PC or workstation.
5. Navigate to the **Maintenance > Controller > Image Management** page.
   a. Select the **Local File** option.
   b. Click **Browse** to navigate to the saved image file on your PC or workstation.
6. Select the downloaded image file.
7. Choose the nonboot partition from the **Partition to Upgrade** radio button.
8. Choose **Yes** in the **Reboot Controller After Upgrade** radio button to automatically reboot after upgrading. Choose **No**, if you do not want the switch to reboot immediately.

NOTE

Upgrade will not take effect until you reboot the switch.

9. Choose **Yes** in the **Save Current Configuration Before Reboot** radio button.
10. Click **Upgrade**.

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

    If you chose to automatically reboot the switch in step 8, the reboot process starts automatically within a few seconds (unless you cancel it).

12. When the reboot process is complete, log in to the WebUI and navigate to the **Monitoring > NETWORK > All WLAN Controllers** page to verify the upgrade.

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

1. Log in to the WebUI to verify all your switches are up after the reboot.
2. Navigate to the **Monitoring > NETWORK > Network Summary** page to determine if your APs are up and ready to accept clients. In addition, verify that the number of access points and clients are what you would expect.
3. Verify that the number of access points and clients are what you would expect.
4. Test a different type of client for each access method that you use and in different locations when possible.
5. Complete a backup of all critical configuration data and files on the compact flash file system to an external server or mass storage facility. See Backing up Critical Data on page 92 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.

Install Using the CLI

CAUTION

Confirm that there is at least 40 MB of free memory and at least 60 MB of flash space available for an upgrade using the CLI. For details, see Memory Requirements on page 91.

Upgrading From an Older Version of AOS-W

Before you begin, verify the version of AOS-W currently running on your switch. For more information, see Upgrading From an Older Version of AOS-W on page 94.

Follow steps 2 through 7 of the procedure described in Upgrading From a Recent Version of AOS-W on page 96 to install the interim version of AOS-W, and then repeat steps 1 through 7 of the procedure to download and install AOS-W 6.5.0.0.

Upgrading From a Recent Version of AOS-W

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

- AOS-W 3.4.4.1 or later
- AOS-W 5.0.3.1 or the latest version of AOS-W 5.0.x
- AOS-W 6.0.1.0 or later version of AOS-W 6.x

To install the AOS-W software image from a PC or workstation using the CLI on the switch:

1. Download AOS-W 6.5.0.0 from the customer support site.
2. Open an SSH session on your master (and local) switches.
3. Execute the **ping** command to verify the network connection from the target switch to the SCP/FTP/TFTP server.

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

or

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

or

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

4. Execute the **show image version** command to check if the AOS-W images are loaded on the switch's flash partitions. The partition number appears in the **Partition** row; **0:0** is partition 0, and **0:1** is partition 1. The active boot partition is marked as **Default boot**.

5. Execute the **copy** command to load the new image onto the nonboot partition.

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

or

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

or

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

or

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

NOTE

The USB option is available on the OAW-40xx Series and OAW-4x50 Seriesswitches.

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

```
(host)# reload
```

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

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

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

1. Log in to the CLI to verify that all your switches are up after the reboot.
2. Execute the **show ap active** command to determine if your APs are up and ready to accept clients.
3. Execute the **show ap database** command to verify that the number of access points and clients are what you expected.
4. Test a different type of client for each access method that you use and in different locations when possible.
5. Complete a backup of all critical configuration data and files on the compact flash file system to an external server or mass storage facility. See Backing up Critical Data on page 92 for information on creating a backup.

Downgrading

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

CAUTION

If you upgraded from AOS-W 3.3.x to AOS-W 5.0, the upgrade script encrypts the internal database. New entries created in AOS-W 6.5.0.0 are lost after the downgrade (this warning does not apply to upgrades from AOS-W 3.4.x to AOS-W 6.1).

CAUTION

If you 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 6.5.0.0 to 5.0.3.2, changes made to WIPS in AOS-W 6.x prevent the new predefined IDS profile assigned to an AP group from being recognized by the older version of AOS-W. This unrecognized profile can prevent associated APs from coming up, and can trigger a profile error.

These new IDS profiles begin with *ids-transitional* while older IDS profiles do not include *transitional*. If you have encountered this issue, execute the **show profile-errors** and **show ap-group** commands to view the IDS profile associated with the AP group

CAUTION

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

Before You Begin

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

1. Back up your switch. For details, see Backing up Critical Data on page 92.
2. Verify that the control plane security is disabled.
3. Set the switch to boot with the previously saved pre-AOS-W 6.5.0.0 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 is displayed if system boot parameters are set for incompatible image and configuration files.
5. After downgrading the software on the switch, perform the following steps:
   - Restore pre-AOS-W 6.5.0.0 flash backup from the file stored on the switch. Do not restore the AOS-W 6.5.0.0 flash backup file.
   - You do not need to reimport the WMS database or RF Plan data. However, if you have added changes to RF Plan in AOS-W 6.5.0.0, the changes do not appear in RF Plan in the downgraded AOS-W version.
   - If you installed any certificates while running AOS-W 6.5.0.0, you need to reinstall the certificates in the downgraded AOS-W version.

Downgrading Using the WebUI

The following section describes how to use the WebUI to downgrade the software on the switch.

1. If the saved preupgrade configuration file is on an external FTP/TFTP server, copy the file to the switch by navigating to the **Maintenance > File > Copy Files** page.

   a. For **Source Selection**, select FTP/TFTP server, and enter the IP address of the FTP/TFTP server and the name of the preupgrade configuration file.
   b. For **Destination Selection**, enter a file name (other than default.cfg) for Flash File System.
2. Set the switch to boot with your preupgrade configuration file by navigating to the **Maintenance > Controller > Boot Parameters** page.
   a. Select the saved preupgrade configuration file from the **Configuration File** drop-down list.
   b. Click **Apply**.
3. Determine the partition on which your previous software image is stored by navigating to the **Maintenance > Controller > Image Management** page. If there is no previous software image stored on your system partition, load it into the backup system partition (you cannot load a new image into the active system partition) by performing the following steps:
   a. Enter the FTP/TFTP server address and image file name.
   b. Select the backup system partition.
   c. Click **Upgrade**.
4. Navigate to the **Maintenance > Controller > Boot Parameters** page.
   a. Select the system partition that contains the preupgrade image file as the boot partition.
   b. Click **Apply**.
5. Navigate to the **Maintenance > Controller > Reboot Controller** page. Click **Continue**. The switch reboots after the countdown period.
6. When the boot process is complete, verify that the switch is using the correct software by navigating to the **Maintenance > Controller > Image Management** page.

Downgrading Using the CLI

The following section describes how to use the CLI to downgrade the software on the switch.

1. If the saved preupgrade configuration file is on an external FTP/TFTP server, use the following command to copy it to the switch:

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

   or

   ```
   (host) # copy tftp: <tftphost> <image filename> system: partition 1
   ```

2. Set the switch to boot with your preupgrade configuration file.

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

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

   In the following example, partition 1, the backup system partition, contains the backup release AOS-W 6.1.3.2. Partition 0, the default boot partition, contains the AOS-W 6.5.0.0 image.

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

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

5. Reboot the switch.

```
(host) # reload
```

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

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

Before You Call Technical Support

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

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