AOS-W 8.4.0.0

Alcatel·Lucent Enterprise

Release Notes

Copyright Information

Alcatel-Lucent and the Alcatel-Lucent Enterprise logo are trademarks of Alcatel-Lucent. To view other trademarks used by affiliated companies of ALE Holding, visit:

https://www.al-enterprise.com/en/legal/trademarks-copyright

All other trademarks are the property of their respective owners. The information presented is subject to change without notice. Neither ALE Holding nor any of its affiliates assumes any responsibility for inaccuracies contained herein. (2019)

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.

Contents ... **3**

Revision History ... 5

Release Overview ... **6**

Chapter Overview ... 6

Related Documents ... 6

Supported Browsers ... 7

Contacting Support ... 7

New Features and Enhancements ... **8**

Supported Hardware Platforms ... **22**

switch Platforms ... 22

AP Platforms ... 22

Virtual Platforms ... 24

Regulatory Updates ... **25**

Resolved Issues ... **26**

Known Issues and Limitations ... **66**

Upgrade Procedure ... **90**

Migrating from AOS-W 6.x to AOS-W 8.x ... 90

Important Points to Remember and Best Practices 91
Memory Requirements 91
Backing up Critical Data 92
Upgrading 94
Downgrading 97
Before You Call Technical Support 99
Glossary of Terms 100

Revision History

The following table provides the revision history of this document.

Table 1: *Revision History*

Revision	Change Description
Revision 02	■ Added description for known issue, 194140. ■ Removed description of known issue, 188600.
Revision 01	Initial release.

This AOS-W release notes includes the following topics:

NOTE

Throughout this document, branch switch and local switch are termed as managed device.

Chapter Overview

Use the following links to navigate to the corresponding topics:

- New Features and Enhancements on page 8 describes the new features and enhancements introduced in this release.
- Supported Hardware Platforms on page 22 describes the hardware platforms supported in this release.
- Regulatory Updates on page 25 lists the regulatory updates in this release.
- Resolved Issues on page 26 lists the issues resolved in this release.
- Known Issues and Limitations on page 66 lists the issues identified in this release.
- Upgrade Procedure on page 90 describes the procedures for upgrading your WLAN network to the latest AOS-W version.
- Glossary of Terms on page 100 lists the acronyms and abbreviations.

Related Documents

The following guides are part of the complete documentation for the Alcatel-Lucent user-centric network:

- *AOS-W Getting Started Guide*
- *AOS-W User Guide*
- *AOS-W CLI Reference Guide*
- *AOS-W Migration Guide*
- *AOS-W API Guide*
- *Alcatel-Lucent Mobility Master Licensing Guide*
- *Alcatel-Lucent Virtual Appliance Installation Guide*
- *Alcatel-Lucent Mobility Master Hardware Appliance Installation Guide*

Supported Browsers

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

- Microsoft Internet Explorer 11 on Windows 7 and Windows 8
- Microsoft Edge (Microsoft Edge 38.14393.0.0 and Microsoft EdgeHTML 14.14393) on Windows 10
- Firefox 48 and later on Windows 7, Windows 8, Windows 10 and Mac OS
- Apple Safari 8.0 or later on Mac OS
- Google Chrome

Contacting Support

Table 2: *Contact Information*

Contact Center Online	
Main Site	https://www.al-enterprise.com
Support Site	https://businessportal2.alcatel-lucent.com
Email	ebg_global_supportcenter@al-enterprise.com
Service & Support Contact Center Telephone	
North America	1-800-995-2696
Latin America	1-877-919-9526
EMEA	+800 00200100 (Toll Free) or +1(650)385-2193
Asia Pacific	+65 6240 8484
Worldwide	1-818-878-4507

This chapter describes the features and/or enhancements introduced in AOS-W 8.4.0.0.

AirGroup

AP Name

The **show airgroup aps** command is modified to list the name of the neighbor AP, if available, in the **Neighbor AP name** parameter. If the name of the neighbor AP name is not available, the BSSID of the neighbor AP is listed.

Air Management - IDS

Legend Alphabetizing

Starting from AOS-W 8.4.0.0, the output legends like flags and statuses for the command, **show ap debug client-table** is sorted in alphabetical order to increase readability.

AMON

Support for Smart AMON

AMON feeds are now made programmable and cloud friendly to help minimize the AMON telemetry traffic between the switch and the Cloud.

This feature enables the following new capabilities to the AMON feeds to Cloud destination over Websockets:

- Tuned for per-destination-tuned low-over head AMON feeds
- Cloud bootstrapping support
- AMON feed compression

AP Platform

IEEE 802.11ad Support

IEEE 802.11ad, also known as WiGig, is a multi-gigabit Wi-Fi technology that allows managed devices to communicate at multi-Gigabit speeds over a 60 GHz frequency band. This technology comprises of two radios, 5 GHz and 60 GHz.

IEEE 802.11ax Support

IEEE 802.11ax, also known as High-Efficiency WLAN (HEW), is a multi-gigabit Wi-Fi technology that allows managed devices to communicate on both the 2.4 GHz and 5 GHz frequency bands. This technology improves spectrum efficiency and area throughput in dense deployment scenarios of APs or stations in both indoor and outdoor environments.

OAW-AP510 Series Campus Access Points

NOTE

The OAW-AP510 Series Campus Access Points is categorized under **Early Availability** release. Refer to the following section, for a list of features that are targeted for a future release.

The Alcatel-Lucent OAW-AP510 Series OAW-APs (OAW-AP514 and OAW-AP515) are high-performance, multi-radio wireless devices that can be deployed in either switch-based (AOS-W) or switch less (Alcatel-Lucent AOS-W Instant) network environments. These APs deliver high performance concurrent 2.4 GHz and 5 GHz 802.11ax Wi-Fi functionality with MIMO radios (2x2 in 2.4 GHz, 4x4 in 5 GHz), while also supporting legacy 802.11a/b/g/n/ac wireless services.

The Alcatel-Lucent OAW-AP510 Series OAW-APs are equipped with an integrated BLE and Zigbee radio that provide the following capabilities:

- Location beacon applications
- Wireless console access
- IoT gateway applications

Ethernet ports on the access points are used to connect the device to the wired networking infrastructure and provide (802.3at class 4) PoE power to the device. The access points are equipped with a USB-A port that is compatible with selected cellular modems and other peripherals. When active, this port can supply up to 5W/1A to a connected device.

The following features are targeted for future releases and are currently not supported on the Alcatel-Lucent OAW-AP510 Series OAW-APs:

- Orthogonal Frequency Division Multiple Access (OFDMA)
- Multi User MIMO
- Transmit Beam Forming (TxBF)
- BSS Coloring
- Target Wait Time (TWT)
- Multi Band Operation (MBO)
- Spectrum analysis
- Mesh
- Cellular modem support
- 512 associated clients per radio (currently limited to 230 clients)

For complete technical details see the *Alcatel-Lucent OAW-AP510 Series Campus APs Datasheet*. For installation instructions, see the *Alcatel-Lucent OAW-AP510 Series OAW-APs Installation Guide*.

OAW-AP303P Campus Access Points

The OAW-AP303P access point is a high-performance dual-radio wireless device that supports IEEE 802.11ac Wave 2 standard. This AP uses MU-MIMO (Multi-User Multiple-Input, Multiple-Output) technology to provide secure wireless connectivity for both 2.4 GHz 802.11 b/g/n/ac and 5 GHz 802.11 a/n/ac Wi-Fi networks.

This AP provides the following capabilities:

- IEEE 802.11a/b/g/n/ac operation as a wireless access point
- IEEE 802.11a/b/g/n/ac operation as a wireless air monitor
- IEEE 802.11a/b/g/n/ac spectrum monitor
- Compatibility with IEEE 802.3af/at/bt PoE
- Supports PoE (E1 port) with PSE power
- Integrated BLE/Zigbee radio

For complete technical details, see the *Alcatel-Lucent OAW-AP303 Series Campus Access Points datasheet*. For installation instructions, see the *Aruba OAW-AP303P Campus Access Points Installation Guide*.

OAW-AP387 Access Points

The OAW-AP387 outdoor access points are high-performance dual-radio wireless devices that support IEEE 802.11ad Wave 2 standard. This AP uses MU-MIMO (Multi-User Multiple-Input, Multiple-Output) technology to provide secure mesh connectivity for both 5 GHz 802.11a, 802.11n, and 802.11ac, and 60 GHz 802.11ad Wi-Fi networks. The OAW-AP387 series access points can be deployed in either a controller-based (AOS-W) or controller-less (AOS-W InstantOS) network environment.

This AP provides the following capabilities:

- Point-to-point mesh deployment in 60 GHz and 5 GHz radios
- Compatibility with IEEE 802.3af and IEEE 802.3at PoE power sources
- Integrated BLE radio

NOTE

OAW-AP387 does not support wireless access.

For complete technical details and installation instructions, see *Alcatel-Lucent OAW-AP387 Series Outdoor Access Points Installation Guide*.

NetInsight Integration with AirMatch

AOS-W is now integrated with NetInsight, Alcatel-Lucent's Network Analytics and Assurance solution. The analytics engine in NetInsight can push radio profile EIRP recommendations, channel-bandwidth recommendations, and regulatory domain profile recommendations to an AP. The following command is introduced as part of this feature:

- **show ap analytics recommendations**

IP Conflict Detection

Starting from this release, APs can detect and resolve an IP conflict.

Green AP

AOS-W now supports a power saving feature, where based on NetInsight inputs, the feature dynamically enables, disables, or reduces functionality of an allocated AP to reduce the consumption of energy.

OAW-AP510 Series access points support the Green AP feature.

Support for Channels 169 and 173

AOS-W supports channel 169 and 173 for outdoor APs on 5 GHz band subject to country compliance rules.

Support for Inseego U730L 4G Modem

AOS-W 8.4.0.0 supports Inseego U730L 4G modems for Verizon network on Mobility Controllers and OAW-RAPs. OAW-AP203R, OAW-AP203RP, and OAW-AP303H access points support the U730L modem.

The U730L modem must be setup in the enterprise mode before it can be plugged into the USB port of an AP, managed device, or OmniAccess Mobility Controller.

To enable the U730L modem in enterprise mode:

1. Plug the U730L modem into a laptop running Windows or MacOS and ensure that the wireless adapter is U730L.
2. Navigate to http://my.usb/labtestinfo in a web browser.
3. Click **Enterprise Mode**.
4. Click **OK** in the pop-up window.

Wait for the U730L modem to reboot and come up before unplugging it from the laptop.

Support for Wired AP Mode

AOS-W supports **Wired AP mode** to bridge the port E1 and port E0 wired traffic.

Support for ZTE MF861 4G Modem for AT&T network

AOS-W 8.4.0.0 supports ZTE MF861 4G modems for AT&T network on Mobility Controllers and OAW-RAPs.

WIDS

You can configure to reduce the number of frames copied for the purpose of WIDS aggregate MPDU optimization from the AP system profile.

WMM DSCP mapping

Starting from this release, the WMM DSCP mapping supports IPv6 packets only in the upstream direction of the decrypt tunnel mode.

Auto-Provisioning of APs

AOS-W now allows you to automate and simplify AP provisioning by assigning pre-provisioning rules to new APs.

Configuring Preferred Uplink

Starting AOS-W 8.4.0.0 Ethernet port1 can be configured as the primary uplink and Ethernet port0 can be configured as the downlink interface, in an active-standby uplink mode of deployment. This enhancement is supported in OAW-AP210AP-318, OAW-AP374, OAW-AP375, and OAW-AP377.

AP-Wireless

Mute AP Radio

From this release, the **rf dot11a-radio-profile** and **rf dot11g-radio-profile** commands include the **am-tx-mute** parameter. Enable the **am-tx-mute** parameter to prevent an AP that operates in the Air Monitor or spectrum mode from creating spurious transmissions during AP boot. By default, the **am-tx-mute** is disabled.

NOTE

Enable the **am-tx-mute** parameter in the **rf dot11a-radio-profile** or **rf dot11g-radio-profile** command only for APs that operate in the Air Monitor or spectrum mode.

To enable the **am-tx-mute** parameter, execute the following commands:

```
(host) (config) #rf dot11a-radio-profile default
(host) (config) (rf dot11a-radio-profile "default")#am-tx-mute
```

Authentication

802.11w Support for Tunnel Mode

The 802.11w standard is now supported in tunnel mode with a Virtual AP configured with WPA3 security mode.

EAP-TLS Fragmentation

As part of 802.1X authentication, AOS-W supports EAP-TLS fragmentation in non-termination mode.

Multiple Pre-Shared Key for WLAN SSID Profile

WPA2 PSK-based deployments generally consist of a single passphrase configured as part of a WLAN SSID profile. This single passphrase is applicable for all clients that associate with the SSID. Starting from AOS-W 8.4.0.0, Multiple Pre-Shared Key (MPSK) in conjunction with ClearPass Policy Manager are supported for WPA and WPA2 PSK-based deployments. Every client connected to the WLAN SSID may have its own unique PSK.

Support for New Wi-Fi Alliance Security Enhancements

AOS-W supports new WPA3 and enhanced-open security improvements with the following features:

- WPA3
  - Simultaneous Authentication of Equals (SAE) replaces WPA2-PSK with a password based authentication resistant to dictionary attacks.
  - WPA3-Enterprise optionally adds usage of Suite-B 192-bit minimum-level security suite aligned with CNSA for enterprise networks.
- Enhanced Open replaces open unencrypted wireless networks thereby mitigating exposure of user data to passive traffic sniffing

AOS-W implements WPA3 (including the optional CNSA mode) and the optional Enhanced Open enhancement as specified in the certification programs of Wi-Fi Alliance. The OAW-AP300 SeriesOAW-AP310 Series, OAW-AP320 Series, OAW-AP340 Series, OAW-AP360 Series, OAW-AP370 Series, OAW-AP514, and OAW-AP515 access points support WPA3 and Enhanced Open.

EAP-TLS Supplicant Support

The EAP-TLS supplicant support allows you to add a Fully Qualified Domain Name (FQDN) as a suffix to an AP name or a group of APs for factory certificates.

Base OS Security

CP Firewall Limit

AOS-W now increases the limit of CP firewall rules from 32 to 96. You can now configure up to 96 firewall CP rules. A **Max CP firewall limit (96) reached configuration** error message is displayed when the maximum limit of 96 rules is reached.

Firewall Visibility

Prioritize RTP Traffic

Starting from this release, the RTP traffic is prioritized based on the DSCP value set by the end user device. This allows the RTP traffic to pass through the managed devices.

Management Users

Admin Password Recovery

Starting from this release, AOS-W allows you to disable the default password recovery feature and create an alternate password recovery user to reset the admin password.

Implementing Management User Audits

The administrator can track the following details:

- Location of the last successful login
- Date and time stamp of the last successful login
- Number of successful attempts over a period of time
- Number of unsuccessful attempts since the last successful login

Implementing Password Validation

When a PSK-based management user changes the password, a check is added to ensure that there is at least a difference of 8 characters between the new password and the old password.

Configuring Concurrent Sessions

A check is added to limit the number of concurrent sessions that an administrator account can maintain. If the admin user tries to create a new session after the maximum concurrent user sessions limit is reached, then the system displays an error message and does not allow the user to login although the login credentials entered are valid.

NOTE

This option can be configured only using the CLI.

Maintaining Standard Mandatory Notice and Consent Banner

Starting from this release, a configuration option is added to enable retaining the Login Banner on the WebUI login page until the user clicks the **I Accept** button, only after which the login prompt is displayed.

Zeroizing TPM Keys

Starting from this release, you can zeroize a cryptographic module. This involves erasing sensitive parameters such as electronically stored data, cryptographic keys, and critical security parameters from a switch or an AP to prevent disclosure of information if the equipment is permanently and irrevocably decommissioned.

VIA Client Audit

Starting from this release, when a user authenticates and accesses the VIA client, a notification with details about the last successful logon date and time stamp is provided.

Jumbo Frames

Starting from this release, Jumbo Frames is supported on Mobility Controller Virtual Appliance.

BLE

IoT Enhancements

AOS-W supports IoT applications through BLE. AOS-W supports multiple transport mechanisms, payload encoding, payload content, and periodicity of information updates. For example, some door locks from Assa Abloy use ZigBee for back-end connectivity. An AP with a USB ZigBee radio provides gateway services to relay the door lock information to a management server.

Branch Office

Using ZTP with DHCP to Provision Managed Devices

Managed devices can get the information required for provisioning from a DHCP server instead of Activate. You can use Option 43 of DHCP to broadcast the master information to the managed devices.

Enhancements to Uplink Configuration

The uplink configuration is now simplified and enhanced to configure multiple WAN paths to the VPN Concentrator for a branch office network by allowing you to specify the link type and link names.

Hub and Spoke VPN Support

AOS-W provides support for Hub and Spoke VPN which enables automatic VPN tunnel establishment with the VPN concentrators for managed devices in a branch network.

Support for Static IP Routing using Automatic VPN Tunnel

AOS-W supports forwarding of IP routes using the IPsec tunnel to VPN Concentrator that is established using the Hub and Spoke VPN configuration in a branch network.

Captive Portal

Support for Captive Portal URL VSA

Starting from this release, AOS-W supports **Aruba-Captive-Portal-URL** VSA attribute to dynamically redirect users to Captive Portal home page.

Adding AP's MAC address in the redirection URL

Starting from this release, you can include the AP's MAC address in the redirection URL when using external captive portal servers.

Cluster

EST Support for Cluster

The cluster members use enrolled certificate for IPsec tunnel authentication instead of using factory certificates.

Remote AP support with Cluster behind NAT

OAW-RAPs can map the managed device's private address to a public space by obtaining the private IP and public IP address mapping from a cluster. Therefore, the cluster behind NAT is supported with OAW-RAPs.

Scheduled Cluster Upgrade

Scheduled cluster upgrade feature allows you to schedule the upgrade to a specified time to avoid manual intervention. The cluster is upgraded automatically at the scheduled time. You can view, delete, or reschedule the scheduled cluster upgrade.

CLI Enhancements

Show user-table

If the **show user-table** command is executed from the **[mynode]** or **[mm]** prompts of the Mobility Master CLI, the following alert message is displayed:

This command is not applicable on master switch

Show ap mesh debug link-table

The **Show ap mesh debug link-table** command is introduced to display the mesh link table information for a remote mesh point or remote mesh portal.

ClientInsight

ClientInsight for AOS-W

ClientInsight is designed to support the next generation data-driven wireless network automation. It is an integration of ClientMatch and NetInsight.

High Availability

AP Ageout

The AP Ageout process now allows the switch to age out the APs based on the last activity timestamp of the AP.

IPv6 Support

IPsec Support

Starting from this release, Remote APs support IPv6 clients in Split-Tunnel forwarding mode in a VAP profile.

Aeroscout and RTLS Server Support

Starting from this release, an AP can connect to the Aeroscout or RTLS location server using a configurable IPv6 address.

MultiZone Profile

Starting from this release, you can configure an IPv6 address in one data zone of an AP MultiZone profile.

External Captive Portal

AOS-W now supports external captive portal for IPv6.

WebCC Support

Starting from this release, the WebCC feature also supports classification of IPv6 sessions on the managed device.

License Management

License Management with ASP

Starting from this release, the AOS-W License Automation feature is supported, where the Mobility Master obtains the AOS-W licenses from ASP or LMS automatically. The users need not manually add the licenses on the Mobility Master.

Mesh

Mesh Auto Role Detection

AOS-W now allows you to set **mesh auto** under **Configuration** > **Access Points** > **Provision** > **Mesh role**. Mesh auto enables auto-detection of mesh point or mesh portal based on system initialization or operation. The **mesh-auto** parameter is introduced under the **provision-ap** command to enable auto-detection of mesh using the CLI.

NetDestination

NetDestination and NetServices Alias

NetDestination and NetServices aliases can now be configured using the AOS-W 8.4.0.0 WebUI.

PPPoE

Support for Multiple PPPoE Uplinks

Starting from this release, managed devices can be configured to support the same gateway IP address over multiple PPPoE uplinks.

SES-imagotag ESL System

SES-imagotag ESL System for AOS-W

The USB aerials for SES-imagotag's Electronic Shelf Label (ESL) is now supported on OAW-AP303H, OAW-AP300 Series access points, OAW-AP310 Series access points, OAW-AP320 Series access points, OAW-AP330 Series access points, OAW-AP340 Series access points, and OAW-AP510 Series access points. The following commands are introduced as part of this feature:

- **sesimagotag-esl-channel**
- **sesimagotag-esl-serverip**
- **show ap debug esl-status**
- **show ap debug ses-esl-log**

SNMP

Support for SNMP Traps over Websocket

A switch's SNMP traps can now be sent over Websocket.

Enhancements to LinkUp and LinkDown Traps

The **IfDescr** and **IfName** objects are added to the **LinkUp** and **LinkDown** traps to include the description and name details of the interface.

Enhancements to wlxBSSIDIsup and wlxBSSIDIsdown Traps

The name of the AP is added to the **wlxBSSIDIsup** and **wlxBSSIDIsdown** traps. The output of the **show snmp trap-queue** command lists the name and MAC address of the APs associated with the BSSID.

Tunnel Node

Support for Trusted and Untrusted VLANs on a Single L2 GRE Tunnel

Starting from this release, a single IPv4 and IPv6 Layer-2 GRE tunnel can carry both trusted and untrusted VLANs.

Alcatel-Lucent Dynamic Segmentation Solution

The Dynamic Segmentation solution is Alcatel-Lucent's ability to assign policy (roles) to a wired port, based on the access method of a client. Further, using ClearPass Policy Manager, we can add context such as time-of-day and type-of-machine. The solution also provides users the ability to segment client traffic via traditional, locally switched VLANs or to tunnel traffic back to an Aruba Mobility Controller.

Starting from this release, enhancements made to the WebUI provides visibility into wired clients, tunneled switches, and so on. The Alcatel-Lucent Dynamic Segmentation solution removes the need for user VLANs to be created on the Alcatel-Lucent access switch. Instead it uses user-role based VLANs to assign roles for Dynamic Segmentation users so that user's traffic gets classified in a VLAN.

Support is extended for downloadable user roles in cluster deployments. This feature provides seamless redundancy for dynamic policy assignments.

Starting from this release, IPv6 support is available for Alcatel-Lucent Dynamic Segmentation solution.

Starting from this release, a license is required to activate the Dynamic Segmentation feature and is similar to AP licensing. If the license is not installed, switches will not be allowed to form tunnels to the Alcatel-Lucent access switch and the feature will not function.

UCC

Support for Microsoft Teams

AOS-W 8.4.0.0 can detect, classify, and prioritize voice and video services for Teams, which is the new cloud-based UCC application from Microsoft. The information for Microsoft Teams traffic is currently monitored and represented in the UCC dashboard as Skype for Business traffic because the client media session attributes are unchanged between Skype for Business and Teams.

Web Server

Backward Compatibility

AOS-W 8.4.0.0 introduces the Backward Compatibility feature that enables managed devices to receive register requests on the older HTTP port 80. This option is beneficial when managed devices and OAW-IAPs have not been upgraded to AOS-W 8.4.0.0 simultaneously in a network. When only managed devices are upgraded, users must enable this feature so that managed devices do not drop register requests received on the older HTTP port 80, which can result in service disruption.

WebUI

AP Packet Capture

AP Packet Capture feature allows you to manually start capturing AP packets on an access point that is UP and download the files using the WebUI.

AirMatch

Starting from this release, a toggle switch is added to enable the **Automatically deploy AirMatch optimizations** setting.

ARM Profile

Starting from this release, the following ARM profile configuration parameters are available only on stand-alone switch and master switch mode.

- **Assignment**

- **Allowed bands for 40 MHz channels**
- **80 MHz support**
- **Max TX EIRP**
- **Min TX EIRP**

Client Match

Starting from this release, a single check box is added to enable or disable Client Match on both 2.4 GHz and 5 GHz radio settings.

Dashboard Monitoring

New **Dashboard** is not supported in the Master switch mode.

RF Management

Starting from this release, the following RF management configuration parameters are available only on the Mobility Master mode.

- **Max Channel Bandwidth**
- **Min Channel Bandwidth**
- **Min EIRP**
- **Max EIRP**
- **eirp-offset**

Scheduled Upgrade

The AOS-W version of the managed devices or cluster members can be scheduled to upgrade at a predetermined date and time through the WebUI. The managed devices or cluster members can be scheduled to manually download and install the predetermined AOS-W image from a FTP, SCP, or TFTP server or a local file at the scheduled date and time. The date and time of a scheduled upgrade can be changed or the scheduled upgrade can be canceled through the WebUI. The WebUI displays the status of the scheduled upgrade in graphical and tabular views with details like name of managed device or cluster member, current version of AOS-W installed, version of AOS-W to install, number of access points connected to the managed device or members in a cluster.

Support for Unicode Characters

Support for unicode characters in ESSID is added.

VIA VPN Client Capability

The VIA client now provides a new Vendor Identifier string that forwards Layer-2 GRE packets containing Ethernet frames using the IPsec tunnel established with the managed device.

VIA VPN Client Visibility

The VIA client users are separately displayed on the WebUI for VPN client visibility. You can view the client users in the **Dashboard > Clients > Remote Clients** page in the WebUI.

VIA Unique Identifier

Client's MAC address is used as the unique identifier when authentication is sent to ClearPass Policy Manager.

Dashboard Monitoring

AOS-W now supports the option to delete one or more inactive APs that are either replaced or no longer used in a deployment.

Support for New Parameter in AP System Profile

Starting from this release, a new parameter, **AP USB Power mode**, is introduced to the **Advanced** accordion of the **AP system profile** option in the **Configuration** > **System** > **Profiles** page. This parameter enables or disables the USB port on various AP platforms that have external ports.

Support for Redirect-DNS

Starting from this release, you can configure and redirect the domain to a dedicated DNS server in an IPv4 and IPv6 domain.

Enhancement to the switch WebUI

Starting from this release, you can perform the following tasks on the switches using the WebUI:

- Drag and Drop
- Edit Action

This chapter describes the hardware platforms supported in AOS-W 8.4.0.0.

switch Platforms

The following table displays the switch platforms that are supported in AOS-W 8.4.0.0.

Table 3: *Supported switch Platforms in AOS-W 8.4.0.0*

switch Family	switch Model
OAW-40xx Series	OAW-4005, OAW-4008, OAW-4010, OAW-4024, OAW-4030
OAW-4x50 Series	OAW-4450, OAW-4550, OAW-4650, OAW-4750, OAW-4750XM, OAW-4850

AP Platforms

The following table displays the AP platforms that are supported in AOS-W 8.4.0.0.

Table 4: *Supported AP Platforms in AOS-W 8.4.0.0*

AP Family	AP Model
OAW-AP100 Series	OAW-AP104, OAW-AP105
OAW-AP103 Series	OAW-AP103
OAW-AP110 Series	OAW-AP114, OAW-AP115
OAW-AP130 Series	OAW-AP134, OAW-AP135
OAW-AP 170 Series	OAW-AP175AC, OAW-AP175AC-F1, OAW-AP175DC, OAW-AP175DC-F1, OAW-AP175P, OAW-AP175P-F1
OAW-AP200 Series	OAW-AP204, OAW-AP205

Table 4: *Supported AP Platforms in AOS-W 8.4.0.0*

AP Family	AP Model
OAW-AP203H Series	OAW-AP203H
OAW-AP205H Series	OAW-AP205H
OAW-AP207 Series	OAW-AP207
OAW-AP203R Series	OAW-AP203R, OAW-AP203RP
OAW-AP210 Series	OAW-AP214, OAW-AP215
OAW-AP 220 Series	OAW-AP224, OAW-AP225
OAW-AP228 Series	OAW-AP228
OAW-AP270 Series	OAW-AP274, OAW-AP275, OAW-AP277
OAW-AP300 Series	OAW-AP304, OAW-AP305
OAW-AP303 Series	OAW-AP303, OAW-AP303P
OAW-AP303H Series	OAW-AP303H
OAW-AP310 Series	OAW-AP314, OAW-AP315
OAW-AP318 Series	OAW-AP210AP-318
OAW-AP320 Series	OAW-APAP-324, OAW-AP325
OAW-AP330 Series	OAW-AP334, OAW-AP335
OAW-AP340 Series	OAW-AP344, OAW-AP345
OAW-AP360 Series	OAW-AP365, OAW-AP367
OAW-AP370 Series	OAW-AP374, OAW-AP375, OAW-AP377
OAW-AP387 Series	OAW-AP387

Table 4: *Supported AP Platforms in AOS-W 8.4.0.0*

AP Family	AP Model
OAW-AP510 Series	OAW-AP514, OAW-AP515
OAW-RAP155 Series	OAW-RAP155, OAW-RAP155P
OAW-RAP100 Series	OAW-RAP108, OAW-RAP109
OAW-RAP3 Series	OAW-RAP3WN, OAW-RAP3WNP

Virtual Platforms

The following Mobility Master Hardware Appliance and Mobility Master Virtual Appliance platforms that are supported in AOS-W 8.4.0.0.

- MM-HW-1K
- MM-HW-5K
- MM-HW-10K
- MM-VA-50
- MM-VA-500
- MM-VA-1K
- MM-VA-5K
- MM-VA-10K

The following the Mobility Controller Virtual Appliance platforms that are supported in AOS-W 8.4.0.0.

- MC-VA-10
- MC-VA-50
- MC-VA-250
- MC-VA-1K

Chapter 4
Regulatory Updates

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.

For a complete list of countries and the regulatory domains in which the APs are certified for operation, refer to the Downloadable Regulatory Table or the DRT Release Notes at businessportal2.alcatel-lucent.com.

The following default DRT file version is part of AOS-W 8.4.0.0:

- DRT-1.0_67861

This chapter describes the issues resolved in AOS-W 8.4.0.0.

Table 5: *Resolved Issues in AOS-W 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
149222	**Symptom:** The WebUI of a Mobility Master did not display any devices. The fix ensures that the **local-ip** related commands are restricted only to /mm path. **Scenario:** This issue occurred when a user configured a managed device from the **/mm/mynode** node hierarchy using CLI. This issue was observed in the WebUI of Mobility Masters running AOS-W 8.0.0.0 or later versions.	IPsec	All platforms	AOS-W 8.0.0.0	AOS-W 8.4.0.0
154096	**Symptom:** The channel of a virtual AP was inconsistent after a radar event was detected. This issue is resolved by allowing a managed device to change the channel when a virtual AP is created and a radar event is detected on the channel. **Scenario:** This issue occurred when a virtual AP in bridge-always forwarding mode had disconnected from a managed device detected a radar event on the channel and selected a new channel. This issue was observed in OAW-AP300 Series access points running AOS-W 8.2.0.0.	AP Regulatory	OAW-AP300 Series access points	AOS-W 8.2.0.0	AOS-W 8.4.0.0
157199	**Symptom:** An AP crashed unexpectedly. The log file lists the reason for the event as **kernel BUG at kernel/timer.c:869!**. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue was observed in OAW-AP225 access points running AOS-W 8.4.0.0.	AP-Wireless	OAW-AP225 access points	AOS-W 8.4.0.0	AOS-W 8.4.0.0
159973	**Symptom:** Certificates loaded on a managed device failed to synchronize between Mobility Master and the standby Mobility Master. The fix ensures that the certificates loaded on a managed device are synchronized successfully. **Scenario:** This issue was observed in Mobility Masters running AOS-W 8.1.0.0 or later versions.	Certificate Manager	All platforms	AOS-W 8.1.0.0	AOS-W 8.4.0.0

Table 5: *Resolved Issues in AOS-W 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
161891	**Symptom:** An AP crashed and rebooted unexpectedly. The log file listed the reason for the event as **Reboot caused by kernel panic: Fatal exception**. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue occurred when clustering was enabled. This issue was observed in OAW-AP200 Series access points running AOS-W 8.2.0.0 or later versions.	AP-Wireless	OAW-AP200 Series access points	AOS-W 8.2.0.0	AOS-W 8.4.0.0
162623	**Symptom:** The output of the **show ap arm history ap-name <ap-name>** command did not display a radar detection event for an AP. The fix ensures that the output of the **show ap arm history ap-name <ap-name>** command displays a radar detection event when a radar event is detected for an AP. **Scenario:** This issue was observed in APs running AOS-W 8.2.0.0.	ARM	All platforms	AOS-W 8.2.0.0	AOS-W 8.4.0.0
165804	**Symptom:** The HTTP security header was not detected on ports 8080 or 8088 in a managed device. This issue is resolved by enabling the HTTP security header in the **httpd.conf** file. **Scenario:** This issue was observed in managed devices running AOS-W 8.4.0.0.	switch-Platform	All platforms	AOS-W 8.4.0.0	AOS-W 8.4.0.0
165908	**Symptom:** A Mobility Master crashed and rebooted unexpectedly. The log file listed the reason for the event as **Control Processor Kernel Panic**. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue occurred due to a softlock causing the crash. This issue was observed in OAW-4x50 Series switches running AOS-W 8.2.0.0 or later versions. **Duplicates:** 170224, 171074, 171396, 173372, 174322, 174370, 174917, 175009, 177151, 177457, 177662, 178307, 180558, 180741, 181173, 183588, 185596, 186993, 187232, 187418	switch-Platform	OAW-4x50 Series switches	AOS-W 8.2.0.0	AOS-W 8.4.0.0
166800 173645 176278	**Symptom:** False detections of type-5 radars were triggered in the FCC domain. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue was observed in APs running AOS-W 8.0.0.0 or later versions.	AP-Wireless	All platforms	AOS-W 8.0.0.0	AOS-W 8.4.0.0

Table 5: *Resolved Issues in AOS-W 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
169256 175610 176992 182160	**Symptom:** A managed device did not learn some of the ARP response that it received from an AP. The fix ensures that the managed device learns the ARP responses. **Scenario:** This issue occurred when the session table was corrupted during synchronization of high value sessions between active UAC and standby UAC. Hence, some ARP sessions had the **d** or deny flag and the managed device dropped the corresponding ARP responses. This issue was observed in managed devices running AOS-W 8.1.0.2 or later versions.	switch-Datapath	All platforms	AOS-W 8.1.0.2	AOS-W 8.4.0.0
170249 172066 175830 175931 176688 179004 181990 182574 182752	**Symptom:** A client was unable to connect to an AP that reported 100% CPU utilization. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue was observed in access points running AOS-W 8.3.0.1.	AP-Wireless	All platforms	AOS-W 8.3.0.1	AOS-W 8.4.0.0
172217	**Symptom:** The **write memory** command did not show the configurations that were committed. The fix ensures that the **write memory** command works as expected. **Scenario:** This issue occurred when a user configured ACLs, VLANs, and interface configuration and issued the **write memory** command. This issue was observed in managed devices running AOS-W 8.2.0.1.	Configuration	All platforms	AOS-W 8.2.0.1	AOS-W 8.4.0.0
173353	**Symptom:** The **TM** column (time used by MGMT frames) in the output of the **show ap radio-summary dot11g** command always displayed 100. The fix ensures that the actual value is displayed. **Scenario:** This issue was observed in access points running AOS-W 8.0.0.0 or later versions.	AP-Platform	All platforms	AOS-W 8.0.0.0	AOS-W 8.4.0.0
173788 174490 178159	**Symptom:** Clients switched between APs or sometimes to the other band on the same AP. The fix ensures that the clients age out normally when roaming. **Scenario:** This issue occurred when a client sent packets that indicated it is about to roam but attempted to re-associate with the same AP. This issue was observed in APs running AOS-W 8.2.0.0 or later versions.	AP-Wireless	All platforms	AOS-W 8.2.0.0	AOS-W 8.4.0.0

Table 5: *Resolved Issues in AOS-W 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
174799	**Symptom:** A managed device displayed the **Module Authentication is busy. Please try later** message when the **show firewall dns-names** command was executed. The fix ensures that the managed device processes the **show firewall dns-names** command as expected. **Scenario:** This issue occurred when multiple DNS names were configured in a managed device and one DNS name had too many IP addresses associated with it. This issue was observed in managed devices running AOS-W 8.4.0.0.	Base OS Security	All platforms	AOS-W 8.4.0.0	AOS-W 8.4.0.0
175087	**Symptom:** An AP buffered packets for a long time and replies to the **ping** command was delayed. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue was observed in OAW-AP207 access points running AOS-W 8.0.0.0.	AP-Wireless	OAW-AP207 access points	AOS-W 8.0.0.0	AOS-W 8.4.0.0
175138	**Symptom:** The **Configurations > Services > Guest provisioning** page appears blank and non-editable. The fix ensures that the **Guest Provisioning** page is displayed correctly. **Scenario:** This issue occurred when a user entered the **&** character in the email field. This issue was observed in managed devices running AOS-W 8.2.0.2 or later versions.	Guest Provisioning	All platforms	AOS-W 8.2.0.2	AOS-W 8.4.0.0
175140	**Symptom:** OAW-AP325 access points were not coming up on the managed device. This issue was resolved by fixing IP reassembly code. **Scenario:** This issue occurred because of an issue in the reassembly code of the managed devices. This issue was observed in Mobility Master Virtual Appliances running AOS-W 8.0.0.0 or later versions.	switch -Datapath	OAW-AP325 access points	AOS-W 8.2.0.2	AOS-W 8.4.0.0
175550	**Symptom:** A user could not disable the security logging for the **aaa** process using the **logging security process aaa subcat aaa level debugging** command. The fix ensures that a user can disable the security logging for the **aaa** process. **Scenario:** This issue was observed in managed devices running AOS-W 8.2.0.2 or later versions.	Configuration	All platforms	AOS-W 8.2.0.2	AOS-W 8.4.0.0

Table 5: *Resolved Issues in AOS-W 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
175669	**Symptom:** The **show ap active** command did not show any flag for an AP that was operating in restricted mode because of 802.3af PoE (POE-AF). This issue is resolved by showing the **p** flag in the **show ap active** command for an AP that operates in restricted mode. **Scenario:** This issue was observed in access points running AOS-W 8.0.0.0	AP-Platform	All platforms	AOS-W 8.0.0.0	AOS-W 8.4.0.0
176105	**Symptom:** The configuration of an AP was lost and the AP rebooted repeatedly. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue occurred due to a missing boot environment configuration. This issue was observed in OAW-AP205 access points running AOS-W 8.0.0.0 or later versions.	AP-Platform	OAW-AP205 access points	AOS-W 8.0.0.0	AOS-W 8.4.0.0
176330 177428	**Symptom:** The **Diagnostics > Technical Support > Copy Files** page of the WebUI displayed a success message although the TFTP file transfer failed. The fix ensures that the WebUI displays the correct message. **Scenario:** This issue occurred when a user attempted to copy a file using TFTP. This issue was observed in Mobility Master running AOS-W 8.2.0.0 or later versions.	Configuration	All platforms	AOS-W 8.2.0.0	AOS-W 8.4.0.0
176434	**Symptom:** The Captive Portal page was not displayed correctly on client devices. The fix ensures that the Nginx collects the correct configuration rule. **Scenario:** This issue occurred when the Nginx collected the wrong configuration rule while searching for the CSS file. This issue was observed in Mobility Master Virtual Appliance running AOS-W 8.2.0.2 or later versions.	Captive Portal	All platforms	AOS-W 8.2.0.2	AOS-W 8.4.0.0
176444	**Symptom:** The startup wizard did not allow adding licenses to a stand-alone switch. The fix ensures that the licenses are added successfully. **Scenario:** This issue was observed in stand-alone switches running AOS-W 8.2.1.0.	switch - Platform	All platforms	AOS-W 8.2.1.0	AOS-W 8.4.0.0
176622	**Symptom:** The UCC data export function was missing from the AOS-W version running on a Mobility Master. This issue was resolved by adding the **show ucc call-info cdrs filelog** command, allowing the output of the command to be exported as a .csv file. **Scenario:** This issue was observed in Mobility Masters running AOS-W 8.0.0.0 or later versions.	UCC	All platforms	AOS-W 8.0.0.0	AOS-W 8.4.0.0

Table 5: *Resolved Issues in AOS-W 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
176774 177016	**Symptom:** An AP crashed and rebooted unexpectedly. The log file listed the reason for the event as **Kernel panic - not syncing: Fatal exception in interrupt**. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue was observed in OAW-AP225 access points running AOS-W 8.0.0.0.	AP-Wireless	OAW-AP225 access points	AOS-W 8.0.0.0	AOS-W 8.4.0.0
176902	**Symptom:** Managed devices dropped ARP response from silent clients. The fix ensures that managed devices do not drop ARP responses from silent clients. **Scenario:** This issue occurred when the protect ARP spoofing feature was enabled and a managed devices deleted the datapath user entries of silent clients. This issue was observed in managed devices running AOS-W 8.0.0.0.	switch-Datapath	All platforms	AOS-W 8.0.0.0	AOS-W 8.4.0.0
176927	**Symptom:** High channel utilization and beacon failures were observed in some APs, and the issues continued to be displayed until the APs were rebooted. The fix ensures that these performance issues are not observed in the APs. **Scenario:** This issue was observed in APs running AOS-W 8.3.0.0 or later versions.	AP-Wireless	All platforms	AOS-W 8.3.0.0	AOS-W 8.4.0.0
176930	**Symptom:** An AirGroup server that was connected as a Per User Tunneled Node client was not showing up as an AirGroup server on the Mobility Master. This issue is resolved by using tunneled_user GSM channel for subscription. **Scenario:** This issue occurred when a tunneled_node GSM channel was used for user subscription. This issue was observed in managed devices running AOS-W 8.2.1.0 or later versions.	SDN-Platform	All platforms	AOS-W 8.2.1.0	AOS-W 8.4.0.0
176952	**Symptom:** The **/flash/upload** directory was available to unauthenticated users. The fix ensures that the **/flash/upload** directory sends a **permission denied** message for unauthenticated users. **Scenario:** This issue was observed in managed devices running AOS-W 8.2.0.0.	switch-Platform	All platforms	AOS-W 8.2.0.0	AOS-W 8.4.0.0

Table 5: *Resolved Issues in AOS-W 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
176957	**Symptom:** The user-name attribute in a RADIUS response message was not populated in the user table during captive portal authentication. The fix ensures that managed devices update the username in the user table with the value received as an attribute in a RADIUS response. **Scenario:** This issue was observed in managed devices running AOS-W 8.0.0.0.	Radius	All platforms	AOS-W 8.0.0.0	AOS-W 8.4.0.0
177017	**Symptom:** An AP crashed and rebooted unexpectedly. The log file listed the reason for the event as **Kernel panic - not syncing: Fatal exception in interrupt**. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue was observed in OAW-AP225 access points running AOS-W 8.0.0.0.	AP-Wireless	OAW-AP225 access points	AOS-W 8.0.0.0	AOS-W 8.4.0.0
177045 180877	**Symptom:** An AP rebooted unexpectedly. The log file listed the reason for the event as **external watchdog reset**. The fix ensures that the AP works as expected. **Scenario:** This issue occurred when radio in the AP tried to reset PHY and the driver was stuck. This issue was observed in OAW-AP203H and OAW-AP207 access points running AOS-W 8.3.0.0 or later versions.	AP-Platform	OAW-AP203H and OAW-AP207 access points	AOS-W 8.3.0.0	AOS-W 8.4.0.0
177162	**Symptom:** The position of an ACL that was configured on the default **user-role** was changed unexpectedly. The fix ensures that a managed device retains the ACLs in the correct positions. **Scenario:** This issue occurred when a managed device was reloaded and the ACLs were loaded in the wrong sequence at startup. This issue was observed in managed devices running AOS-W 8.3.0.0.	Configuration	All platforms	AOS-W 8.3.0.0	AOS-W 8.4.0.0
177420	**Symptom:** The HSTS Security header was missing in the HTTP response from the Mobility Master WebUI. The fix ensures that the HSTS header is included in the HTTP response. **Scenario:** This issue was not limited to any specific switch model or AOS-W release version.	Web Server	All platforms	AOS-W 8.2.0.1	AOS-W 8.4.0.0
177618	**Symptom:** The **sapd** process crashed in an AP. This issue is resolved by not sending the nodelist to the AP when there are two APs configured with the same name. **Scenario:** This issue occurred when two APs had the same AP name. This issue was observed in access points running AOS-W 8.2.0.2.	AP-Platform	All platforms	AOS-W 8.2.0.2	AOS-W 8.4.0.0

Table 5: *Resolved Issues in AOS-W 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
177653	**Symptom:** The console log of an AP listed multiple user-miss and resource temporarily unavailable messages. The log on AMP listed multiple sessions for the same client connected to the Remote AP using split-tunnel forwarding mode. The fix ensures that the AP console log does not unnecessarily list user-miss and resource temporarily unavailable messages. **Scenario:** This issue was observed in access points running AOS-W 8.0.0.0.	OAW-RAP	All platforms	AOS-W 8.0.0.0	AOS-W 8.4.0.0
177770	**Symptom:** APs crashed and rebooted unexpectedly. The log files listed the reason for the event as **Kernel panic - not syncing: FW ASSERT at tx_send_setup_ppdu_params**. Enhancements to the wireless driver resolved the issue. **Scenario:** This issue occurred when an ADDBA response was received with a window size of 0 as some of the retried frames were not flushed from the frame queue. This issue was observed in OAW-AP335 access points running AOS-W 8.2.0.2 or later versions	AP-Wireless	OAW-AP335 access points	AOS-W 8.2.0.2	AOS-W 8.4.0.0
177788	**Symptom:** A client experienced a slow network or network connectivity issue although the number of sessions in the AP did not reach the maximum value. The fix ensures that clients get a better network experience. **Scenario:** This issue was observed in OAW-AP315 access points running AOS-W 8.0.0.0.	AP Datapath	OAW-AP315 access points	AOS-W 8.0.0.0	AOS-W 8.4.0.0
177789	**Symptom:** When an incorrect password was entered in an external captive portal multiple times, the error message string **errmsg=Authentication%20failed** was appended to the URL multiple times. The fix ensures that the **errmsg=Authentication%20failed** is appended to the URL once. **Scenario:** This issue occurred when external captive portal was used with a non-cppm server. This issue was observed in managed devices running AOS-W 8.2.1.0 or later versions.	Captive Portal	All platforms	AOS-W 8.2.1.0	AOS-W 8.4.0.0

Table 5: *Resolved Issues in AOS-W 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
177796	**Symptom:** Internal captive portal was displayed incorrectly when the client attempted to log in with blank credentials, using external captive portal. The issue is resolved by displaying an appropriate reason for authentication failure if blank credentials are used to login. **Scenario:** This issue occurred when the client tried to log in with external captive portal using either a blank username, blank password, or both. This issue was observed in managed devices running AOS-W 8.2.0.2 or later versions.	Captive Portal	All platforms	AOS-W 8.2.0.2	AOS-W 8.4.0.0
177891	**Symptom:** The **Authentication** process in a managed device crashed unexpectedly and a client was disconnected. This issue is resolved by ensuring that the role name is valid and not empty. **Scenario:** This issue occurred when a CPPM role download was configured but the role name was invalid or empty. This issue was observed in OAW-4650 switches running AOS-W 8.2.0.2 or later versions.	Base OS Security	OAW-4650 switches	AOS-W 8.2.0.2	AOS-W 8.4.0.0
178032	**Symptom:** An AP was unresponsive for a short period (up to 1.5 seconds) which led to client disconnections. The fix ensures that active-scan in an AP returns to its home channel and clients retain connectivity. **Scenario:** This issue occurred when active-scan was enabled in an AP. With active-scan enabled, an AP left its home channel to scan another channel. However, the AP did not return to its home channel and aborted the channel scanning after 1.5 seconds. While the AP was scanning another channel, clients lost connectivity with the AP and attempted to find another AP. The AP did not complete the channel scan successfully and did not report neighbors in the active scanning channels (2.4 GHz and non-DFS 5 GHz channels). This issue was observed in access points running AOS-W 8.2.0.0.	AP-Wireless	All platforms	AOS-W 8.2.0.0	AOS-W 8.4.0.0
178114 180746	**Symptom:** A OAW-RAP failed to come up. The fix ensures that the Remote AP works as expected. **Scenario:** This issue occurred when the MTU was not adjusted automatically. This issue was observed in OAW-AP305 access points running AOS-W 8.0.1.0 or later versions.	AP Datapath	OAW-AP305 access points	AOS-W 8.0.1.0	AOS-W 8.4.0.0

Table 5: *Resolved Issues in AOS-W 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
178119	**Symptom**: A client was unable to connect to the AP. The fix ensures that the client is able to connect to the AP. **Scenario**: This issue occurred when the AP stopped broadcasting the configured SSID. This issue was observed in OAW-AP225 and OAW-AP325 access points running AOS-W 8.0.0.0 or later versions.	AP-Wireless	OAW-AP225 and OAW-AP325 access points	AOS-W 8.0.0.0	AOS-W 8.4.0.0
178182 179612	**Symptom:** A user experienced intermittent Skype call drops. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue occurred when an AP stopped transmitting packets for a few seconds to track power save status. This issue was observed in access points running AOS-W 8.0.0.0.	AP-Wireless	All platforms	AOS-W 8.0.0.0	AOS-W 8.4.0.0
178221 189525	**Symptom:** The **show airgroup aps** command does not list AirGroup APs on a managed device. The fix ensures that the **show airgroup aps** command lists the AirGroup APs. **Scenario:** This issue was observed in managed devices running AOS-W 8.3.0.0.	AirGroup	All platforms	AOS-W 8.3.0.0	AOS-W 8.4.0.0
178247 178268	**Symptom:** The VIA connection did not work with IKEv2 and SSL-fallback mode. The fix ensures that the VIA connection works with IKEv2 and SSL-fallback mode. **Scenario:** This issue was observed in managed devices running AOS-W 8.3.0.0.	IPsec	All platforms	AOS-W 8.3.0.0	AOS-W 8.4.0.0
178284	**Symptom:** A Mobility Master Virtual Appliance lost network connectivity. The fix ensures that the Mobility Master Virtual Appliance does not lose its network connection. **Scenario:** This issue was observed in Mobility Master Virtual Appliances running AOS-W 8.2.0.2 or later versions.	switch-Datapath	All platforms	AOS-W 8.2.0.2	AOS-W 8.4.0.0
178324	**Symptom:** The 5 GHz channel of an outdoor AP switched to channel 46 which was excluded in the regulatory-domain profile. This issue is resolved by sending only the outdoor channel EIRP list for an outdoor AP. **Scenario:** This issue occurred when an outdoor AP randomly picked up a channel designated for use by an indoor AP from the exhaustive EIRP list. This issue was observed in outdoor access points running AOS-W 8.2.0.0.	AP-Platform	All platforms	AOS-W 8.2.0.0	AOS-W 8.4.0.0

Table 5: *Resolved Issues in AOS-W 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
178329	**Symptom:** The **show ap active** command on an AP displayed an incorrect 5 GHz channel. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue occurred when an AP detected a radar within the 10 seconds interval between a lost connection and a Wi-Fi shutdown. After the connection was re-established, the AP displayed a different channel in the **show ap active** command output. This issue was observed in OAW-AP205 access points running AOS-W 8.0.0.0 or later versions.	AP-Wireless	OAW-AP205 access points	AOS-W 8.0.0.0	AOS-W 8.4.0.0
178351	**Symptom:** A specified GigabitEthernet interface in a managed device did not support maximum transmit rate in kilobits per second. The fix ensures that the maximum transmit rate settings also support kilobits per second. **Scenario:** This issue was observed in managed devices running AOS-W 8.2.1.0 or later versions.	switch-Datapath	All platforms	AOS-W 8.2.1.0	AOS-W 8.4.0.0
178357	**Symptom:** An AP crashed and rebooted unexpectedly. The log files listed the reason for the event as **FW ASSERT at rc_get_nss_from_ chainmask()**. Improvements to the wireless driver resolved the issue. **Scenario:** This issue was observed in OAW-AP300 Series access points running AOS-W 8.2.1.0 or later versions.	AP-Wireless	OAW-AP300 Series access points	AOS-W 8.2.1.0	AOS-W 8.4.0.0
178390	**Symptom:** A few APs failed to switch over to another managed device in a cluster. The fix ensures that the APs switch over to another managed device successfully. **Scenario:** This issue occurred when a managed device rebooted. This issue was observed in managed devices running AOS-W 8.2.1.0.	Cluster-Manager	All platforms	AOS-W 8.2.1.0	AOS-W 8.4.0.0
178394	**Symptom:** When an incorrect password was entered in an external captive portal, **errmsg=Authentication%20failed** was appended incorrectly to the URL and the login page did not load correctly. The fix ensures that the login page loads correctly after an authentication failure. **Scenario:** This issue occurred when external captive portal was used with a non-ClearPass Policy Manager server. This issue was observed in managed devices running AOS-W 8.2.1.0 or later versions.	Captive Portal	All platforms	AOS-W 8.2.1.0	AOS-W 8.4.0.0

Table 5: *Resolved Issues in AOS-W 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
178407 178459 176490 178469 179289	**Symptom:** Clients were unable to send packets that were larger than 978 bytes over an IPsec tunnel. The fix ensures that the clients are able to send packets that are larger than 978 bytes over an IPsec tunnel. **Scenario:** This issue was observed in access points running AOS-W 8.2.0.1 or later versions.	AP Datapath	OAW-AP320 Series access points	AOS-W 8.2.0.1	AOS-W 8.4.0.0
178498	**Symptom:** AirGroup users could use Apple TVs on different AP groups. The fix ensures that the AirGroup users show all available information for the user. **Scenario:** This issue occurred when AirGroup was enabled in centralized mode with auto association. This issue was observed in managed devices running AOS-W 8.2.0.2 or later versions in a cluster setup.	AirGroup	All platforms	AOS-W 8.2.0.2	AOS-W 8.4.0.0
178405	**Symptom:** The output of the **show ap active** command displayed incorrect 5 GHz Channel. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue occurred when the radar detection was set to random, causing the command output to display an incorrect channel. This issue was observed in OAW-AP100 Series access points running AOS-W 8.0.0.0 or later versions.	AP-Wireless	OAW-AP100 Series access points	AOS-W 8.0.0.0	AOS-W 8.4.0.0
178419 180044 181059	**Symptom:** The mDNS RADIUS requests were sent with the NAS-IP address in reverse order to the ClearPass Policy Manager. This issue is resolved by correcting the endianess of the IP address. **Scenario:** This issue occurred because of wrong endianess. This issue was observed in managed devices running AOS-W 8.3.0.0 or later versions.	AirGroup	All platforms	AOS-W 8.3.0.0	AOS-W 8.4.0.0
178609	**Symptom:** A managed device retained the port-channel **trusted** and **trunk allowed vlan** in the setup configuration instead of receiving it from the Mobility Master. This lead to a connectivity issue. The fix ensures that the managed device retains the correct port-channel configuration that is received from the Mobility Master. **Scenario:** This issue occurred when the port-channel in the setup configuration of the managed device was different from the configuration that was received from the Mobility Master. This issue was observed in managed devices running AOS-W 8.2.0.2 or later versions.	Configuration	All platforms	AOS-W 8.2.0.2	AOS-W 8.4.0.0

Table 5: *Resolved Issues in AOS-W 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
178633	**Symptom:** An AP console displayed the **fsl_dpa ethernet.17 eth0: Err FD status = 0x00000020** error message. The fix ensures that the AP works as expected. **Scenario:** This issue occurred when the AP received bad checksum uplink packets. This issue was observed in OAW-AP335 access points running AOS-W 8.3.0.0 or later versions.	AP Datapath	OAW-AP335 access points	AOS-W 8.3.0.0	AOS-W 8.4.0.0
178709	**Symptom:** The **Ipsec-map name** drop-down list was blank under the **Configuration** > **Roles & Policies** > **Policies** > **Route Policy** > **New forwarding Rule** table. This issue is resolved by adding the drop-down options and also providing a text box for adding the IPsec map name manually. **Scenario:** This issue was observed in managed devices running AOS-W 8.2.1.0 or later versions.	WebUI	All platforms	AOS-W 8.2.1.0	AOS-W 8.4.0.0
178719 179348 180890 186926	**Symptom:** Managed devices crashed and rebooted unexpectedly. The log files listed the reason for the event as **Reboot Cause: Hardware Watchdog Reset (Intent:cause:register ee:ee:50:4).** **Scenario:** This issue occurred when the CPU memory was full. This issue was observed in managed devices running AOS-W 8.2.1.0 or later versions.	switch-Platform	All platforms	AOS-W 8.2.1.0	AOS-W 8.4.0.0
178758	**Symptom:** A split-tunnel user was stuck with large idle time on a managed device. This issue is resolved by aging out the station when a client is not responsive after associating with an AP but does not complete the 4-way handshake in bridge, split-tunnel, or D-tunnel forwarding modes. **Scenario:** This issue occurred because of stale entries in the client-table of the driver. This issue was observed in access points running AOS-W 8.0.0.0.	AP-Wireless	All platforms	AOS-W 8.0.0.0	AOS-W 8.4.0.0
178760 179950 189003	**Symptom:** OAW-IAPs connected to a managed device obtained reversed IP addresses. The fix ensures that the OAW-IAPs get the IP addresses in the correct format. **Scenario:** This issue occurred when a MAC address of an OAW-IAP was configured with a remote-ip address in the remote whitelist database using the **whitelist-db rap add mac-address** command. This issue was observed in Mobility Controller Virtual Appliance running AOS-W 8.3.0.0 or later versions.	CPsec	All platforms	AOS-W 8.3.0.0	AOS-W 8.4.0.0

Table 5: *Resolved Issues in AOS-W 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
178764 183584	**Symptom:** The **Syslogd** process in an AP crashed and generated core files frequently. The fix ensures that the crash does not occur. **Scenario:** This issue was observed in OAW-AP300 Series, OAW-AP310 Series, OAW-AP303 Series, OAW-AP303H Series, OAW-AP318 Series, OAW-AP320 Series, OAW-AP330 Series, OAW-AP340 Series, OAW-AP360 Series, and OAW-AP370 Series access points running AOS-W 8.2.1.1 or later versions.	AP-Platform	OAW-AP300 Series, OAW-AP310 Series, OAW-AP303 Series, OAW-AP303H Series, OAW-AP318 Series, OAW-AP320 Series, OAW-AP330 Series, OAW-AP340 Series, OAW-AP360 Series, and OAW-AP370 Series access points	AOS-W 8.2.1.1	AOS-W 8.4.0.0
178839	**Symptom:** When an AP with static channel or EIRP was rebooted, the opmode changed on other Dual 5 GHz APs as well. This resulted in 2.4 GHz APs getting EIRP computed for 5 GHz AP and vice-versa. The fix ensures that the auto opmode switching is disabled for the AP when static EIRP or static channel settings are detected on the AP. **Scenario:** This issue occurred under the following conditions: ■ The Dual 5G APs were configured with static channels or EIRP. ■ The AP was rebooted. ■ The value of **dual-5ghz-mode** was set to **automatic** in the **ap system-profile**. This issue was observed in APs running AOS-W 8.3.0.0.	AirMatch	All platforms	AOS-W 8.3.0.0	AOS-W 8.4.0.0
178870	**Symptom:** Changes did not reflect in DPI classification when a single rule was deleted in the custom application. The fix ensures that the changes made in the custom application reflect in the DPI classification. **Scenario:** This issue occurred when multiple rules were configured within the custom application and a single rule was deleted. This issue was observed in managed devices running AOS-W 8.3.0.0.	DPI	All platforms	AOS-W 8.3.0.0	AOS-W 8.4.0.0

Table 5: *Resolved Issues in AOS-W 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
179047	**Symptom:** An AP crashed unexpectedly. The log file listed the reason for the event as **PC is at wlc_apps_bss_ps_off_done+0x54/0x118 [wl] and LR is at wlc_mbss_shm_ssid_upd+0x2f8/0x330 [wl]**. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue was observed in OAW-AP345 access points running AOS-W 8.3.0.0.	AP-Wireless	OAW-AP345 access points	AOS-W 8.3.0.0	AOS-W 8.4.0.0
179107	**Symptom:** A stand-alone switch displayed the error message, **Module licensemgr is busy. Please try later**. The fix ensures that a validation check is added to prevent addition of unsupported licenses. **Scenario:** This issue was observed in Mobility Controller Virtual Appliance running AOS-W 8.1.0.4 or later versions.	Licensing	All platforms	AOS-W 8.1.0.4	AOS-W 8.4.0.0
179124	**Symptom:** A managed device displayed the following error messages: **ERRS |wms| WMS Event Table Cleanup: The system call to pthread_create() has failed with error [Resource temporarily unavailable.** Enhancements to memory management resolved the issue. **Scenario:** This issue occurred because of a memory leak. This issue was observed in managed devices running AOS-W 8.2.1.0.	Air Management - IDS	All platforms	AOS-W 8.2.1.0	AOS-W 8.4.0.0
179151	**Symptom:** Mobility Master failed to upgrade from AOS-W 8.2.0.2 to AOS-W 8.2.1.0 version. The fix ensures that the Mobility Master is able to upgrade to the latest AOS-W version. **Scenario:** This issue occurred when the AOS-W version was copied to an incorrect directory causing an error in upgrading the Mobility Master. This issue occurred in Mobility Masters running AOS-W 8.2.0.2.	Image Upgrade	All platforms	AOS-W 8.2.0.2	AOS-W 8.4.0.0
179215	**Symptom:** AirMatch deployed the APs with wider channel bandwidth when the number of configured channels was less than 3. The fix ensures that AirMatch deploys the APs with correct channel bandwidth. **Scenario:** This issue occurred when frequency reuse channel bandwidth selection logic did not scale well when the number of channels were less than 3. This issue was observed in APs running AOS-W 8.2.0.0 or later versions.	AirMatch	All platforms	AOS-W 8.2.0.0	AOS-W 8.4.0.0
179347	**Symptom:** The default node did not change its path when the group name was changed in a Mobility Master. **Scenario:** This issue was observed in Mobility Master Virtual Appliance running AOS-W 8.3.0.0 or later versions.	Configuration	All platforms	AOS-W 8.3.0.0	AOS-W 8.4.0.0

Table 5: *Resolved Issues in AOS-W 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
179360	**Symptom:** A managed device displayed the **Module L2TP is busy. Please try later error** message and did not provide an L2TP IP address. The fix ensures that the managed device provides an L2TP IP address and works as expected. **Scenario:** This issue occurred when the **show vpdn l2tp local pool** command was executed. This issue was observed in managed devices running AOS-W 8.0.0.0.	IPsec	All platforms	AOS-W 8.0.0.0	AOS-W 8.4.0.0
179408	**Symptom:** The log of a Mobility Master displayed the **|localdb| |wl-sync| Skipping db_sync** message. The fix ensures that the Mobility Master does not log the message for unnecessary managed devices. **Scenario:** This issue occurred when a Mobility Master synchronized the whitelist database to managed devices by using the MAC address of the managed device. This issue was observed in OAW-4650 switches running AOS-W 8.0.0.0.	802.1X	OAW-4650 switches	AOS-W 8.0.0.0	AOS-W 8.4.0.0
179483	**Symptom:** A user was unable to delete **folder _config1** folder on the Mobility Master WebUI. This issue is resolved by adding a check at the end of datastore initialization. **Scenario:** This issue occurred due to dummy nodes created in the datastore that were not deleted after a executing a configuration difference. This issue was observed in a Mobility Master Virtual Appliances running AOS-W 8.2.1.0.	Configuration	Mobility Master Virtual Appliance	AOS-W 8.2.1.0	AOS-W 8.4.0.0
179485	**Symptom:** Mobility Master rebooted unexpectedly. The log file listed the reason for the event as **profmgr** process crash. The fix ensures that Mobility Masters work as expected. **Scenario:** This issue was observed in Mobility Masters running AOS-W 8.2.1.0.	L2 Forwarding	All platforms	AOS-W 8.2.1.0	AOS-W 8.4.0.0
179627	**Symptom:** The **FPAPPs** process was stuck in a managed device. The fix ensures that the managed device works as expected. **Scenario:** This issue occurred when the initial full-setup wizard was used to switch a OAW-4450 switch that was running in stand-alone mode to a managed device and an invalid netmask was entered. This issue was observed in OAW-4450 switches running AOS-W 8.2.1.0.	L2 Forwarding	OAW-4450 switches	AOS-W 8.2.1.0	AOS-W 8.4.0.0

Table 5: *Resolved Issues in AOS-W 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
179656	**Symptom:** An AP crashed and rebooted unexpectedly. The log file listed the reason for the event as **Kernel panic - not syncing: Fatal exception in interrupt**. The fix ensures that the AP works as expected. **Scenario:** This issue occurred when the mesh role in the AP provisioning profile was set to mesh point in OAW-AP300 Series access points running AOS-W 8.3.0.0 or later versions.	AP-Wireless	OAW-AP300 Series access points	AOS-W 8.3.0.0	AOS-W 8.4.0.0
179837 182068	**Symptom:** The usage time was incorrectly displayed in the **Dashboard > Usage** page. There was a time difference when compared to the switch's clock that was set through NTP. The fix ensures that the correct usage time is displayed. **Scenario:** This issue occurred because the DST was not considered when calculating the usage time. This issue was observed in Mobility Masters running AOS-W 8.3.0.0 or later versions.	WebUI	All platforms	AOS-W 8.3.0.0	AOS-W 8.4.0.0
179867	**Symptom:** An AP switched to APM mode unexpectedly. This issue is resolved by checking the AP certificate information if the new bandwidth has channels available during bandwidth upgrade. If a channel is not available for the new bandwidth, a debug message is logged with the reason for the unsuccessful bandwidth upgrade. **Scenario:** This issue occurred during bandwidth upgrade when AirMatch changed the min-channel-bandwidth in the 5 GHz radio profile of an AP to a value that did not match the AP certificate information for the country code. This issue was observed in access points running AOS-W 8.2.1.0.	AirMatch	All platforms	AOS-W 8.2.1.0	AOS-W 8.4.0.0
179869	**Symptom:** A managed device did not display any validation error message when the user deleted role default session ACL by executing the **no access-list session apprf-<role name>-sacl** command. The fix ensures that the appropriate validation message is displayed when the user tries to delete the role default session ACL. **Scenario:** This issue occurred when the system flags applicable to the user role were erased on reboot of the Mobility Master. This issue was observed in managed devices running AOS-W 8.2.1.0 or later versions in a Mobility Master-Managed Device topology.	Configuration	All platforms	AOS-W 8.2.1.0	AOS-W 8.4.0.0

Table 5: *Resolved Issues in AOS-W 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
179936 189520	**Symptom:** A few APs stopped responding to pings randomly. The fix ensures that the AP works as expected. **Scenario:** This issue was observed in OAW-AP105 access points running AOS-W 8.0.0.0 or later versions.	AP-Wireless	OAW-AP105 access points	AOS-W 8.0.0.0	AOS-W 8.4.0.0
179942	**Symptom:** A client was not able to send or receive traffic to or from an AP. The fix ensures that the AP sends a PAPI message to the User Anchor Controller (UAC) and the clients are able to send or receive traffic to or from an AP. **Scenario:** This issue occurred when the **station management** process in an AP sent a PAPI message to the AP Anchor Controller (AAC) instead of the UAC. This issue was observed in a cluster topology running AOS-W 8.2.1.0 with 802.11r enabled.	Station Management	All platforms	AOS-W 8.2.1.0	AOS-W 8.4.0.0
179970	**Symptom:** The **flags** column in the output of the **show ap bss-table** displayed wrong characters for AP Ethernet wired clients. This issue is resolved by setting the first bytes of the flags to null before checking if an Ethernet wired port is enabled. **Scenario:** This issue occurred when both wireless radios were disabled and the wired Ethernet port was enabled but the flags were not initialized. This issue was observed in managed devices running AOS-W 8.0.0.0.	Station Management	All platforms	AOS-W 8.0.0.0	AOS-W 8.4.0.0
180033	**Symptom:** When the port was connected to a 1 Gbps switch, some OAW-AP340 Series access points failed to enable the Eth0 interface. The fix ensures that the Ethernet link is stable after the switch is restarted by physically turning off the power supply and turning it on again. **Scenario:** This issue occurred only when the switch was restarted by turning off the power to the switch. If you have not upgraded to AOS-W 8.3.0.3, restart the switch without interrupting the power supply as a workaround. This issue was observed in OAW-AP340 Series access points running AOS-W 8.3.0.0 or later versions	AP-Platform	OAW-AP340 Series access Points	AOS-W 8.3.0.0	AOS-W 8.4.0.0

Table 5: *Resolved Issues in AOS-W 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
180045 185407	**Symptom:** The **Configuration** > **Roles and Policies** page of the WebUI displayed an incorrect position for the policies for each user role. The fix ensures that the WebUI displays the correct position of the role policies. **Scenario:** This issue was observed in managed devices running AOS-W 8.3.0.0 or later versions.	Configuration	All platforms	AOS-W 8.3.0.0	AOS-W 8.4.0.0
180118	**Symptom:** An AP broadcasted an SSID that was configured with opensystem encryption as a WEP SSID. The fix ensures that the AP broadcasts the SSID with opensystem encryption as expected. **Scenario:** This issue occurred when the **sapd** process failed to copy the BSSID and MAC address as part of storing HA keys. This issue was observed in access points running AOS-W 8.4.0.0.	AP-Platform	All platforms	AOS-W 8.0.0.0	AOS-W 8.4.0.0
180146 188443	**Symptom:** 802.1X clients failed RADIUS authentication. The fix ensures that the clients do not fail RADIUS authentication. **Scenario:** This issue occurred when termination was enabled on the managed device and the TLS handshake failed. This issue was observed in managed devices running AOS-W 8.2.0.0 or later versions.	802.1X	All platforms	AOS-W 8.2.0.0	AOS-W 8.4.0.0
180340	**Symptom:** An AP failed to boot using APBoot version 1.2.5.0. The fix ensures that the AP works as expected. **Scenario:** This issue was observed in OAW-AP135 access points running AOS-W 8.3.0.0 or later versions.	AP-Wireless	OAW-AP135 access points	AOS-W 8.3.0.0	AOS-W 8.4.0.0
180398	**Symptom:** A cluster upgrade did not go beyond the first node in a cluster. This issue is resolved by updating the correct model name of the device during upgrade. **Scenario:** This issue occurred when a wrong model name was applied to a device during upgrade. This issue was observed in managed devices running AOS-W 8.2.1.0.	Configuration	All platforms	AOS-W 8.2.1.0	AOS-W 8.4.0.0

Table 5: *Resolved Issues in AOS-W 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
180400	**Symptom:** The derived VLAN of a client was changed to a different VLAN. This issue is resolved by not synchronizing the registration information of the client. Hence, MAC authentication occurs for the first time after a client disconnects and reconnects. The VLAN is cached for reuse during the next iteration. **Scenario:** This issue occurred when a client disconnected and reconnected back to the Standby User Anchor Controller (S-UAC) after a cluster failover. This issue was observed in a cluster topology with managed device running AOS-W 8.2.1.0 or later versions.	Cluster-Manager	All platforms	AOS-W 8.2.1.0	AOS-W 8.4.0.0
180489	**Symptom:** The CLI-based upgrade of a managed device failed with the **Timed out, Try again** error message. The fix ensures that CLI-based upgrade of a managed device works as expected. **Scenario:** This issue occurred in a slow network connection when the **copy scp** command failed to download the AOS-W image after 15 minutes. This issue was observed in managed devices running AOS-W 8.2.1.0.	Image Upgrade	All platforms	AOS-W 8.2.1.0	AOS-W 8.4.0.0
180496 180615 183615 185103 185484 185485 186458 186990 188060	**Symptom:** AirGroup lost all the learned server and user details and also failed to learn any new user or server. The fix ensures that AirGroup learns all users and servers appropriately. **Scenario:** This issue occurred when AirGroup was enabled in centralized mode. This issue was observed in managed devices running AOS-W 8.2.1.1 or later versions.	AirGroup	All platforms	AOS-W 8.2.1.1	AOS-W 8.4.0.0
180601 184241 186662	**Symptom: mDNS** process crashes on a Mobility Master. The fix ensures that the **mDNS** process does not crash. **Scenario:** This issue occurred because of memory corruption. This issue was observed in Mobility Masters running AOS-W 8.2.1.0 or later versions.	AirGroup	All platforms	AOS-W 8.2.1.0	AOS-W 8.4.0.0
180879	**Symptom:** Active client entries were incorrectly deleted from AirGroup. The fix ensures that only the stale client entries are deleted. **Scenario:** This issue occurred because the **mDNS** service incorrectly identified the active client entries as stale entries. This issue was observed in Mobility Masters running AOS-W 8.2.0.0 or later versions.	AirGroup	All platforms	AOS-W 8.2.0.0	AOS-W 8.4.0.0

Table 5: *Resolved Issues in AOS-W 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
181043	**Symptom:** APs crashed and rebooted unexpectedly. The fix ensures that the APs work as expected. **Scenario:** This issue occurred because of retransmitted PAPI messages. This issue was observed in OAW-AP225 access points running AOS-W 8.0.0.0 or later versions.	Station Management	OAW-AP225 access points	AOS-W 8.0.0.0	AOS-W 8.4.0.0
181143	**Symptom:** The same product key was generated when the Mobility Master Virtual Appliance or Mobility Controller Virtual Appliance was cloned. This issue is resolved by generating the product key based on the UUID of the system. **NOTE:** If a cloned Mobility Master Virtual Appliance or Mobility Controller Virtual Appliance that runs any version lower than AOS-W 8.2.2.0 was upgraded to AOS-W 8.2.2.0 and higher, AOS-W 8.3.0.2 and higher, or AOS-W 8.4.0.0 and higher, in the respective releases, the serial number and passphrase were changed and all licenses associated with the older serial number were invalidated. Migrate or regenerate the existing licenses for the new serial number after the upgrade. Contact Alcatel-Lucent Technical Support before the upgrade. **Scenario:** This issue occurred when an OVA-based Mobility Master Virtual Appliance or Mobility Controller Virtual Appliance was deployed, an OVF template was exported, and the exported OVF template was deployed. This issue was observed in Mobility Controller Virtual Appliance or Mobility Master Virtual Appliance running AOS-W 8.2.0.0.	switch-Platform	All platforms	AOS-W 8.2.0.0	AOS-W 8.4.0.0
181221	**Symptom:** Clients were unable to connect to the managed device. This issue is resolved by adding the entries to the route-cache table when the router IP table buffer overflows. **Scenario:** This issue occurred when enforce DHCP was enabled and route IP table buffer overflowed. This issue was observed in Mobility Masters running AOS-W 8.2.1.0 or later versions.	switch-Datapath	All platforms	AOS-W 8.2.1.0	AOS-W 8.4.0.0
181355	**Symptom:** The **mDNS** process crashed on a managed device. The fix ensures that the managed device works as expected. **Scenario:** This issue occurred because the hash table used to store MAC address was corrupt due to a race condition. This issue was observed in managed devices running AOS-W 8.3.0.0.	AirGroup	All platforms	AOS-W 8.3.0.0	AOS-W 8.4.0.0

Table 5: *Resolved Issues in AOS-W 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
181418 183863	**Symptom:** The ISAKMP process crashed unexpectedly in a managed device. The fix ensures that the managed device works as expected. **Scenario:** This issue is observed in managed devices running AOS-W 8.0.1.0 or later versions.	IPsec	All platforms	AOS-W 8.0.1.0	AOS-W 8.4.0.0
181440 182153	**Symptom:** A Mobility Master on Hyper V took longer than usual to boot. The fix ensures that the Mobility Master boots as expected. **Scenario:** This issue occurred when the **rngd** process was not running. This issue was observed in a Mobility Master running AOS-W 8.3.0.0.	switch-Platform	All platforms	AOS-W 8.3.0.0	AOS-W 8.4.0.0
181564	**Symptom:** A OAW-RAP lost the gateway ARP after using split-tunnel mode virtual AP. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue occurred when the OAW-RAP missed caching the ARP data for a specific gateway. This issue was observed in OAW-RAPs running AOS-W 8.0.0.0 or later versions.	OAW-RAP	All platforms	AOS-W 8.0.0.0	AOS-W 8.4.0.0
181553	**Symptom:** A managed device crashed when the AP was downloading a build image. The fix ensures that the managed device does not crash in such occurrences. **Scenario:** This issue was observed in managed devices connected to OAW-AP325 access points that downloaded the AOS-W 8.4.0.0 build image.	switch-Platform	All platforms	AOS-W 8.4.0.0	AOS-W 8.4.0.0
181606	**Symptom:** The output of the **show ap debug log** command displayed the **Bridge entry insertion failure** error message. The fix ensures that the error message is not displayed. **Scenario:** This issue was observed in OAW-AP225 and OAW-AP335 access points running AOS-W 8.3.0.0 or later versions.	AP Datapath	OAW-AP225 and OAW-AP335 access points	AOS-W 8.3.0.0	AOS-W 8.4.0.0
181615	**Symptom:** Mobility Masters lost licenses if the Mobility Master was unplugged within 3 hours of adding the license and there were no configuration changes made on the Mobility Master. The fix ensures that the database is backed up every time the write memory command is executed. **Scenario:** This issue occurred because the database backup was not triggered when the write memory command was not executed. This issue is not limited to any specific platform or AOS-W version.	Configuration	All platforms	AOS-W 8.3.0.0	AOS-W 8.4.0.0

Table 5: *Resolved Issues in AOS-W 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
181630	**Symptom:** User was not able to disable the **openflow-profile** on a managed device. The fix ensures that the **openflow-profile** is enabled by default. **Scenario:** This issue occurred when user disabled the **openflow-profile** at a configuration level lower than /md. This issue was observed in managed devices running AOS-W 8.2.1.1 or later versions.	SDN	All platforms	AOS-W 8.2.1.1	AOS-W 8.4.0.0
181678	**Symptom:** Same license key was displayed multiple times on a managed device when the **show license** command was executed. **Scenario:** This issue was observed in managed devices running AOS-W 8.2.1.0 or later versions.	Licensing	All platforms	AOS-W 8.2.1.0	AOS-W 8.4.0.0
181721 178075	**Symptom:** Download speeds were less than normal. The fix ensures that higher download speeds are achieved even in noisy conditions. **Scenario:** This issue occurred in extremely noisy environments on 2.4 GHz channels. This issue was observed in OAW-AP300 Series access points connected to a OAW-4010 switch.	AP-Wireless	All platforms	AOS-W 8.0.0.0	AOS-W 8.4.0.0
181729	**Symptom:** The **show running-config** command did not list an ACL although the **show configuration effective** command listed the same ACL. The fix ensures that the **show running-config** command lists the ACL. **Scenario:** This issue was observed in managed devices running AOS-W 8.2.0.0.	Base OS Security	All platforms	AOS-W 8.2.0.0	AOS-W 8.4.0.0
181773	**Symptom:** Managed devices rebooted unexpectedly. The log file listed the reason for the event as **Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:4)**. The fix ensures that the managed devices work as expected. **Scenario:** This issue was observed in managed devices running AOS-W 8.2.1.0 or later versions.	switch-Datapath	All platforms	AOS-W 8.2.1.0	AOS-W 8.4.0.0
181801	**Symptom:** APs are unable to auto-negotiate Ethernet speed correctly with the switch. The fix ensures that the Ethernet speed and duplex setting are taken directly from the switch. **Scenario:** This issue occurred because of an inadequate cable. This issue was observed in OAW-AP205 access points running AOS-W 8.0.0.0 or later versions.	AP-Wireless	OAW-AP205 Access Points	AOS-W 8.0.0.0	AOS-W 8.4.0.0

Table 5: *Resolved Issues in AOS-W 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
182049	**Symptom:** A client lost connectivity with an AP. The fix ensures that a client does not lose connectivity with an AP. **Scenario:** This issue occurred when the position of a validuser ACL deny rule was changed. This issue was observed in managed devices running AOS-W 8.2.1.1.	Configuration	All platforms	AOS-W 8.2.1.1	AOS-W 8.4.0.0
182248 182524	**Symptom:** Although the cluster node was up, the cluster upgrade failed with the **Cannot upgrade cluster as cluster node is down** error message. The fix ensures that the cluster upgrade completes successfully. **Scenario:** This issue occurred when a Mobility Master was upgraded and reloaded and a managed device reconnected back to the Mobility Master. The AOS-W version on the Mobility Master and the managed device was different and the managed device ignored the active master IP address information that was sent by the Mobility Master. This issue was observed in a topology with active and standby Mobility Masters when both active and standby Mobility Masters were upgraded to AOS-W 8.2.1.1 while the managed devices were running AOS-W 8.2.1.0 as cluster members.	Configuration	All platforms	AOS-W 8.2.1.1	AOS-W 8.4.0.0
182352	**Symptom:** An AP did not take the EIRP settings from the radio profile and transmit with high EIRP. The fix ensures that the feasible opmode list does not contain a blank entry, the AP takes the EIRP settings from the radio profile, and transmits with the correct EIRP. **Scenario:** This issue occurred when a blank entry was stored in the feasible opmode list for radio. This issue was observed in access points running AOS-W 8.2.1.1, managed devices running AOS-W 8.2.0.0, and Mobility Master running AOS-W 8.3.0.0.	AirMatch	All platforms	AOS-W 8.2.1.1	AOS-W 8.4.0.0
182486	**Symptom:** A client was not able to access the internet. The fix ensures that the VLAN ID will be taken from the route-cache entry for the PPPoE gateway. **Scenario:** This issue occurred when the PPPoE interface included the **ip nat outside** configuration. This issue was observed in managed devices running AOS-W 8.2.1.0.	VLAN	All platforms	AOS-W 8.2.1.0	AOS-W 8.4.0.0

Table 5: *Resolved Issues in AOS-W 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
182590	**Symptom:** An error message, **Error reading transceiver ID Prom on 0/0/0** was displayed when the Small Form-factor Pluggable transceiver (SFP module) was connected to the switch. The fix ensures that the SFP modules are supported. **Scenario:** This issue was observed in stand-alone switches running AOS-W 8.3.0.0.	switch-Platform	All platforms	AOS-W 8.3.0.0	AOS-W 8.4.0.0
182604	**Symptom:** The **Illegal operation on the interface** error was observed when the user tried to add or remove a trusted VLAN on the managed device. The fix ensures that the error message is not displayed. **Scenario:** This issue occurred when the user tried to configure the GigabitEthernet interface with a valid port range. This issue was observed in managed devices running AOS-W 8.2.0.0 or later versions.	VLAN	All platforms	AOS-W 8.2.0.0	AOS-W 8.4.0.0
182612 182372	**Symptom:** Clients were unable to resolve ARP requests. The fix ensures that the clients are able to resolve ARP requests. **Scenario:** This issue occurred because the AP memory utilization rate was high, leading to drop in client traffic. This issue was observed in access points running AOS-W 8.3.0.0.	AP Datapath	All platforms	AOS-W 8.3.0.0	AOS-W 8.4.0.0
182683	**Symptom:** A blank redirect page was displayed when **WISPr** client was trying to configure Captive Portal on a managed device. The fix ensures that the correct page is displayed when Captive Portal is configured on a managed device. **Scenario:** This issue occurred when a managed device was experiencing high CPU utilization. This issue was observed in managed devices running AOS-W 8.1.0.0 or later versions.	WISPr Interoperability	All platforms	AOS-W 8.1.0.0	AOS-W 8.4.0.0

Table 5: *Resolved Issues in AOS-W 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
182780	**Symptom:** The output of few **show datapath** commands displays the MAC address in upper case. This fix ensures that the output is displayed in lower case. **Scenario:** This issue occurred when the following show datapath commands were issued. This issue is not restricted to any switch or AOS-W versions. ■ **show datapath route-cache** ■ **show datapath station** ■ **show datapath bridge** ■ **show datapath firewall-agg-sess** ■ **show datapath tunnel** ■ **show datapath tunnel station-list** ■ **show datapath user** ■ **show datapath user rad-counter**	switch- Datapath	All platforms	AOS-W 8.2.1.0	AOS-W 8.4.0.0
182909	**Symptom:** An AP displayed incorrect ACL index value on the user datapath. The fix ensures that the correct value is displayed. **Scenario:** This issue was observed in APs connected to a stand-alone switch running AOS-W 8.0.0.0 or later versions.	AP Datapath	All platforms	AOS-W 8.0.0.0	AOS-W 8.4.0.0
182941	**Symptom:** A managed device displayed the following alert message: **Expecting string of length 1 to 32**. This issue was resolved by increasing the string length to 255 characters. **Scenario:** This issue occurred when a user attempted to add a trunk VLAN of string length greater than 32 characters. This issue was observed in managed devices running AOS-W 8.2.1.0 or later versions.	VLAN	All platforms	AOS-W 8.2.1.0	AOS-W 8.4.0.0
182981	**Symptom:** XML data was displayed when the show license aggregate command was executed from API. The fix ensures that the JSON output is displayed instead of the XML data. **Scenario:** This issue occurred when the command was run over the API on the Mobility Master. This issue was observed in Mobility Masters running AOS-W 8.3.0.1.	Configuration	All platforms	AOS-W 8.3.0.1	AOS-W 8.4.0.0
183015	**Symptom:** An AP deauthenticated a client immediately after authenticating it. The fix ensures that the AP retains the authenticated clients. **Scenario:** This issue was observed in access points running AOS-W 8.3.0.0.	AP Datapath	All platforms	AOS-W 8.3.0.0	AOS-W 8.4.0.0

Table 5: *Resolved Issues in AOS-W 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
183034	**Symptom:** Clients got disconnected after roaming although auto connect was enabled. The fix ensures that the clients do not get disconnected. **Scenario:** This issue was observed in access points running AOS-W 8.0.1.0 or later versions in an IPv6 deployment.	AP-Platform	All platforms	AOS-W 8.2.1.1	AOS-W 8.4.0.0
183134	**Symptom:** The **profmgr** process crashed multiple times. The fix ensures that the Mobility Master Virtual Appliance works as expected **Scenario:** This issue occurred when SSID is defined on one node and Virtual APs or the AP groups were defined on lower nodes. This issue was observed in Mobility Master Virtual Appliance running AOS-W 8.3.0.0.	AP-Platform	All platforms	AOS-W 8.3.0.0	AOS-W 8.4.0.0
183464 190191	**Symptom:** Some APs failed to display interference though there was high RF interference. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue was observed in OAW-AP200 Series access points running AOS-W 8.0.0.0 or later versions.	AP-Wireless	OAW-AP200 Series access points	AOS-W 8.0.0.0	AOS-W 8.4.0.0
183929	**Symptom:** The Edge browser did not redirect a user to the correct page after the user successfully completed Captive Portal authentication. This issue is resolved by redirecting the user to the correct page after a successful Captive Portal authentication. **Scenario:** This issue occurred when the redirect URI was not stored while storing the original URL. After successfully completing Captive Portal authentication, the user was redirected back the original URL instead of the URL with the redirect URI. This issue was observed in managed devices running AOS-W 8.2.1.1.	Captive Portal	All platforms	AOS-W 8.2.1.1	AOS-W 8.4.0.0
184082 184587	**Symptom:** Some APs failed to switch between Backup LMS IP and LMS IP. The fix ensures that the APs switch between Backup LMS IP and LMS IP successfully. **Scenario:** This issue was observed in Mobility Masters running AOS-W 8.3.0.0 or later versions.	AP-Platform	All platforms	AOS-W 8.3.0.0	AOS-W 8.4.0.0

Table 5: *Resolved Issues in AOS-W 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
184426	**Symptom:** An AP deauthenticated a client unexpectedly. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue occurred because of an unexpected internal ageout and long connection delay. This issue was observed in OAW-AP300 Series, OAW-AP310 Series, OAW-AP320 Series, OAW-AP330 Series, OAW-AP360 Series, and OAW-AP370 Series access points running AOS-W 8.2.1.0.	AP-Wireless	OAW-AP300 Series, OAW-AP310 Series, OAW-AP320 Series, OAW-AP330 Series, OAW-AP360 Series, and OAW-AP370 Series access points	AOS-W 8.2.1.0	AOS-W 8.4.0.0
184786	**Symptom:** APs were not broadcasting on Virtual APs and on start up, displayed D flag, in the output of the command **show ap database**, indicating that the AP configuration either had errors or was missing, after managed devices were rebooted in a cluster. The fix ensures that the comparison of named VLAN is not case sensitive. **Scenario:** This issue was observed in managed devices running AOS-W 8.2.0.2 or later versions in a cluster setup.	AP-Platform	All platforms	AOS-W 8.2.0.2	AOS-W 8.4.0.0
184868	**Symptom:** The SNMP query for **OID: wlsxSysExtInternalTemparature** was displaying 0 for a Mobility Master. The fix ensures that the query displays the actual temperature. **Scenario:** This issue was observed in OAW-4x50 switches running AOS-W 8.2.1.1.	SNMP	OAW-4x50 switches	AOS-W 8.2.1.1	AOS-W 8.4.0.0
185082	**Symptom:** The Active AP Load Balancing information is not displayed in the output when the **show lc-cluster group-profile** command was executed. The fix ensures that the Active AP Load Balancing information is displayed. **Scenario:** This issue was observed in managed devices in a cluster setup are running AOS-W 8.2.1.1 or later versions.	Cluster-Manager	All platforms	AOS-W 8.2.1.1	AOS-W 8.4.0.0
185309	**Symptom:** Clients connected to OAW-AP345 access points were unable to go online using TKIP encryption. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue occurred when the clients were connected through bridge mode SSID using TKIP encryption. This issue was observed in OAW-AP345 access points running AOS-W 8.3.0.0.	AP-Wireless	OAW-AP345 access points	AOS-W 8.3.0.0	AOS-W 8.4.0.0

Table 5: *Resolved Issues in AOS-W 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
185508	**Symptom:** The WebUI was unresponsive after adding an additional license. The fix ensures that the WebUI works as expected. **Scenario:** This issue occurred when a user attempted to add an additional license and the Mobility Master already had 230 licenses. This issue was observed in Mobility Masters running AOS-W 8.3.0.1.	Licensing	All platforms	AOS-W 8.3.0.1	AOS-W 8.4.0.0
185597	**Symptom:** The output of the **show switches** command displayed the IPv6 address of a standby Mobility Master as **none**. The fix ensures that the output of the **show switches** command displays the IPv6 address of the standby Mobility Master. **Scenario:** This issue occurred when the **show switches** command was executed on a Mobility Master. This issue was observed in Mobility Masters running AOS-W 8.2.1.1.	Configuration	All platforms	AOS-W 8.2.1.1	AOS-W 8.4.0.0
185679 187734 188214 189144 189191 191414	**Symptom:** An AP crashed and rebooted unexpectedly. The fix ensures that the AP works as expected. **Scenario:** This issue was observed in APs running AOS-W 8.2.2.0 or later versions.	AP-Platform	All platforms	AOS-W 8.2.2.0	AOS-W 8.4.0.0
186110	**Symptom:** The configuration synchronization failed and the status of the synchronization displayed **CONFIG Failure**. This issue is resolved by changing the user-role **default-iap-user-role** as a read only role. **Scenario:** This issue occurred when the **default-iap-user-role** was edited. This issue was observed in Mobility Masters running AOS-W 8.3.0.1 or later versions.	Base OS Security	All platforms	AOS-W 8.3.0.1	AOS-W 8.4.0.0
186224	**Symptom:** Clients could not connect to a bridge mode virtual AP after a VLAN assignment failure. The fix ensures that the clients connect to the virtual APs. **Scenario:** This issue occurred when the VLAN in a Mobility Master was removed causing subsequent deauthentication of all the clients associated with the virtual APs. This issue was observed in Mobility Masters running AOS-W 8.0.0.0 or later versions.	Station Management	All platforms	AOS-W 8.0.0.0	AOS-W 8.4.0.0

Table 5: *Resolved Issues in AOS-W 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
186399	**Symptom:** ClientMatch steered clients to the same radio because of load balancing even though the BSSID of the radio and the AP were same. The fix ensures that ClientMatch does not steer the clients to the same radio. **Scenario:** This issue was observed in managed devices running AOS-W 8.2.1.1.	ARM	All platforms	AOS-W 8.2.1.1	AOS-W 8.4.0.0
186509	**Symptom:** A client failed dynamic WEP reauthentication with an AP. This issue is resolved by not dropping the unencrypted Rx EAPOL frames when dynamic WEP reauthentication is enabled. **Scenario:** This issue occurred when the wireless driver dropped unencrypted Rx EAPOL frames after the WEP key was set. This issue was observed in OAW-AP305, OAW-AP315, and OAW-AP335 access points operating in bridge mode and running AOS-W 8.2.1.1	AP-Wireless	All platforms	AOS-W 8.2.1.1	AOS-W 8.4.0.0
186608	**Symptom:** The **datapath** process in a managed device crashed while initiating a Skype call from a wireless client. The fix ensures that the managed device works as expected. **Scenario:** This issue was observed in managed devices running AOS-W 8.3.0.1 or later versions.	switch-Datapath	All platforms	AOS-W 8.3.0.1	AOS-W 8.4.0.0
186815	**Symptom:** The CPPM profile entries were not updated in the node hierarchies when the CPPM profile was configured in AirGroup server. The fix ensures that the CPPM profile entries are updated in different node hierarchies. **Scenario:** This issue occurred when the user added or deleted RFC 3576 servers by executing the **airgroupprofile cppm rfc-3576- server <rfc-3576-server>** command. This issue was observed in Mobility Master running AOS-W 8.2.1.1 or later versions.	AirGroup	All platforms	AOS-W 8.2.1.1	AOS-W 8.4.0.0
187027	**Symptom:** A user cannot import a CSV file that contained guest information on a managed device. This issue is resolved by removing the extra space from the sponsor email address field in the CSV file during file extraction. **Scenario:** This issue occurred when a sponsor email address was given as an input in the CSV file and an extra space was added to the sponsor email address field during the file extraction. This issue was observed in managed devices running AOS-W 8.3.0.0 or later versions.	Guest Provisioning	All platforms	AOS-W 8.3.0.0	AOS-W 8.4.0.0

Table 5: *Resolved Issues in AOS-W 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
187191	**Symptom:** Wireless clients were not added as OpenFlow hosts in the Mobility Master. Enhancements to the wireless driver resolved the issue. **Scenario:** This issue was observed in Mobility Masters running AOS-W 8.2.1.1 or later versions.	SDN	All platforms	AOS-W 8.2.1.1	AOS-W 8.4.0.0
187364	**Symptom:** The configuration changes made to the system-defined **validuser** ACL rules were not applied upon reboot of a managed device. The fix ensures that the configuration changes in the ACL rule are applied instead of the default ACL rules. **Scenario:** This issue was observed in managed devices running AOS-W 8.2.1.1 or later versions.	Base OS Security	All platforms	AOS-W 8.2.1.1	AOS-W 8.4.0.0
187390	**Symptom:** VoIP clients faced connectivity issues when IPv6 was enabled. The fix ensures that UCC functionalities work as expected in an IPv6 cluster. **Scenario:** This issue occurred when UCC flows were processed using the IPv6 address instead of the IPv4 address of the managed device in an IPv6 cluster. This issue was observed in managed devices running AOS-W 8.2.1.1 or later versions.	UCC	All platforms	AOS-W 8.2.1.1	AOS-W 8.4.0.0
187696	**Symptom:** A Mobility Master failed to install correct netdestination into datapath causing guest captive portal to fail. The fix ensures that the Mobility Master sends netdestination updates to datapath. **Scenario:** This issue occurred when: ■ netdestination was used in captive portal ACL. ■ there were multiple PAPI failures. This issue was observed in Mobility Masters running AOS-W 8.3.0.1 or later versions.	Base OS Security	All platforms	AOS-W 8.3.0.1	AOS-W 8.4.0.0
187735	**Symptom:** The configured MTU value of an AP was incorrect in the managed device. The fix ensures that the correct MTU value is reflected in the managed device. **Scenario:** This issue occurred when the AP was rebooted after configuring the SAP MTU in the AP system-profile. This issue was observed in access points running AOS-W 8.1.0.0 or later versions.	Mesh	All platforms	AOS-W 8.1.0.0	AOS-W 8.4.0.0

Table 5: *Resolved Issues in AOS-W 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
187744 189352 191419	**Symptom:** APs were rebooting randomly. The log files for the event listed the reason as Reboot caused by kernel panic: Fatal exception. The fix ensures that the AP works as expected. **Scenario:** This issue occurred when EIRP table was not sent to the AP when either 2G or 5G channel list was empty. This issue was observed in APs running AOS-W 8.3.0.0 or later versions.	AP Regulatory	All platforms	AOS-W 8.3.0.0	AOS-W 8.4.0.0
187745	**Symptom:** AP requested for less Poe-at power in the LLDP negotiation, which lead to insufficient power. The fix ensures that the AP requests for 25.5W instead of 20.8W for Poe-at LLDP negotiation. **Scenario:** This issue occurred when the AP requested for 20.8W. This issue was observed in OAW-AP377 running AOS-W 8.3.0.2 or later versions.	AP-Wireless	OAW-AP377 access points	AOS-W 8.3.0.2	AOS-W 8.4.0.0
187819 188349	**Symptom:** An AP crashed and rebooted unexpectedly. The log files listed the reason for the reboot as **Reboot caused by kernel panic: Watchdog timeout received**. The fix ensures that the AP works as expected. **Scenario:** This issue occurred due to a large number of debug messages printed in the log files. This issue was observed in OAW-AP335 access points running AOS-W 8.2.1.1 or later versions.	AP-Wireless	OAW-AP335 access points	AOS-W 8.2.1.1	AOS-W 8.4.0.0
187865	**Symptom:** User was able to telnet the access point although the telnet option was disabled in the ap-system profile. The fix ensures that the user cannot telnet the access point if the option is disabled in the ap-system profile. **Scenario:** This issue was observed in stand-alone OAW-4650 switches running AOS-W 8.3.0.0 or later versions.	AP-Platform	OAW-4650 switches	AOS-W 8.3.0.0	AOS-W 8.4.0.0
187939	**Symptom:** The **authentication** process in a managed device leaked memory and generated a crash report. Improvements to memory management resolved this issue. **Scenario:** This issue occurred when the 802.1X authentication load was high. This issue was observed in OAW-AP377 running AOS-W 8.3.0.2 or later versions.	802.1X	All platforms	AOS-W 8.4.0.0	AOS-W 8.4.0.0

Table 5: *Resolved Issues in AOS-W 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
188025	**Symptom:** PEFNG license count was displayed incorrectly in the **Mobility Master > Configuration > License > License usage > PEF** column. The fix ensures that the correct license count is displayed. **Scenario:** This issue was observed in Mobility Master running AOS-W 8.2.1.1 or later versions.	WebUI	All platforms	AOS-W 8.2.1.1	AOS-W 8.4.0.0
188037	**Symptom:** Mesh APs were coming up unlicensed on a Data zone. The fix ensures that for a mesh AP in a MultiZone, no licenses are consumed in Data zone but in a Primary zone, the mesh APs consume licenses even if there are no Virtual APs for that mesh AP. **Scenario:** This issue occurred when MultiZone is enabled and a virtual AP is assigned to the Data zone. This issue was observed in APs connected to managed devices running AOS-W 8.2.1.1 or later versions in Mesh mode.	AP-Platform	All platforms	AOS-W 8.2.1.1	AOS-W 8.4.0.0
188135 188987	**Symptom:** The **STM** process in a managed device displayed the **Dynamic BSS tunnel could not be setup for bssid** error message. The fix ensures that the error message is not displayed on the managed device. **Scenario:** This issue was observed in managed devices running AOS-W 8.2.1.1 or later versions.	AP-Platform	All platforms	AOS-W 8.2.1.1	AOS-W 8.4.0.0
188497	**Symptom:** A managed device sent RSSI AMON data to **mgmt-server destinations** even though the location was disabled in **mgmt-server profile**. The fix ensures that the managed device does not send RSSI AMON data to **mgmt-server destination**. **Scenario:** This issue was observed in managed devices running AOS-W 8.2.1.1 or later versions.	AMON	All platforms	AOS-W 8.2.1.1	AOS-W 8.4.0.0
188517	**Symptom:** Multiple APs crashed unexpectedly. The fix ensures that the APs work as expected. **Scenario:** This issue was observed in APs running AOS-W 8.3.0.0 or later versions.	AP-Wireless	All platforms	AOS-W 8.3.0.0	AOS-W 8.4.0.0
188601	**Symptom:** A managed device was unable to synchronize the configuration with the Mobility Master. This issue is resolved by not allowing the deletion of any system-generated ACL from the user role. **Scenario:** This issue occurred during the deletion of a system-generated ACL from a user role. This issue was observed in managed devices running AOS-W 8.2.1.0.	Base OS Security	All platforms	AOS-W 8.2.1.0	AOS-W 8.4.0.0

Table 5: *Resolved Issues in AOS-W 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
188659	**Symptom:** An SNMP walk reported incorrect values for Broadcast/ Multicast packets. The fix ensures that the correct values are reported during SNMP walk. **Scenario:** This issue was observed in Mobility Masters running AOS-W 8.3.0.3 or later versions.	SNMP	All platforms	AOS-W 8.3.0.3	AOS-W 8.4.0.0
188667 190096 190508	**Symptom:** APs were unable to boot on a stand-alone switch and APs rebooted with the reason, **Error:RC_ERROR_ISAKMP_N_CERT_ SELFSIGNED_VERIFY_FAILED**. Enhancements to the wireless driver resolved the issue. **Scenario:** This issue occurred when CPsec was enabled. This issue was observed in OAW-AP303 access points running AOS-W 8.3.0.0 or later versions on a Mobility Controller Virtual Appliance.	AP-Platform	OAW-AP303 access points	AOS-W 8.3.0.0	AOS-W 8.4.0.0
188978	**Symptom:** During RADIUS session timeout, fixed 802.1X deauthentication occurred followed by 802.1X reauthentication. This issue is resolved by correctly populating the termination-action in the RADIUS AV pairs. **Scenario:** This issue occurred when the termination-action in the RADIUS AV pairs was not populated correctly. This issue was observed in managed devices running AOS-W 8.4.0.0.	802.1X	All platforms	AOS-W 8.4.0.0	AOS-W 8.4.0.0
189024	**Symptom:** An AP did not receive an IP address when its ENET1 port was used as uplink and the ENET0 port was simultaneously connected to a client. The fix ensures that the ENET1 port is default uplink when both ENET0 and ENET1 ports are L2 connected. Also, the ENET0 port can be provisioned as default uplink too. **Scenario:** This issue was observed in OAW-AP210AP-318, OAW-AP374, OAW-AP375, and OAW-AP377 access points running AOS-W 8.3.0.0.	AP-Platform	OAW-AP210AP-318, OAW-AP374, OAW-AP375, and OAW-AP377 access points	AOS-W 8.3.0.0	AOS-W 8.4.0.0
189035 189956 189981	**Symptom:** Users were unable to connect to AirGroup servers intermittently. The fix ensures that the users are able to connect to AirGroup servers. **Scenario:** This issue occurred when the CPPM queries sent from the clients did not reach the AirGroup servers. This issue was observed in Mobility Master Hardware Appliances running AOS-W 8.2.1.0 in a master-standby topology.	AirGroup	All platforms	AOS-W 8.2.1.0	AOS-W 8.4.0.0

Table 5: *Resolved Issues in AOS-W 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
189064	**Symptom:** Jabber desktop sharing caused unwanted traffic to reach a Mobility Master. Withdrawing the support for Jabber desktop sharing resolved this issue. **Scenario:** This issue occurred because of the wide range of ports being used by Jabber. This issue was observed in Mobility Masters running AOS-W 8.3.0.0 or later versions.	UCC	All platforms	AOS-W 8.3.0.0	AOS-W 8.4.0.0
189159	**Symptom:** IP phones experienced voice gaps and about 500 msec packet losses periodically. The fix ensures that only the 20 MHz setting is considered. **Scenario:** This issue occurred as APs enabled **Extended Capabilities (ID 127) 20/40 BSS Coexistence Management Support** in the beacon although only 20 MHz is set by the user. This led to off-channel scanning and hence, the packet loss. This issue was observed in APs running AOS-W 8.2.0.0 or later versions.	AP-Wireless	All platforms	AOS-W 8.2.0.0	AOS-W 8.4.0.0
189270	**Symptom:** An attribute (**Filter-ID**) that assigns VLANs to the users was missing from a managed device even though the attribute was available in the device configuration settings. The fix ensures that the managed device works as expected. **Scenario:** This issue was observed in managed devices in a cluster setup running AOS-W 8.2.1.1.	Configuration	All platforms	AOS-W 8.2.1.1	AOS-W 8.4.0.0
189353	**Symptom:** The output of the **show ap arm client-match neighbors ap-name** command displayed very high entries. The fix ensures that the command output is displayed correctly. **Scenario:** This issue occurred when the command output was displayed in a loop. This issue was observed in Mobility Masters running AOS-W 8.2.1.1 or later versions.	ARM	All platforms	AOS-W 8.2.1.1	AOS-W 8.4.0.0
189486 189904 190298	**Symptom:** A managed device crashed and rebooted unexpectedly. The log file listed the reason for this event as **Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2)**. The fix ensures that the managed device works as expected. **Scenario:** This issue occurred in a cluster setup when an IPv6 client initiated and stopped multiple FTP transfers. This issue was observed in OAW-4x50 Series switches running AOS-W 8.3.0.2 or later versions.	switch- Datapath	OAW-4x50 Series switches	AOS-W 8.3.0.2	AOS-W 8.4.0.0

Table 5: *Resolved Issues in AOS-W 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
189521	**Symptom:** An AP displayed high rate of PHY errors when hybrid - spectrum mode was enabled. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue was observed in OAW-AP300 Series access points running AOS-W 8.0.0.0 or later versions.	AP-Wireless	OAW-AP300 Series access points	AOS-W 8.0.0.0	AOS-W 8.4.0.0
189523 191049	**Symptom:** An AP that terminated on a managed device with CPsec enabled did not come up after a cluster failover. The fix ensures that the AP comes up after a cluster failover. **Scenario:** This issue occurred when a cluster failover message timed out in the AP after a cluster failover. This issue was observed in access points running AOS-W 8.2.0.0 or later versions.	AP-Platform	All platforms	AOS-W 8.2.0.0	AOS-W 8.4.0.0
189539	**Symptom:** The **mDNS** process on the Mobility Master utilized memory space that is equal to or greater than the assigned value. The issue was resolved by clearing the memory and internal data structures of the **mDNS** packets. **Scenario:** This issue was observed in Mobility Masters running AOS-W 8.2.2.1 or later versions in a master-standby topology.	AirGroup	All platforms	AOS-W 8.2.2.1	AOS-W 8.4.0.0
189552	**Symptom:** IP access restrictions on VLAN interface did not work as expected and did not block expected traffic. The fix ensures that the VLAN interface IP access group traffic restrictions block the correct traffic. **Scenario:** This issue was observed in managed devices running AOS-W 8.2.2.1 or later versions.	VLAN	All platforms	AOS-W 8.3.0.3	AOS-W 8.4.0.0
189722	**Symptom:** Configuration failure was observed on a Mobility Master in standby mode. The fix ensures that all configurations are applied to the standby Mobility Master. **Scenario:** This issue was observed in Mobility Masters running AOS-W 8.2.2.1 or later versions.	Logging	All platforms	AOS-W 8.2.2.1	AOS-W 8.4.0.0
189795	**Symptom:** A mesh point failed to come up after the mesh portal was rebooted. The fix ensures that mesh point comes up on a Mobility Master. **Scenario:** This issue occurred when the Mobility Master failed to set up a mesh link. This issue was observed in Mobility Masters running AOS-W 8.3.0.2 or later versions.	Mesh	All platforms	AOS-W 8.3.0.2	AOS-W 8.4.0.0

Table 5: *Resolved Issues in AOS-W 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
190291	**Symptom:** An error message, **Max CP firewall limit (32) reached** was displayed even when less than the maximum number of ACE 32 entries were added to the device using the **firewall cp** command. The fix ensures that the error message is displayed only when the maximum limit is reached. **Scenario:** This issue occurred when firewall rules were configured and deleted from multiple managed devices. This issue was observed in Mobility Masters running AOS-W 8.2.1.0 or later versions.	Base OS Security	All platforms	AOS-W 8.2.1.0	AOS-W 8.4.0.0
190347	**Symptom:** The user was unable to add untrusted VLANs to interface from the **Mobility Master > Interfaces > Ports > Allowed VLANs> Add Allowed VLAN > Trust** page of the WebUI. The fix ensures that the user can add untrusted VLANs using the WebUI. **Scenario:** This issue was observed in Mobility Masters running AOS-W 8.3.0.3 or later versions.	WebUI	All platforms	AOS-W 8.3.0.3	AOS-W 8.4.0.0
190396	**Symptom:** The console logs of an AP showed the standby IP address as 0.0.0.0. During a failover, the AP lost connectivity with the standby managed device and it did not come up. The fix ensures that the AP failover occurs when the standby managed device is up and the AP obtains the correct IP address of the standby managed device. **Scenario:** This issue occurred during a cluster failover when an AP lost connectivity with the standby managed device. This issue was observed in APs running AOS-W 8.3.0.1.	AP Datapath	All platforms	AOS-W 8.3.0.1	AOS-W 8.4.0.0
190448	**Symptom:** A few APs did not get HA standby IP address and failed to connect to a switch. The fix ensures that the AP connects to the switch. **Scenario:** This issue was observed in stand-alone switches running AOS-W 8.3.0.3 or later versions.	HA-Lite	All platforms	AOS-W 8.3.0.3	AOS-W 8.4.0.0
190542	**Symptom:** A radio experienced a high number of resets in APs. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue occurred when the APs were in Air Monitor mode. This issue was observed in OAW-AP335 access points running AOS-W 8.3.0.0 or later versions.	AP-Wireless	OAW-AP335 access points	AOS-W 8.3.0.0	AOS-W 8.4.0.0

Table 5: *Resolved Issues in AOS-W 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
190571	**Symptom:** An AP failed to come up. The fix ensures that the AP works as expected **Scenario:** This issue occurred on an AP with EST key type **X9.62/SECG curve**. This issue was observed in OAW-AP303H access points running AOS-W 8.2.0.0 or later versions.	CPsec	OAW-AP303H access points	AOS-W 8.2.0.0	AOS-W 8.4.0.0
190666	**Symptom:** The **authentication** process in a switch crashed unexpectedly, which resulted in access points rebooting and caused the cluster to failover. The fix ensures that the OAW-4650 switch works as expected. **Scenario:** This issue was observed in OAW-4650 switches running AOS-W 8.3.0.3.	Base OS Security	OAW-4650 switches	AOS-W 8.3.0.3	AOS-W 8.4.0.0
190677 191836 191870	**Symptom:** The **DDS** process in a managed device crashed unexpectedly. The fix ensures that the managed device works as expected. **Scenario:** This issue was observed in managed devices running AOS-W 8.2.2.2 in a Mobility Master-Managed Device topology.	DDS	All platforms	AOS-W 8.2.2.2	AOS-W 8.4.0.0
190772	**Symptom:** The **show tech-support** command displayed incorrect output. This issue is resolved by executing the **show tech-support** command in **/mm** node. **Scenario:** This issue was observed in Mobility Masters running AOS-W 8.4.0.0.	Configuration	All platforms	AOS-W 8.0.0.0	AOS-W 8.4.0.0
190778	**Symptom:** All the managed devices were displayed as DOWN when the **show switches** command was executed. The fix ensures that the correct status is displayed when the **show switches** command is executed. **Scenario:** This issue occurred when the Mobility Master lost all routes to the active VPNC. This issue was observed in Mobility Masters running AOS-W 8.4.0.0.	IPsec	All platforms	AOS-W 8.4.0.0	AOS-W 8.4.0.0
190795	**Symptom:** An AP failed to come up. The fix ensures that the AP works as expected. **Scenario:** This issue occurred when a OAW-RAP was configured to use PPPoE. This issue was observed in OAW-AP203R, OAW-AP303H, and OAW-AP305 access points running AOS-W 8.3.0.3 or later versions.	OAW-RAP	OAW-AP203R, OAW-AP303H, and OAW-AP305 access points	AOS-W 8.3.0.3	AOS-W 8.4.0.0

Table 5: *Resolved Issues in AOS-W 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
190797	**Symptom:** Incremental Frame Check Sequence received (FCS Rx) errors are observed in APs. Enhancements to the wireless driver resolved this issue. **Scenario:** The issue occurred when the APs were connected using a cable with length greater than 100 meters. This issue was observed in OAW-AP365 access points running AOS-W 8.3.0.0 or later versions.	AP-Wireless	OAW-AP365 access points	AOS-W 8.3.0.0	AOS-W 8.4.0.0
190925	**Symptom:** Managed Device did not forward broadcast ARP packets to silent clients through GRE tunnels although the **no suppress-arp** parameter was set. The fix ensures that the **no suppress-arp** command overrides the **broadcast-filter arp** command to allow unknown broadcast ARP packets through GRE Tunnels. **Scenario:** This issue was observed in managed devices running AOS-W 8.3.0.3 or later versions.	switch - Datapath	All platforms	AOS-W 8.3.0.3	AOS-W 8.4.0.0
190957	**Symptom:** A managed device crashed and rebooted unexpectedly. The log file listed the reason for this event as **Hardware Watchdog Reset (Intent:cause:register 54:86:0:8020)**. The fix ensures that the managed device works as expected. **Scenario:** This issue was observed in OAW-4850 switches running AOS-W 8.3.0.3 or later versions.	switch-Datapath	OAW-4850 switches	AOS-W 8.3.0.3	AOS-W 8.4.0.0
191092 191483	**Symptom:** Multiple processes in a managed device crashed unexpectedly. The fix ensures that the managed device works as expected. **Scenario:** The issue occurred due to a memory leak and high CPU utilization on the managed device. This issue was observed in managed devices running AOS-W 8.2.0.2 or later versions.	SDN	All platforms	AOS-W 8.2.0.2	AOS-W 8.4.0.0
191276	**Symptom:** Some clients get disconnected with error message **idle time out**. The fix ensures that the clients do not get disconnected. **Scenario:** This issue occurred when clients received user idle time out value of 300 seconds instead of 43200 seconds. This issue was observed in OAW-4x50 Series switches running AOS-W 8.0.0.0 or later versions.	Base OS Security	OAW-4x50 Series switches	AOS-W 8.0.0.0	AOS-W 8.4.0.0

Table 5: *Resolved Issues in AOS-W 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
192112	**Symptom:** A managed device showed Skype error messages in the HTTPD logs and dropped XML messages that were meant for UCM. The visibility of Skype for Business call records were missing from the WebUI. The fix ensures that the managed device works as expected and does not drop the XML messages that are meant for UCM. **Scenario:** This issue was observed in managed devices running AOS-W 8.2.2.2.	Web Server	All platforms	AOS-W 8.2.2.2	AOS-W 8.4.0.0
192345	**Symptom:** Configuration failure occurred when IoT transport profile was used in a managed device. The fix ensures that the configuration failure does not occur on the managed device. **Scenario:** This issue was observed in Mobility Masters and managed devices running AOS-W 8.4.0.0 and AOS-W 8.3.0.0 respectively in a Mobility Master-Managed Device topology.	BLE	All platforms	AOS-W 8.3.0.0	AOS-W 8.4.0.0
192468	**Symptom:** An AP in IPv6 environment did not preempt to the active managed device although preemption was enabled. The fix ensures that the AP preempts to the active managed device when required. **Scenario:** This issue was observed in access points running AOS-W 8.2.0.0 in an IPv6 high-availability topology.	AP-Platform	All platforms	AOS-W 8.2.0.0	AOS-W 8.4.0.0

Chapter 6
Known Issues and Limitations

This chapter describes the known issues and limitations identified in AOS-W 8.4.0.0.

Limitations

This section describes the limitations in AOS-W 8.4.0.0.

Fast BSS Transition

802.11r feature is not supported in WLAN SSIDs using WPA-3 security.

Zigbee Radio Mode

For Zigbee radio mode, there is no support provided through the WebUI.

Known Issues for OAW-AP510 Series Access Points

Table 6: *Known Issues for OAW-AP510 Series access Points in AOS-W 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version
185579	**Symptom:** Invalid transmissions are observed when an AP boots up in the Air Monitor mode. **Scenario:** This issue is observed in OAW-AP510 Series access points running AOS-W 8.4.0.0. **Workaround:** None.	AP-Wireless	OAW-AP510 Series access points	AOS-W 8.4.0.0
186310 188308	**Symptom:** An AP sends multicast traffic to clients at a lower rate. **Scenario:** This issue occurs when **bcmc-optimization** is enabled and DMO is disabled. This issue is observed in OAW-AP303P and OAW-AP515 access points running AOS-W 8.4.0.0. **Workaround:** None.	AP-Wireless	OAW-AP303P and OAW-AP515 access points	AOS-W 8.4.0.0
186918	**Symptom:** Air time fairness feature is not functional although the value of the **shaping-policy** parameter is set to **default-access**. **Scenario:** This issue is observed in OAW-AP510 Series access points running AOS-W 8.4.0.0. **Workaround:** None.	AP-Wireless	OAW-AP510 Series access points	AOS-W 8.4.0.0
186957	**Symptom:** The beacon and probe response packets do not display the country capabilities information element for 5 GHz non-DFS channel. **Scenario:** This issue is observed in OAW-AP510 Series access points running AOS-W 8.4.0.0. **Workaround:** None.	AP-Wireless	OAW-AP510 Series access points	AOS-W 8.4.0.0
188308	**Symptom:** Video multicast frames are transmitted at the lowest configured rate on an AP. **Scenario:** This issue occurs when **mcast-rate-opt** parameter is enabled on the AP. This issue is observed in OAW-AP510 Series access points running AOS-W 8.4.0.0. **Workaround:** None.	AP-Wireless	OAW-AP510 Series access points	AOS-W 8.4.0.0
188356 190747	**Symptom:** Clients reconnect to the AP frequently as the effective rates and advertised rates are not the same. **Scenario:** This issue is observed in OAW-AP510 Series access points running AOS-W 8.4.0.0. **Workaround:** Ensure that the **g-basic-rates <mbps>** and **g-tx-rates <mbps>** parameters of the wlan SSID profile are set to the default value.	AP-Wireless	OAW-AP510 Series access points	AOS-W 8.4.0.0

Table 6: *Known Issues for OAW-AP510 Series access Points in AOS-W 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version
188717	**Symptom:** CSR does not work for 2G and 5G networks. **Scenario:** This issue is observed in OAW-AP510 Series access points running AOS-W 8.4.0.0 or later versions. **Workaround:** None.	AP-Wireless	OAW-AP510 Series access points	AOS-W 8.4.0.0
189298	**Symptom:** System LED is blinking with a green light after an AP connects to a managed device and boots up. **Scenario:** This issue occurs when 2.4 GHz radio is disabled. This issue is observed in OAW-AP510 Series access points running AOS-W 8.4.0.0. **Workaround:** Modify any one of the 2.4 GHz radio profiles.	AP-Wireless	OAW-AP510 Series access points	AOS-W 8.4.0.0
189519	**Symptom:** Older Intel driver chipsets are unable to detect SSIDs with **high efficiency** enabled on the AP. **Scenario:** This issue is observed in OAW-AP510 Series access points running AOS-W 8.4.0.0 where the Intel driver is running a version prior to 20.70.x.x version. **Workaround:** Upgrade the Intel drivers to the latest version or disable the **high efficiency** parameter in the SSID profile by executing the following command : **(host) [node] # wlan he-ssid-profile default no high-efficiency-enable**	AP-Wireless	OAW-AP510 Series access points	AOS-W 8.4.0.0
190654 193387	**Symptom:** APs reboot unexpectedly and experience packet loss. The log file lists the reason for the event as **Kernel Panic**. **Scenario:** This issue occurs when Jumbo frames are enabled between a managed device and the AP. This issue is observed in OAW-AP510 Series access points running AOS-W 8.4.0.0. **Workaround:** Disable Jumbo frames or set the framed-mtu <mtu> to 1500 or 1578 in the AP System profile.	AP-Wireless	OAW-AP510 Series access points	AOS-W 8.4.0.0
191669	**Symptom:** The performance of **Iperf throughput** test drops when a **Multicast** process runs at the same time on an AP. **Scenario:** This issue is observed in OAW-AP510 Series access points running AOS-W 8.4.0.0. **Workaround:** None.	AP-Wireless	OAW-AP510 Series access points	AOS-W 8.4.0.0

Table 6: *Known Issues for OAW-AP510 Series access Points in AOS-W 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version
191774	**Symptom:** Some APs running in 2G radio mode fail to transit from 1ss to 2ss power mode. **Scenario:** This issue occurs if there is a delay in the LLDP negotiation between an AP and a managed device. This issue is observed in OAW-AP510 Series access points running AOS-W 8.4.0.0. **Workaround:** None.	AP-Wireless	OAW-AP510 Series access points	AOS-W 8.4.0.0
192771 189897	**Symptom:** The value returned from noise floor calculation is inaccurate when there is interference. **Scenario:** This issue is observed in OAW-AP510 Series access points running AOS-W 8.4.0.0. **Workaround:** None.	AP-Wireless	OAW-AP510 Series access points	AOS-W 8.4.0.0
193223	**Symptom:** An AP took longer than usual to transfer packets to clients. **Scenario:** This issue occurs when a Surface Pro client does not aggregate traffic. This issue is observed in OAW-AP510 Series access points running AOS-W 8.4.0.0. **Workaround:** Disable aggregation for transmission using the **wlan ht-ssid-profile <> no mpdu-agg** command.	AP-Wireless	OAW-AP510 Series access points	AOS-W 8.4.0.0

Known Issues

The following known issues are observed in AOS-W 8.4.0.0.

Table 7: *Known Issues in AOS-W 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version
124928	**Symptom:** The route-cache does not update the IPsec tunnel IDs correctly after a failover link comes up. **Scenario:** This issue is observed in managed devices running AOS-W 8.3.0.0. **Workaround:** None.	Routing	All platforms	AOS-W 8.3.0.0
151952	**Symptom:** When a managed device reboots, APs and clients boot without IP addresses and other fields. **Scenario:** This issue is observed in managed devices running AOS-W 8.0.1.0. **Workaround:** None.	Monitoring	All platforms	AOS-W 8.0.1.0
159222 179137	**Symptom:** The number of clients displayed in the active-standby IP field on the Mobility Master dashboard is incorrect. **Scenario:** This issue occurs due to a cluster failover causing race condition. This issue is observed in Mobility Masters running AOS-W 8.1.0.0 or later versions. **Workaround:** None.	Base OS Security	All platforms	AOS-W 8.1.0.0
164332	**Symptom:** The IPM default list for an AP is not displayed even though the IPM feature is enabled in the WebUI. **Scenario:** This issue is observed in APs running AOS-W 8.2.0.0 or later versions. **Workaround:** None.	AP-Platform	All platforms	AOS-W 8.2.0.0
164916	**Symptom:** A managed device does not display an error when executing the **show license-pool-profile-root** command. **Scenario:** This issue occurs when the managed device is a license client. This issue is observed in managed devices running AOS-W 8.2.0.0. **Workaround:** None.	Licensing	All platforms	AOS-W 8.2.0.0
166937	**Symptom:** The AirGroup process in a managed device stops responding. **Scenario:** This issue occurs when an AirGroup profile is changed in a managed device with mDNS servers and users. This issue is observed in managed devices running AOS-W 8.2.0.0. **Workaround:** None.	AirGroup	All platforms	AOS-W 8.2.0.0
167795	**Symptom:** An AP fails to detect a microwave inverter. **Scenario:** This issue occurs in APs where either the **Hybrid** or **Spectrum** mode in 2.4 GHz is enabled. This issue is observed in OAW-AP345 access points running AOS-W 8.3.0.0. or later versions. **Workaround:** None.	Spectrum-Interferer Classification	OAW-AP345 access points	AOS-W 8.3.0.0

Table 7: *Known Issues in AOS-W 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version
168457	**Symptom:** The license count in **Mobility Master > Licenses** page in the WebUI does not reflect the ACR license usage. **Scenario:** This issue occurs when the license count is not communicated to the applications running on Standby Mobility Master. This issue is observed in Mobility Masters running AOS-W 8.2.0.0 or later versions. **Workaround:** None.	Licensing	All platforms	AOS-W 8.2.0.0
170058	**Symptom:** A managed device crashes and reboots unexpectedly. The log file lists the reason for the event as **Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2)**. **Scenario:** This issue is observed in OAW-4x50 Series switches running AOS-W 8.0.0.0 or later versions. **Workaround:** None.	switch-Datapath	OAW-4x50 Series switches	AOS-W 8.0.0.0
170105 171721	**Symptom:** Some clients get deauthenticated and fail to connect to an AP. The log files list the reason for this event as **Reason Ptk Challenge Failed** and **deauth_reason 52**. **Scenario:** This issue is observed in APs running AOS-W 8.0.0.0 or later versions. **Workaround:** None.	AP-Wireless	All platforms	AOS-W 8.0.0.0
171246 187010 187759 187764 188678 188679 188681 189142	**Symptom:** A managed device crashes and reboots unexpectedly. **Scenario:** This issue is observed in OAW-4750XM switches running AOS-W 8.2.0.0. in a Mobility Master - Managed Device topology. **Workaround:** None.	switch- Datapath	OAW-4750XM switches	AOS-W 8.2.1.0
171397	**Symptom:** The WAN health-check is enabled in the default configuration. **Scenario:** This issue is observed in managed devices running AOS-W 8.2.0.1. **Workaround:** None.	Branch switch	All platforms	AOS-W 8.2.0.1
172942	**Symptom:** A managed device reboots unexpectedly. The log file lists the reason for the event as **Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2**. **Scenario:** This issue is observed in OAW-4750XM switches running AOS-W 8.0.0.0 or later versions. **Workaround:** None.	switch-Datapath	OAW-4750XM switches	AOS-W 8.0.0.0

Table 7: *Known Issues in AOS-W 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version
173070	**Symptom:** The number of clients displayed in the AppRF dashboard in the WebUI is different from those that are displayed in the CLI. **Scenario:** This issue is observed in Mobility Masters running AOS-W 8.0.0.0 or later versions. **Workaround:** None.	Firewall Visibility	All platforms	AOS-W 8.0.0.0
175233	**Symptom:** A client loses ping packets. **Scenario:** This issue occurs when the client aware scanning is enabled. This issue is observed in access points running AOS-W 8.4.0.0. **Workaround:** None.	AP-Wireless	All platforms	AOS-W 8.4.0.0
175636	**Symptom:** An AP retransmits the ping packets twice even though the channel is not busy. **Scenario:** This issue occurs when dual 5 GHz radio channel is enabled. This issue is observed in OAW-AP340 Series access points running AOS-W 8.3.0.0 or later versions. **Workaround:** None.	AP-Wireless	OAW-AP340 Series access points	AOS-W 8.3.0.0
176435	**Symptom:** The IP health-check in a managed device shows **Unreachable** although the outside network was reachable. **Scenario:** This issue is observed in managed devices running AOS-W 8.2.0.2. **Workaround:** None.	switch-Datapath	All platforms	AOS-W 8.2.0.2
176879	**Symptom:** Some clients are unable to pass traffic due to unresponsive ARP gateway. **Scenario:** This issue occurs because the device detects AES replay. This issue is observed in APs running AOS-W 8.0.0.0 or later versions. **Workaround:** Moving to a different AP restores connectivity.	AP-Wireless	All platforms	AOS-W 8.0.0.0
176991	**Symptom:** The **Configuration > Roles and Policies > Roles** table does not display **denyall and default-iap-user-role** roles. **Scenario:** This issue is observed in OAW-4010 switches running AOS-W 8.2.0.2 or later versions. **Workaround:** Reload the switch to see **Denyall** in the WebUI.	Authentication	OAW-4010switches	AOS-W 8.2.0.2
177001	**Symptom:** An AP reboots unexpectedly. The log file lists the reason for the event as **Reboot caused by kernel panic: Fatal exception in interrupt" - code: bad PC value**. **Scenario:** This issue is observed in OAW-AP315 access points running AOS-W 8.3.0.0 or later versions. **Workaround:** None.	AP-Wireless	OAW-AP315 access points	AOS-W 8.3.0.0

Table 7: *Known Issues in AOS-W 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version
177283	**Symptom:** Some APs experience packet loss and display the error message, **wl0: wlc_ ampdu_watchdog: no memory**. **Scenario:** This issue is observed in OAW-AP340 Series access points running AOS-W 8.3.0.0 or later versions. **Workaround:** None.	AP-Wireless	OAW-AP340 Series access points	AOS-W 8.3.0.0
177297	**Symptom:** Some APs display duplicate netdestination entries after an AP failover and switchover to standby mode. **Scenario:** This issue is observed in managed devices in a cluster setup running AOS-W 8.1.0.0 or later versions. **Workaround:** None.	Cluster-Manager	All platforms	AOS-W 8.1.0.0
177664	**Symptom:** An AP reboots unexpectedly. The log file lists the reason for the event as **Reboot caused by kernel panic: Fatal exception in interrupt (PC is at irq_work_ run)**. **Scenario:** This issue is observed in OAW-AP315 access points running AOS-W 8.3.0.0 or later versions. **Workaround:** None.	AP-Wireless	OAW-AP315 access points	AOS-W 8.3.0.0
178008	**Symptom:** Some APs stop sending beacon frames and disconnect all clients. **Scenario:** This issue occurs when the static channel of the AP is changed from 36E to 36S. This issue is observed in OAW-AP340 Series access points running AOS-W 8.3.0.0 or later versions. **Workaround:** None.	AP-Wireless	OAW-AP340 Series access points	AOS-W 8.3.0.0
178124	**Symptom:** Redirects fail for large cookies on Edge browser. **Scenario:** This issue occurs when: ■ the maximum HTTP header size is 8000. ■ requests that have large or higher number of cookies turn into bad requests. This issue is observed in Mobility Masters running AOS-W 8.0.0.0 or later versions. **Workaround:** None.	Web Server	All platforms	AOS-W 8.0.0.0
178711	**Symptom:** Wireless clients using PBR are unable to route traffic. **Scenario:** This issue occurs when IPsec tunnel is enabled on the Mobility Master. This issue is observed in Mobility Masters running AOS-W 8.2.1.0. **Workaround:** None.	Policy Based Routing	All platforms	AOS-W 8.2.1.0

Table 7: *Known Issues in AOS-W 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version
179219	**Symptom:** AirMatch skips a number of APs and deploys a limited number of APs. **Scenario:** This issue occurs after the timezone is changed. This issue is observed in managed devices running AOS-W 8.3.0.0. **Workaround:** None.	AirMatch	All platforms	AOS-W 8.3.0.0
179307	**Symptom:** The **DHCP** process crashes in a managed device. **Scenario:** This issue is observed in managed devices running AOS-W 8.0.1.0 or later versions. **Workaround:** None.	DHCP	All platforms	AOS-W 8.0.1.0
179356	**Symptom:** A managed device crashes and reboots unexpectedly. Once the managed device reboots, it fails to create the nexthop index and stops communicating with the Mobility Master. **Scenario:** This issue is observed in managed devices running AOS-W 8.0.1.0 or later versions. **Workaround:** None.	switch-Datapath	All platforms	AOS-W 8.0.1.0
179723 188611 189642	**Symptom:** An AP crashes and reboots unexpectedly. **Scenario:** This issue is observed in OAW-AP300 Series access points running AOS-W 8.2.1.0 or later versions. **Workaround:** None.	AP-Wireless	OAW-AP300 Series access points	AOS-W 8.2.1.0
180349	**Symptom:** The user is not able to disable the **prohibit ip-spoofing** using the **Configuration > Services > Firewall > Prohibit IP spoofing** check box in the WebUI. **Scenario:** This issue was observed in a managed devices running AOS-W 8.3.0.0 or later versions. **Workaround:** None.	switch-Datapath	All platforms	AOS-W 8.3.0.0
180383	**Symptom:** A client is deauthenticated unexpectedly. **Scenario:** This issue occurs when the User Anchor Controller (UAC) is down. This issue is observed in managed devices running AOS-W 8.2.1.0 in a cluster topology. **Workaround:** None.	Station Management	All platforms	AOS-W 8.2.1.0
180571	**Symptom:** Some clients experience a sudden decrease in the network speed. **Scenario:** This issue occurs when BA-MSDU and jumbo frames are enabled on a managed device. The managed device creates TCP retransmits and multiple duplicate packets, causing the speed to drop. This issue is observed in managed devices running AOS-W 8.3.0.0 or later versions. **Workaround:** None.	switch-Datapath	All platforms	AOS-W 8.3.0.0

Table 7: *Known Issues in AOS-W 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version
180973	**Symptom:** A managed device does not steer traffic as expected. **Scenario:** This issue occurs when a probe profile with UDP mode and corresponding threshold profile with **mos** value are configured. This issue is observed in managed devices running AOS-W 8.3.0.0. **Workaround:** None.	switch-Datapath	All platforms	AOS-W 8.3.0.0
181026	**Symptom:** Wireless clients are assigned default VLAN and MAC authentication roles after failing 802.1X authentication. **Scenario:** This issue occurs when a wireless client passes the MAC authentication but fails the 802.1X authentication. This issue is observed in OAW-4005 switches in a stand-alone mode running AOS-W 8.2.1.0 or later versions. **Workaround:** None.	Base OS Security	OAW-4005 switches	AOS-W 8.2.1.0
182054	**Symptom:** An AP crashes and reboots unexpectedly. The log file lists the reason for this event as **Reboot caused by kernel panic: Out of memory**. **Scenario:** This issue is observed in OAW-AP335 access points running AOS-W 8.2.1.1 or later versions. **Workaround:** None.	AP-Wireless	OAW-AP335 access points	AOS-W 8.2.1.1
182224	**Symptom:** The **License Successfully Claimed** message is not displayed for a successful license registration in the **Mobility Master > Configuration > Licenses > Aruba Support Portal (ASP)** page of the WebUI. **Scenario:** This issue is observed in Mobility Master running AOS-W 8.4.0.0. **Workaround:** None	WebUI	All platforms	AOS-W 8.4.0.0
182409	**Symptom:** The **Eth0** port of an AP that operates in dual 5 GHz mode or dual band mode drops packets. **Scenario:** This issue occurs when an AP uses 1 Gbps uplink and the radios receive more than 1 Gbps traffic. This issue is observed in OAW-AP340 Series access points running AOS-W 8.2.1.1 or later versions. **Workaround:** None.	AP-Platform	OAW-AP340 Series access points	AOS-W 8.2.1.1
182684	**Symptom:** Wireless clients are unable to connect to the VRRP IP of a Mobility Master. **Scenario:** This issue is observed in Mobility Masters running AOS-W 8.3.0.0 or later versions. **Workaround:** None.	switch-Datapath	All platforms	AOS-W 8.3.0.0

Table 7: *Known Issues in AOS-W 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version
182885	**Symptom:** The aggregate number of VIA or PEFV licenses installed on a particular Mobility Master is not displayed in the **Mobility Master > Configuration > Licenses > Aruba Support Portal (ASP)** page of the WebUI. **Scenario:** This issue is observed in Mobility Master running AOS-W 8.4.0.0. **Workaround:** None	WebUI	All platforms	AOS-W 8.4.0.0
183031	**Symptom:** The **IP address** column under **Dashboard > Overview > Wired clients** displays only one IP address. **Scenario:** This issue is observed in Mobility Master running AOS-W 8.4.0.0 or later versions. **Workaround:** None.	WebUI	All platforms	AOS-W 8.4.0.0
183128	**Symptom:** An AP crashes and reboots unexpectedly. The log file lists the reason for this event as **Reboot caused by kernel panic: Rebooting the AP because of FW ASSERT**. **Scenario:** This issue is observed in OAW-AP315 access points running AOS-W 8.3.0.0. **Workaround:** None.	AP-Wireless	OAW-AP315 access points	AOS-W 8.3.0.0
183178	**Symptom:** A OAW-RAP fails to come up when connected to a 4G dongle. **Scenario:** This issue is observed on OAW-AP303H access points running AOS-W 8.3.0.0 or later versions. **Workaround:** None.	Remote AP	OAW-AP303H access points	AOS-W 8.3.0.0
183192	**Symptom:** Unable to check the ASP connection status of the standby Mobility Master from the **Mobility Master > Configuration > Licenses > Aruba Support Portal (ASP)** page in the WebUI. **Scenario:** This issue is observed in Mobility Master running AOS-W 8.4.0.0. **Workaround:** View the standby Mobility Master ASP connection status using CLI, **show asp status standby** command in the active Mobility Master.	WebUI	All platforms	AOS-W 8.4.0.0
183193	**Symptom:** User is unable to use the **Enter** key to sign in from the **Signin to ASP** popup window after entering the correct credentials. **Scenario:** This issue is observed in Mobility Master running AOS-W 8.4.0.0. **Workaround:** None.	WebUI	All platforms	AOS-W 8.4.0.0

Table 7: *Known Issues in AOS-W 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version
183213	**Symptom:** ASP account information is not displayed in the **Mobility Master > Configuration > System > General > Aruba Support Portal** page in the WebUI. **Scenario:** This issue is observed in Mobility Master running AOS-W 8.4.0.0. **Workaround:** View the ASP account information by executing the command, **show asp account-info**.	WebUI	All platforms	AOS-W 8.4.0.0
183325	**Symptom:** A managed device crashes and reboots unexpectedly. The log file lists the reason for this event as **Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2)**. **Scenario:** This issue is observed in managed devices running AOS-W 8.0.0.0 or later versions. **Workaround:** None.	switch-Datapath	All platforms	AOS-W 8.0.0.0
183430	**Symptom:** User is unable to move from external licensing server mode to ASP mode automatically without manually enabling the ASP profile. **Scenario:** This issue is observed in Mobility Master running AOS-W 8.4.0.0. **Workaround:** None.	Licensing	All platforms	AOS-W 8.4.0.0
184030	**Symptom:** The cumulative count of licenses allocated and installed from both active and standby Mobility Masters is not displayed once the active Mobility Master comes up after a failover. **Scenario:** This issue is observed in Mobility Master running AOS-W 8.4.0.0. **Workaround:** To view the cumulative count of licenses allocated and installed from both active and standby Mobility Masters, navigate to **Mobility Master > Configuration > License > License Inventory** tab and click **update now** link, once the Mobility Master comes up after failover.	Licensing	All platforms	AOS-W 8.4.0.0
183580	**Symptom:** An AP crashes and reboots unexpectedly. The log file lists the reason for this event as **Reboot caused by kernel panic: Fatal exception**. **Scenario:** This issue is observed in OAW-AP303H access points running AOS-W 8.2.1.1. **Workaround:** None.	AP-Wireless	OAW-AP303H access points	AOS-W 8.2.1.1

Table 7: *Known Issues in AOS-W 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version
183973 186151	**Symptom:** Wireless clients failed to reconnect to the SSID after being dropped from the network. The managed device lists the following error messages: ■ **user repkey change failed** ■ **macuser repkey change failed** **Scenario:** This issue occurs when the GSM slot in a user channel is not deleted, which reduces the available GSM slots to zero. This issue is observed in managed devices running AOS-W 8.2.1.1. **Workaround:** Reboot the managed device.	Base OS Security	All platforms	AOS-W 8.2.1.1
184104	**Symptom:** An AP crashes and reboots unexpectedly. The log file lists the reason for the event as **Reboot caused by kernel panic: Rebooting the AP because of FW HANG (PCIE error(s) detected)** **Scenario:** This issue is observed in OAW-AP335 access points running AOS-W 8.2.1.1. **Workaround:** Reboot the managed device.	AP-Wireless	OAW-AP335 access points	AOS-W 8.2.1.1
184849	**Symptom:** Clients are unable to make or receive calls. A **Network busy** error message is displayed. **Scenario:** This issue occurs when WMM is disabled on the managed device. This issue is observed in OAW-AP315 access points running AOS-W 8.2.1.1. **Workaround:** None.	WMM	OAW-AP315 access points	AOS-W 8.2.1.1
185165	**Symptom:** A managed device crashes unexpectedly. The log files list the reason for this event as **Reboot Cause: Reboot by Upgrade Manager Intent:cause:register 60:86:50:60).** **Scenario:** This issue is observed in managed devices running AOS-W 8.2.1.1 or later versions. **Workaround:** None.	switch platform	All platforms	AOS-W 8.2.1.1
185499	**Symptom:** Managed devices at the branch office are unable to receive IP address from the branch uplink pool. **Scenario:** This issue is observed in managed devices running AOS-W 8.2.1.0 or later versions. **Workaround:** None.	IPsec	All platforms	AOS-W 8.2.1.0
185561	**Symptom:** A client experiences pixelated video when streaming a multicast video stream. **Scenario:** This issue is observed in managed devices running AOS-W 8.3.0.0. **Workaround:** None.	Multicast	All platforms	AOS-W 8.3.0.0

Table 7: *Known Issues in AOS-W 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version
185647	**Symptom:** A switch experiences low throughput while transmitting data through per user tunneled-node tunnels. **Scenario:** This issue occurs when the transmitted data packets are lesser than 256 bytes. This issue is observed in stand-alone switches running AOS-W 8.4.0.0. **Workaround:** None.	Tunnel-Node-Manager	All platforms	AOS-W 8.4.0.0
185687	**Symptom:** APs crash and reboot unexpectedly. The log files lists the reason for the event as **Fatal exception: Data Cache Parity Error**. **Scenario:** This issue is observed in OAW-AP335 access points running AOS-W 8.2.1.1 or later versions. **Workaround:** None.	AP-Wireless	OAW-AP335 access points	AOS-W 8.2.1.1
187572	**Symptom:** All the upstream routers are receiving a lot of OSPF log errors. **Scenario:** This issue is observed in managed devices running AOS-W 8.1.0.0 or later versions. **Workaround:** None.	OSPF	All platforms	AOS-W 8.1.0.0
185834	**Symptom:** Some clients face a delay in receiving the IP address using a DHCP server. **Scenario:** This issue is observed in OAW-4550 switches running AOS-W 8.0.0.0 or later versions. **Workaround:** None.	DHCP	OAW-4550 switches	AOS-W 8.0.0.0
185873	**Symptom:** The hotspot-shield application is not classified for some Android clients. **Scenario:** This issue occurs as the android client does not provide support for this application. This issue is observed in OAW-4750 switches running AOS-W 8.3.0.2 or later versions. **Workaround:** None.	DPI	OAW-4750 switches	AOS-W 8.3.0.2
185938	**Symptom:** A managed device crashes and displays the **profmgr Module crashed** message. **Scenario:** This issue is observed in managed devices running AOS-W 8.2.0.1 or later versions. **Workaround:** None.	Configuration	All platforms	AOS-W 8.2.0.1
186324 192783	**Symptom:** The **Dashboard** > **Infrastructure** > **Cluster** page displays only the wireless clients count and not wired or remote count of PUTN clients. **Scenario:** This issue is observed in managed devices running AOS-W 8.4.0.0. **Workaround:** None.	WebUI	All platforms	AOS-W 8.4.0.0

Table 7: *Known Issues in AOS-W 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version
186739	**Symptom:** A managed device loses the IP address information during reboot of the Mobility Master due to power cycle failure. **Scenario:** This issue occurs in managed devices that are configured by zero-touch provisioning. This issue is observed in managed devices running AOS-W 8.2.1.1 or later versions. **Workaround:** ■ Set the secondary master IP on VLAN 4094 when the managed device is configured by zero-touch provisioning. ■ Do not change the master IP to any VLAN other than the one configured in the setup dialog.	Configuration	All platforms	AOS-W 8.2.1.1
187033	**Symptom:** The **Usage** page under **Dashboard** > **Overview** does not display the transmitted and received throughput data (bps) for PUTN clients. **Scenario:** This issue is observed in managed devices running AOS-W 8.4.0.0. **Workaround:** None.	WebUI	All platforms	AOS-W 8.4.0.0
187098	**Symptom:** Firewall DNS names do not age out leading to high CPU utilization in datapath. **Scenario:** This issue occurs when a large number of netdestinations with many name based entries are configured on a Mobility Master. These netdestination names get resolved to the DNS IP addresses which in turn retain the firewall DNS names causing CPU over utilization. This issue is observed in Mobility Masters running AOS-W 8.0.0.0 or later versions. **Workaround:** None.	switch-Datapath	All platforms	AOS-W 8.0.0.0
187411	**Symptom:** The **mdns** and **authentication** processes consume high memory in a managed device although AirGroup is disabled. **Scenario:** This issue is observed in managed devices running AOS-W 8.3.0.0. **Workaround:** None.	Base OS Security	All platforms	AOS-W 8.3.0.0
187621	**Symptom:** Some wireless clients face intermittent VRRP heartbeat drops. **Scenario:** This issue is observed in managed devices running AOS-W 8.0.0.0 or later versions. **Workaround:** None.	VRRP	All platforms	AOS-W 8.0.0.0
187729	**Symptom:** Some wireless clients fail to get authenticated when the authentication process utilization exceeded 100%. **Scenario:** This issue is observed in managed devices running AOS-W 8.0.0.0 or later versions. **Workaround:** None.	Base OS Security	All platforms	AOS-W 8.0.0.0

Table 7: *Known Issues in AOS-W 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version
187884	**Symptom:** A mesh point that is behind a remote mesh portal does not receive an IP address. **Scenario:** This issue occurs when the channel of a mesh point is changed. This issue is observed in access points running AOS-W 8.3.0.0. **Workaround:** None.	Mesh	All platforms	AOS-W 8.3.0.0
188018 188011 188954	**Symptom:** An AP crashes and reboots unexpectedly. The log file lists the reason for this event as **Reboot caused by kernel panic: Rebooting the AP because of FW HANG.** **Scenario:** This issue is observed in OAW-AP300 Series access points running AOS-W 8.0.0.0 or later versions. **Workaround:** None.	AP-Wireless	OAW-AP300 Series access points	AOS-W 8.0.0.0
188021	**Symptom:** A managed device generates the following console error **|snmp| An internal system error has occurred at file ../unix/aruba_main.c function snmpRequestProcessing line 704 error Cannot send snmp response**. **Scenario:** This issue is observed in managed devices running AOS-W 8.3.0.0. **Workaround:** None.	SNMP	All platforms	AOS-W 8.3.0.0
188429	**Symptom:** A total of 10 capacity licenses are allowed per allocation attempt, with a maximum of 4 per type. A validation message for the same is not displayed when the count exceeds 10. **Scenario:** This issue is observed in Mobility Masters running AOS-W 8.4.0.0. **Workaround:** Allocate licenses according to the limits.	Licensing	All platforms	AOS-W 8.4.0.0
188639	**Symptom:** The **Access Points** page under **Managed Network** > **Dashboard** becomes unresponsive and does not display any information. **Scenario:** This issue occurs when the OmniAccess Mobility Controller WebUI is accessed using Firefox browser. This issue is observed in OmniAccess Mobility Controllers running AOS-W 8.4.0.0. **Workaround:** Switch to Google Chrome browser.	WebUI	All platforms	AOS-W 8.4.0.0
189012	**Symptom:** License synchronizing message, **Status: Error, License syncing is already in progress, please try later**, is displayed as an error instead of a warning or an information. **Scenario:** This issue is observed in Mobility Masters running AOS-W 8.4.0.0. **Workaround:** None.	Licensing	All platforms	AOS-W 8.4.0.0

Table 7: *Known Issues in AOS-W 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version
189134	**Symptom:** APs are not tagging the correct VLAN ID. **Scenario:** This issue occurs when ports are set as trunk mode and the uplink and downlink packets are tagged as VLAN 2. This issue is observed in OAW-AP303H access points running AOS-W 8.2.0.0 or later versions. **Workaround:** None.	AP Datapath	OAW-AP303H access points	AOS-W 8.3.0.0
189698	**Symptom:** The Eth0 port of an AP does not work in **LACP bndl** state when the Eth1 port of the AP is down or the AP is rebooted. **Scenario:** This issue occurs when: ■ a LACP port channel is created on Eth0 and Eth1 ports of an AP. ■ the peer port of Eth1 (on switch) is shut down. This issue is observed in access points running AOS-W 8.4.0.0. **Workaround:** None.	AP-Platform	All platforms	AOS-W 8.4.0.0
189748	**Symptom:** Wired clients lose connectivity to the gateway resulting in a loss of network. **Scenario:** This issue occurs because the AP uplink port detects duplicate IP address sourced by multiple MAC addresses. This issue is observed in APs running AOS-W 8.0.0.0 or later versions. **Workaround:** None.	AP-Platform	All platforms	AOS-W 8.0.0.0
189885	**Symptom:** Managed devices fail to upgrade because of password failure during a scheduled upgrade. **Scenario:** This issue occurs when the managed devices are upgraded using the WebUI and the password is automatically picked from the configured upgrade-profile. However, the Mobility Master sends an incorrect password with the upgrade command. This issue is observed in managed devices running AOS-W 8.4.0.0. **Workaround:** Configure the upgrade profile for scheduling upgrade before upgrading any managed device.	WebUI	All platforms	AOS-W 8.4.0.0
189921	**Symptom:** The **Age** column under **Dashboard** > **Overview** > **Wired Clients** table, and the **Tunneled Switches** table under **Dashboard** > **Infrastructure** display incorrect values. **Scenario:** This issue occurs when there is no NTP synchronization between the devices. This issue is observed in Mobility Masters running AOS-W 8.4.0.0. **Workaround:** Perform an NTP synchronization across all connected Mobility Masters and managed devices.	WebUI	All platforms	AOS-W 8.4.0.0

Table 7: *Known Issues in AOS-W 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version
189952	**Symptom:** SNMP process crashes on a switch unexpectedly. **Scenario:** This issue is observed in OAW-4x50 Series switches running AOS-W 8.2.1.1 or later versions. **Workaround:** None.	SNMP	All platforms	AOS-W 8.2.1.1
190094	**Symptom:** A client connected to an AP displays low signal strength. **Scenario:** This issue occurs in OAW-AP340 Series access points running AOS-W 8.3.0.3 or later versions. **Workaround:** None.	AP-Wireless	OAW-AP340 Series access points	AOS-W 8.3.0.3
190828	**Symptom:** The **Tunneled Switches** table under **Dashboard** > **Infrastructure** does not display PUTN clients running IPv6 tunnel. **Scenario:** This issue occurs in the Mobility Master UI, when the Mobility Master and managed device communicate over an IPv4 tunnel but the PUTN switch connects with the managed device over an IPv6 tunnel. This issue is observed in Mobility Masters running AOS-W 8.4.0.0. **Workaround:** None.	WebUI	All platforms	AOS-W 8.4.0.0
190869	**Symptom:** Active APs are not displayed in the **Dashboard > Access Points** page in the WebUI. **Scenario:** This issue is observed in managed devices running AOS-W 8.3.0.3 or later versions. **Workaround:** None.	Configuration	All platforms	AOS-W 8.3.0.3
190873	**Symptom:** Clients get disconnected as the APs rebootstrap continuously. **Scenario:** This issue occurs when the **uplink-vlan** parameter is configured in the Remote AP mode using the **ap provisioning-profile** command. This issue is observed in OAW-AP335 access points running AOS-W 8.4.0.0. **Workaround:** None.	AP Datapath	OAW-AP335 access points	AOS-W 8.4.0.0
191050	**Symptom:** switch crashes unexpectedly. **Scenario:** This issue occurs in OAW-4750 switches running AOS-W 8.2.0.0 or later versions. **Workaround:** None.	switch-Platform	OAW-4750 switches	AOS-W 8.2.0.0

Table 7: *Known Issues in AOS-W 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version
191281	**Symptom:** Some VPN clients ignore configured certificate groups when IKEv2 is enabled. **Scenario:** This issue occurs when there is a mismatch between the certificate request and CA certificate. This issue is observed in Mobility Masters running AOS-W 8.3.0.3 or later versions. **Workaround:** None.	IPsec	All platforms	AOS-W 8.3.0.3
191516	**Symptom:** An AP crashes and reboots unexpectedly. The log file lists the reason for this issue as **Kernel panic - Fatal exception running with code version 8.3.0.2**. **Scenario:** This issue is observed in APs running AOS-W 8.3.0.2. **Workaround:** None.	AP-Wireless	All platforms	AOS-W 8.3.0.2
191638	**Symptom:** Clients do not receive the multicast packets as the IPv6 streaming is not working as expected. **Scenario:** This issue occurs when there are clients on two different nodes acting as source and destination. This issue is observed in a cluster where MLD proxy is enabled and the managed devices are running AOS-W 8.4.0.0. **Workaround:** None	Multicast	All platforms	AOS-W 8.4.0.0
191667	**Symptom:** The **SNMP** process crashes in a managed device. **Scenario:** This issue occurs when the **SNMP** process receives a request to query the table, **wlsxSwitchAccessPointTable**. This issue is observed in OAW-4750XM switches running AOS-W 8.2.1.1 or later versions. **Workaround:** None.	SNMP	OAW-4750XM switches	AOS-W 8.2.2.1
191811	**Symptom:** The AirGroup cache entry is dropping HP wired printers after cache expiry. **Scenario:** This issue is observed in Mobility Masters running AOS-W 8.3.0.3 or later versions. **Workaround:** None.	AirGroup	All platforms	AOS-W 8.3.0.3
191816	**Symptom:** A managed device crashes and reboots unexpectedly. The log file lists the reason for the event as **Reboot Cause: Kernel Panic (Intent:cause:register 12:86:0:20).** **Scenario:** This issue is observed in OAW-4450 stand-alone switches running AOS-W 8.2.2.0 or later versions. **Workaround:** None.	switch-Platform	OAW-4450 standalone switches	AOS-W 8.2.2.0

Table 7: *Known Issues in AOS-W 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version
192100	**Symptom:** The **DDS** process in managed device crashes unexpectedly. **Scenario:** This issue is observed in managed devices running AOS-W 8.2.1.1 or later versions. **Workaround:** None.	Base OS Security	All platforms	AOS-W 8.2.1.1
192243	**Symptom:** A Mobility Master crashes and reboots unexpectedly. The log files list the reason for the event as **Reboot Cause: Kernel Panic (Intent:cause:register 12:86:40:2.** **Scenario:** This issue occurs when USB disconnects are seen from the internal flash device. This issue is observed in OmniAccess Mobility Controller running AOS-W 8.2.2.2 or later versions. **Workaround:** None.	switch- Platform	All platforms	AOS-W 8.2.2.2
192344	**Symptom:** The **licensemgr** process crashes unexpectedly in a Mobility Master. The log file lists the reason for the event as **out of memory**. **Scenario:** This issue is observed in Mobility Masters running AOS-W 8.4.0.0. **Workaround:** None.	Licensing	All platforms	AOS-W 8.4.0.0
192346	**Symptom:** An AP drops Skype calls that originate from a client. **Scenario:** This issue is observed in OAW-AP300 Series, OAW-AP310 Series, OAW-AP320 Series, OAW-AP330 Series, OAW-AP340 Series, OAW-AP360 Series, and OAW-AP370 Series access points running AOS-W 8.4.0.0 **Workaround:** None.	AP-Wireless	OAW-AP300 Series, OAW-AP310 Series, OAW-AP320 Series, OAW-AP330 Series, OAW-AP340 Series, OAW-AP360 Series, and OAW-AP370 Series access points	AOS-W 8.4.0.0
192349	**Symptom:** The **mDNS** process running in a managed device consumes more memory than the typical threshold limit. **Scenario:** This issue is observed in managed devices running AOS-W 8.4.0.0 **Workaround:** None.	AirGroup	All platforms	AOS-W 8.4.0.0

Table 7: *Known Issues in AOS-W 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version
192378	**Symptom:** A client faces connectivity problem. **Scenario:** This issue occurs when the **enforce DHCP** feature is enabled. This issue is observed in managed devices running AOS-W 8.3.0.4 **Workaround:** None.	switch-Datapath	All platforms	AOS-W 8.3.0.4
192430	**Symptom:** A cluster upgrade fails unexpectedly. The log file lists the reason for the event as **Image copy fail**. **Scenario:** This issue is observed in managed devices running AOS-W 8.2.1.1 in a cluster topology. **Workaround:** None.	Image Upgrade	All platforms	AOS-W 8.2.1.1
192457	**Symptom:** The **datapath** process crashes unexpectedly in a stand-alone switch. **Scenario:** This issue is observed in OAW-4550 switches running AOS-W 8.4.0.0 **Workaround:** None.	switch-Datapath	7210 switches	AOS-W 8.4.0.0
192484	**Symptom:** Some processes crash after deleting files from the storage space. **Scenario:** This issue is observed in Mobility Masters running AOS-W 8.3.0.2 or later versions. **Workaround:** None.	AirMatch	All platforms	AOS-W 8.3.0.2
192486	**Symptom:** An OAW-IAP fails to receive an IP address and gets terminated. **Scenario:** This issue is observed in stand-alone switches running AOS-W 8.0.0.0 or later versions. **Workaround:** None.	IPsec	All platforms	AOS-W 8.0.0.0
192511	**Symptom:** The client usage graph of an AP displays low usage of client in the WebUI. **Scenario:** This issue is observed in OAW-4750XM switches running AOS-W 8.2.2.0 in a Mobility Master-Managed Device topology. **Workaround:** None.	Station Management	OAW-4750XM switches	AOS-W 8.2.2.0
192618	**Symptom:** A managed device crashes and reboots unexpectedly. **Scenario:** This issue is observed in managed devices running AOS-W 8.2.2.0 or later versions. **Workaround:** None.	Database	All platforms	AOS-W 8.2.2.0
192642	**Symptom:** The **Dashboard > Access Points** page in a Mobility Master does not display the correct statistics of an AP. **Scenario:** This issue is observed in Mobility Masters running AOS-W 8.4.0.0. **Workaround:** None.	WebUI	All platforms	AOS-W 8.4.0.0

Table 7: *Known Issues in AOS-W 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version
192645	**Symptom:** An API lists the station information twice even though the user-table has only one entry for the user. **Scenario:** This issue is observed in managed devices running AOS-W 8.4.0.0. **Workaround:** None.	NBAPI-Helper	All platforms	AOS-W 8.4.0.0
192649	**Symptom:** A license is not sent to a managed device. **Scenario:** This issue occurs when an external Mobility Master or a stand-alone switch is used as a licensing server. This issue is observed in managed devices running AOS-W 8.3.0.3. **Workaround:** None.	Licensing	All platforms	AOS-W 8.3.0.3
186324 192783	**Symptom:** In the **Dashboard > Infrastructure > Cluster** page, clicking on **Active Clients Count** always displays the wireless clients table even if the table is empty. **Scenario:** This issue is observed in managed devices running AOS-W 8.4.0.0. **Workaround:** None.	WebUI	All platforms	AOS-W 8.4.0.0
192901 194140	**Symptom:** Some APs are unable to connect to the managed device. **Scenario:** This issue occurred when the managed device is upgraded from 8.3.0.3 FIPS version to 8.4.0.0 FIPS version. This issue is observed in OAW-AP210AP-318, OAW-AP387, OAW-AP310 Series, OAW-AP320 Series, and OAW-AP370 Series access points connected to managed devices running AOS-W 8.4.0.0 FIPS version. **Workaround:** Downgrade the managed device to 8.3.0.3 FIPS version and factory reset the access points.	AP-Platform	OAW-AP210AP-318, OAW-AP387, OAW-AP310 Series, OAW-AP320 Series, and OAW-AP370 Series access points	AOS-W 8.4.0.0 FIPS
192812	**Symptom:** A per user tunneled-node client is unable to receive stream when the User Anchor Controller (UAC) fails over twice. **Scenario:** This issue occurs when two per user tunneled-node clients with different VLANs are requesting for the same stream and the **no-vlan** parameter is enabled on the per user tunneled-node clients. This issue is observed in managed devices running AOS-W 8.4.0.0. **Workaround:** None.	Multicast	All platforms	AOS-W 8.4.0.0

Table 7: *Known Issues in AOS-W 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version
192915	**Symptom:** Per user tunneled-node clients received duplicate multicast packets. **Scenario:** This issue occurs in the following scenarios: ■ when multicast proxy feature is enabled on user VLANs. ■ when IGMP proxy is enabled for user VLANs. This issue is observed in managed devices running AOS-W 8.4.0.0. **Workaround:** None.	Tunnel-node-manager	All platforms	AOS-W 8.4.0.0
193225	**Symptom:** The **Tunneled clients** column under **Dashboard > Infrastructure > Tunneled Switches** table displays zero. **Scenario:** This issue is observed in Mobility Master running AOS-W 8.4.0.0 or later versions. **Workaround:** None.	WebUI	All platforms	AOS-W 8.4.0.0
193297	**Symptom:** The **Tunneled Switches** table under **Dashboard > Infrastructure > Access Devices** displays zero **Tunneled Clients** for IPv6 tunnels between Mobility Master and the Managed Device. **Scenario:** This issue is observed in Mobility Masters running AOS-W 8.4.0.0. **Workaround:** None.	WebUI	All platforms	AOS-W 8.4.0.0

Table 7: *Known Issues in AOS-W 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version
193378	**Symptom:** The **all deviceClass** filter is applied by default to an IoT transport profile and when this filter is removed, it is not saved in configuration on the managed device. **Scenario:** This issue occurs when a **Telemetry-HTTPS** or **Telemetry-Websocket IoT transport** profile is created. This issue is observed in managed devices running AOS-W 8.4.0.0 in Mobility Master-Managed Device topology **Workaround:** After creating an IoT transport profile, save the configuration, remove the **all deviceClass** filter, and save the configuration.	BLE	All platforms	AOS-W 8.4.0.0
193441	**Symptom:** The **Station Management** process crashes continuously in the managed device because the database upgrade in a managed device fails. **Scenario:** This issue occurs when a managed device running AOS-W 8.4.0.0 version is downgraded to AOS-W 8.3.0.0 or lower versions, and then the **ap gap-db reinit-db** command is executed. Post this, the managed device is again upgraded to AOS-W 8.4.0.0 by changing the boot partition. This issue is observed in managed devices running AOS-W 8.4.0.0. **Workaround:** Copy AOS-W 8.4.0.0 image in any of the partitions instead of switching boot partition using **boot system partition** command.	Database	All platforms	AOS-W 8.4.0.0
193538	**Symptom:** The **Station Management** process crashes continuously in a switch. **Scenario:** This issue occurs when a stand-alone switch running any AOS-W 8.x version is converted to managed node using the **write erase** command and then, upgraded to AOS-W 8.4.0.0 version and rebooted in the managed node. Post this, the switch is again converted to stand-alone mode using **write erase** command. This issue is observed in switches running AOS-W 8.4.0.0 **Workaround:** Execute the **write erase all** command when converting a switch from stand-alone mode to managed node and vice-versa.	Database	All platforms	AOS-W 8.4.0.0

Chapter 7 Upgrade Procedure

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

CAUTION

Read all the information in this chapter before upgrading your Mobility Master, managed device, master switch, and/or stand-alone switch.

Topics in this chapter include:

- Migrating from AOS-W 6.x to AOS-W 8.x on page 90
- Important Points to Remember and Best Practices on page 91
- Memory Requirements on page 91
- MIB Files on page 1
- Memory Requirements on page 91
- Backing up Critical Data on page 92
- Upgrading on page 94
- Downgrading on page 97
- Before You Call Technical Support on page 99

Migrating from AOS-W 6.x to AOS-W 8.x

If you are migrating from AOS-W 6.x to AOS-W 8.x, note the following points:

- Use the interactive migration tool provided on the customer support site to migrate any AOS-W 6.x deployments to one of the following AOS-W 8.x deployments:
  - Master-Local setup to Mobility Master
  - All-Master setup to Mobility Master
  - Master-Local setup to Master switch Mode in AOS-W 8.x
  - Stand-alone switch running AOS-W 8.x

For more information, refer to the *AOS-W 8.x Migration Guide*.

NOTE

Licenses are not migrated by the migration tool from any of the devices to Mobility Master. However, the licenses are preserved when migrating to AOS-W 8.x Master switch Mode or stand-alone switches. For more information on License migration, refer to *Alcatel-Lucent Mobility Master Licensing Guide*.

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 must 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 managed device? Verify this information by navigating to the **Dashboard > 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 managed device (DNS, DHCP Option, Broadcast)?
  - What version of AOS-W is currently on the managed device?
  - Are all managed devices running the same version of software?
  - Which services are used on the managed device (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 managed device. 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 you encounter any issue 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, if required.
- Before you upgrade to this version of AOS-W, assess your software license requirements and load any new or expanded licenses that you might require. For a detailed description of these new license modules, see the “Software Licenses” chapter in the *AOS-W 8.x.0.0 User Guide*.

Memory Requirements

All Alcatel-Lucent managed devices store critical configuration data on an onboard compact flash memory module. Ensure that there is always free flash space on the managed device. 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 100 MB of free memory available for an upgrade using the WebUI or CLI. Execute the **show memory** command to identify the amount of free memory available using the CLI. Do not proceed unless 100 MB of free memory is available. To recover memory, reboot the managed device. After the managed device comes up, upgrade immediately.
- Confirm that there is at least 150 MB of flash space available for an upgrade using the WebUI or CLI. Using the CLI, execute the **show storage** command to identify the amount of flash space available.

CAUTION

In certain situations, a reboot or a shutdown could cause the managed device 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 managed device logs, crash data, or flash backups should be copied to a location off the managed device, then deleted from the managed device to free up flash space. You can delete the following files from the managed device 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 managed device.
- **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 managed device.
- **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 managed device.

Use the following procedure to delete files and free up memory space:

In the WebUI

From the Mobility Master, navigate to **Diagnostic > Technical Support > Delete Files** and remove any aging log files or redundant backups which may have been created by administrator.

In the CLI

```
(host) #delete filename <filename>
```

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
- Custom captive portal pages
- x.509 certificates
- Logs

- Flashbackup

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 a managed device:

1. In the Mobility Master node hierarchy, navigate to the **Maintenance > Configuration Management > Backup** page.
2. Click **Create Backup** to backup the contents of the compact flash file system to the **flashbackup.tar.gz file**.
3. Click **Copy Backup** to copy the file to an external server.

   You can copy the backup file from the external server to the compact flash file system using the file utility in the **Diagnostics > Technical Support > Copy Files** page.
4. To restore the backup file to the Compact Flash file system, navigate to the **Maintenance > Configuration Management > Restore** 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 command line:

1. Make sure you are in the **enable** mode in the 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 take the flash backup.......
File flashbackup.tar.gz created successfully on flash.
Please copy it out of the controller and delete it when done.
```
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 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
Please wait while we restore the flash backup........
Flash restored successfully.
Please reload (reboot) the controller for the new files to take effect.
```

Upgrading

The following sections provide the procedures for upgrading your WLAN network to the latest AOS-W version using the WebUI or CLI.

AOS-W 8.4.0.0 Upgrade Notes

Before you upgrade the Mobility Master from AOS-W 8.0.0.0 to AOS-W 8.4.0.0, note the following points:

- AOS-W 8.4.0.0 supports only a maximum of 3 network adapters for Mobility Master and 4 network adapters for Mobility Master Virtual Appliance. If you have 4 network adapters on your AOS-W 8.0.0.0 Mobility Master Virtual Appliance, you must remove one before upgrading to AOS-W 8.4.0.0 to avoid upgrade failure. To remove a network adapter from AOS-W 8.0.0.0 Mobility Master Virtual Appliance:

NOTE

Before you remove the additional network adapter from the Mobility Master Virtual Appliance, ensure that you copy the AOS-W 8.0.0.0 image on the system partition of Mobility Master Virtual Appliance.

1. Log in to the vSphere client.
2. Select the Mobility Master VM instance and click **Shut down the virtual machine**.
3. Click **Edit Virtual machine settings**.
4. From the **Hardware** tab, select and remove a network adapter that is not active.

- Before upgrading to AOS-W 8.4.0.0 from AOS-W 8.0.0.0, ensure that you configure the MAC address of the management interface as the peer MAC address, if the peer is a Mobility Master Virtual Appliance or Mobility Master. Before reloading the new image on Mobility Master, alter the peer MAC address using the following procedure in the WebUI:

1. From the **Managed Network** node hierarchy, select the managed device.
2. Navigate to **Configuration > Controllers** and enter the management interface MAC address in the **Peer MAC address of master** field.
3. Click **Submit**, and then click **Continue** in the reload popup.
4. Click **Pending Changes**.
5. In the **Pending Changes** window, select the check box and click **Deploy changes**.

Alternatively, you can execute the following CLI command on the Mobility Master at the device level:

```
(host) [<device-mac-address>] (config) #masterip <ipaddr> ipsec <key> peer-mac-1 <mgmt-interface-mac> peer-mac-2 <mgmt-interface-mac> interface vlan <id>
```

- Before upgrading to AOS-W 8.4.0.0, you must share the licenses within the global licensing pool by executing the **license-pool-profile-root** command:

```
(host) [mm](config) #license-pool-profile-root
(host) [mm](License root(/) pool profile) #acr-license-enable
```

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

You can install the software image from a TFTP or FTP server using the WebUI page.

1. Download AOS-W 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 at the factory. Therefore, even if you do not manually verify the SHA hash of a software image, the managed device will not load a corrupted image.

4. Log in to the AOS-W WebUI from the Mobility Master.
5. Navigate to the **Maintenance > Software Management > Upgrade** page.
   a. Select the **Local File** option from the **Upgrade using** drop-down list.
   b. Click **Browse** from the **Image file name** field to navigate to the saved image file on your PC or workstation.
6. Select the downloaded image file.
7. Choose the partition from the **Partition to Upgrade** option.
8. Enable the **Reboot Controller After Upgrade** toggle switch to automatically reboot after upgrading. If you do not want to reboot immediately, disable this option.

NOTE

Note that the upgrade will not take effect until you reboot.

9. Select the **Save Current Configuration** option.
10. Click **Upgrade**.

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

11. Click **OK**.

    If you chose to automatically reboot 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 **Dashboard > WLANs** 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 **Dashboard > Access Points** page to determine if your APs are up and ready to accept clients.
3. Verify that the number of access points and clients are what you would expect.
4. Test a different type of client for each access method that you use, and in different locations when possible.
5. Complete a 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.

In 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 a Recent Version of AOS-W

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

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

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

   or

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

   or

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

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

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

5. Execute the **copy** command to load the new image onto the non-boot 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>
```

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

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

7. Reboot the switch.

```
(host)# reload
```

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

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

When the 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.

Before You Begin

Before you reboot the switch with the pre-upgrade software version, you must perform the following steps:

1. Back up your switch. For details, see Backing up Critical Data on page 92.
2. Verify that the control plane security is disabled.
3. Set the switch to boot with the previously saved pre-AOS-W 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 the 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 flash backup from the file stored on the switch. Do not restore the AOS-W 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, the changes do not appear in RF Plan in the downgraded AOS-W version.
- If you installed any certificates while running AOS-W, 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 pre-upgrade configuration file is on an external FTP/TFTP server, copy the file to the switch by navigating to the **Diagnostics > Technical Support > Copy Files** page.
   a. For **Select source file** option, select FTP or TFTP server, and enter the IP address of the FTP or TFTP server and the name of the pre-upgrade configuration file.
   b. For **Select destination file** option, enter a file name (other than default.cfg) for Flash File System.
2. Determine the partition on which your previous software image is stored by navigating to the **Maintenance > Software Management > Upgrade** page. If there is no previous software image stored on your system partition, load it into the backup system partition by performing the following steps:

CAUTION

> You cannot load a new image into the active system partition

   a. Enter the FTP/TFTP server address and image file name.
   b. Select the backup system partition.
   c. Click **Upgrade**.
3. Navigate to the **Maintenance > Software Management > Boot Parameters** page.
   a. Select the system partition that contains the pre-upgrade image file as the boot partition.
   b. Click **Apply**.
4. Navigate to the **Maintenance > Software Management > Reboot** page. Select **Save configuration before reboot** option and click **Reboot**. The switch reboots after the countdown period.
5. When the boot process is complete, verify that the switch is using the correct software by navigating to the **Maintenance > Software Management > About** 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 pre-upgrade configuration file is on an external FTP/TFTP server, use the following command to copy it to the switch:

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

   or

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

2. Set the switch to boot with your pre-upgrade configuration file.

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

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

```
#show image version
```

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

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

5. Reboot the switch.

```
(host) # reload
```

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

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

Before You Call Technical Support

Before you call 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 device 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 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 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 the logs.
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 device) or any recent changes to your Alcatel-Lucent device 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 Alcatel-Lucent device site access information, if possible.

Glossary of Terms

The following table provides a brief description of the terminology used in this guide.

3DES

Triple Data Encryption Standard. 3DES is a symmetric-key block cipher that applies the DES cipher algorithm three times to each data block.

3G

Third Generation of Wireless Mobile Telecommunications Technology. See W-CDMA.

3GPP

Third Generation Partnership Project. 3GPP is a collaborative project aimed at developing globally acceptable specifications for third generation mobile systems.

4G

Fourth Generation of Wireless Mobile Telecommunications Technology. See LTE.

802.11

802.11 is an evolving family of specifications for wireless LANs developed by a working group of the Institute of Electrical and Electronics Engineers (IEEE). 802.11 standards use the Ethernet protocol and Carrier Sense Multiple Access with collision avoidance (CSMA/CA) for path sharing.

802.11 bSec

802.11 bSec is an alternative to 802.11i. The difference between bSec and standard 802.11i is that bSec implements Suite B algorithms wherever possible. Notably, Advanced Encryption Standard-Counter with CBC-MAC is replaced by Advanced Encryption Standard - Galois/Counter Mode, and the Key Derivation Function (KDF) of 802.11i is upgraded to support SHA-256 and SHA-384.

802.11a

802.11a provides specifications for wireless systems. Networks using 802.11a operate at radio frequencies in the 5 GHz band. The specification uses a modulation scheme known as orthogonal frequency-division multiplexing (OFDM) that is especially well suited to use in office settings. The maximum data transfer rate is 54 Mbps.

802.11ac

802.11ac is a wireless networking standard in the 802.11 family that provides high-throughput WLANs on the 5 GHz band.

802.11b

802.11b is a WLAN standard often called Wi-Fi and is backward compatible with 802.11. Instead of the Phase-Shift Keying (PSK) modulation method used in 802.11 standards, 802.11b uses Complementary Code Keying (CCK) that allows higher data speeds and makes it less susceptible to multipath-propagation interference. 802.11b operates in the 2.4 GHz band and the maximum data transfer rate is 11 Mbps.

802.11d

802.11d is a wireless network communications specification for use in countries where systems using other standards in the 802.11 family are not allowed to operate. Configuration can be fine-tuned at the Media Access Control (MAC) layer level to comply with the rules of the country or district in which the network is to be used. Rules are subject to variation and include allowed frequencies, allowed power levels, and allowed signal bandwidth. 802.11d facilitates global roaming.

802.11e

802.11e is an enhancement to the 802.11a and 802.11b specifications that enhances the 802.11 Media Access Control layer with a coordinated Time Division Multiple Access (TDMA) construct. It adds error-correcting mechanisms for delay-sensitive applications such as voice and video. The 802.11e specification provides seamless interoperability between business, home, and public environments such as airports and hotels, and offers all subscribers high-speed Internet access with full-motion video, high-fidelity audio, and VoIP.

802.11g

802.11g offers transmission over relatively short distances at up to 54 Mbps, compared with the 11 Mbps theoretical maximum of 802.11b standard. 802.11g employs Orthogonal Frequency Division Multiplexing (OFDM), the modulation scheme used in 802.11a, to obtain higher data speed. Computers or terminals set up for 802.11g can fall back to speed of 11 Mbps, so that 802.11b and 802.11g devices can be compatible within a single network.

802.11h

802.11h is intended to resolve interference issues introduced by the use of 802.11a in some locations, particularly with military Radar systems and medical devices. Dynamic Frequency Selection (DFS) detects the presence of other devices on a channel and automatically switches the network to another channel if and when such signals are detected. Transmit Power Control (TPC) reduces the radio frequency (RF) output power of each network transmitter to a level that minimizes the risk of interference.

802.11i

802.11i provides improved encryption for networks that use 802.11a, 802.11b, and 802.11g standards. It requires new encryption key protocols, known as Temporal Key Integrity Protocol (TKIP) and Advanced Encryption Standard (AES).

802.11j

802.11j is a proposed addition to the 802.11 family of standards that incorporates Japanese regulatory extensions to 802.11a; the main intent is to add channels in the radio frequency (RF) band of 4.9 GHz to 5.0 GHz.

802.11k

802.11k is an IEEE standard that enables APs and client devices to discover the best available radio resources for seamless BSS transition in a WLAN.

802.11m

802.11m is an Initiative to perform editorial maintenance, corrections, improvements, clarifications, and interpretations relevant to documentation for 802.11 family specifications.

802.11n

802.11n is a wireless networking standard to improve network throughput over the two previous standards, 802.11a and 802.11g. With 802.11n, there will be a significant increase in the maximum raw data rate from 54 Mbps to 600 Mbps with the use of four spatial streams at a channel width of 40 MHz.

802.11r

802.11r is an IEEE standard for enabling seamless BSS transitions in a WLAN. 802.11r standard is also referred to as Fast BSS transition.

802.11u

802.11u is an amendment to the IEEE 802.11 WLAN standards for connection to external networks using common wireless devices such as smartphones and tablet PCs. The 802.11u protocol provides wireless clients with a streamlined mechanism to discover and authenticate to suitable networks, and allows mobile users to roam between partner networks without additional authentication. An 802.11u-capable device supports the Passpoint technology from the Wi-Fi Alliance Hotspot 2.0 R2 Specification that simplifies and automates access to public Wi-Fi.

802.11v

802.11v is an IEEE standard that allows client devices to exchange information about the network topology and RF environment. This information is used for assigning best available radio resources for the client devices to provide seamless connectivity.

802.1Q

802.1Q is an IEEE standard that enables the use of VLANs on an Ethernet network. 802.1Q supports VLAN tagging.

802.1X

802.1X is an IEEE standard for port-based network access control designed to enhance 802.11 WLAN security. 802.1X provides an authentication framework that allows a user to be authenticated by a central authority.

802.3af

802.3af is an IEEE standard for Power over Ethernet (PoE) version that supplies up to 15.4W of DC power. See PoE.

802.3at

802.3at is an IEEE standard for PoE version that supplies up to 25.5W of DC power. See PoE+.

A-MPDU

Aggregate MAC Protocol Data Unit. A-MPDU is a method of frame aggregation, where several MPDUs are combined into a single frame for transmission.

A-MSDU

Aggregate MAC Service Data Unit. A-MSDU is a structure containing multiple MSDUs, transported within a single (unfragmented) data MAC MPDU.

AAA

Authentication, Authorization, and Accounting. AAA is a security framework to authenticate users, authorize the type of access based on user credentials, and record authentication events and information about the network access and network resource consumption.

ABR

Area Border Router. ABR is used for establishing connection between the backbone networks and the Open Shortest Path First (OSPF) areas. ABR is located near the border of one or more OSPF areas.

AC

Access Category. As per the IEEE 802.11e standards, AC refers to various levels of traffic prioritization in Enhanced Distributed Channel Access (EDCA) operation mode. The WLAN applications prioritize traffic based on the Background, Best Effort, Video, and Voice access categories. AC can also refer to Alternating Current, a form of electric energy that flows when the appliances are plugged to a wall socket.

ACC

Advanced Cellular Coexistence. The ACC feature in APs enable WLANs to perform at peak efficiency by minimizing interference from 3G/4G/LTE networks, distributed antenna systems, and commercial small cell/femtocell equipment.

Access-Accept

Response from the RADIUS server indicating successful authentication and containing authorization information.

Access-Reject

Response from RADIUS server indicating that a user is not authorized.

Access-Request

RADIUS packet sent to a RADIUS server requesting authorization.

Accounting-Request

RADIUS packet type sent to a RADIUS server containing accounting summary information.

Accounting-Response

RADIUS packet sent by the RADIUS server to acknowledge receipt of an Accounting-Request.

ACE

Access Control Entry. ACE is an element in an ACL that includes access control information.

ACI

Adjacent Channel Interference. ACI refers to interference or interruptions detected on a broadcasting channel, caused by too much power on an adjacent channel in the spectrum.

ACL

Access Control List. ACL is a common way of restricting certain types of traffic on a physical port.

Active Directory

Microsoft Active Directory. The directory server that stores information about a variety of things, such as organizations, sites, systems, users, shares, and other network objects or components. It also provides authentication and authorization mechanisms, and a framework within which related services can be deployed.

ActiveSync

Mobile data synchronization app developed by Microsoft that allows a mobile device to be synchronized with either a desktop or a server running compatible software products.

ad hoc network

An ad hoc network is a network composed of individual devices communicating with each other directly. Many ad hoc networks are Local Area Networks (LANs) where computers or other devices are enabled to send data directly to one another rather than going through a centralized access point.

ADO

Active X Data Objects is a part of Microsoft Data Access Components (MDACs) that enables client applications to access data sources through an (Object Linking and Embedding Database) OLE DB provider. ADO supports key features for building client-server and Web-based applications.

ADP

Aruba Discovery Protocol. ADP is an Aruba proprietary Layer 2 protocol. It is used by the APs to obtain the IP address of the TFTP server from which it downloads the AP boot image.

AES

Advanced Encryption Standard. AES is an encryption standard used for encrypting and protecting electronic data. The AES encrypts and decrypts data in blocks of 128 bits (16 bytes), and can use keys of 128 bits, 192 bits, and 256 bits.

AIFSN

Arbitrary Inter-frame Space Number. AIFSN is set by the AP in beacon frames and probe responses. AIFS is a method of prioritizing a particular category of traffic over the other, for example prioritizing voice or video messages over email.

AirGroup

The application that allows the end users to register their personal mobile devices on a local network and define a group of friends or associates who are allowed to share them. AirGroup is primarily designed for colleges and other institutions. AirGroup uses zero configuration networking to allow Apple mobile devices, such as the AirPrint wireless printer service and the AirPlay mirroring service, to communicate over a complex access network topology.

AirWave Management Client

AirWave Management Client is a Windows software utility that enables client devices (such as a laptop) to act as passive RF sensors and augments the AirWave RAPIDS module.

ALE

Analytics and Location Engine. ALE gives visibility into everything the wireless network knows. This enables customers and partners to gain a wealth of information about the people on their premises. This can be very important for many different verticals and use cases. ALE includes a location engine that calculates associated and unassociated device location periodically using context streams, including RSSI readings, from WLAN controllers or Instant clusters.

ALG

Application Layer Gateway. ALG is a security component that manages application layer protocols such as SIP, FTP and so on.

AM

Air Monitor. AM is a mode of operation supported on wireless APs. When an AP operates in the Air Monitor mode, it enhances the wireless networks by collecting statistics, monitoring traffic, detecting intrusions, enforcing security policies, balancing wireless traffic load, self-healing coverage gaps, and more. However, clients cannot connect to APs operating in the AM mode.

AMON

Advanced Monitoring. AMON is used in Aruba WLAN deployments for improved network management, monitoring and diagnostic capabilities.

AMP

AirWave Management Platform. AMP is a network management system for configuring, monitoring, and upgrading wired and wireless devices on your network.

ANQP

Access Network Query Protocol. ANQP is a query and a response protocol for Wi-Fi hotspot services. ANQP includes information Elements (IEs) that can be sent from the AP to the client to identify the AP network and service provider. The IEs typically include information about the domain name of the AP operator, the IP addresses available at the AP, and information about potential roaming partners accessible through the AP. If the client responds with a request for a specific IE, the AP will send a Generic Advertisement Service (GAS) response frame with the configured ANQP IE information.

ANSI

American National Standards Institute. It refers to the ANSI compliance standards for products, systems, services, and processes.

API

Application Programming Interface. Refers to a set of functions, procedures, protocols, and tools that enable users to build application software.

app

Short form for application. It generally refers to the application that is downloaded and used on mobile devices.

ARM

Adaptive Radio Management. ARM dynamically monitors and adjusts the network to ensure that all users are allowed ready access. It enables full utilization of the available spectrum to support maximum number of users by intelligently choosing the best RF channel and transmit power for APs in their current RF environment.

ARP

Address Resolution Protocol. ARP is used for mapping IP network address to the hardware MAC address of a device.

Aruba Activate

Aruba Activate is a cloud-based service that helps provision your Aruba devices and maintain your inventory. Activate automates the provisioning process, allowing a single IT technician to easily and rapidly deploy devices throughout a distributed enterprise network.

ASCII

American Standard Code for Information Interchange. An ASCII code is a numerical representation of a character or an action.

B-RAS

Broadband Remote Access Server. A B-RAS is a server that facilitates and converges traffic from multiple Internet traffic resources such as cable, DSL, Ethernet, or Broadband wireless.

band

Band refers to a specified range of frequencies of electromagnetic radiation.

BGP

Border Gateway Protocol. BGP is a routing protocol for exchanging data and information between different host gateways or autonomous systems on the Internet.

BLE

Bluetooth Low Energy. The BLE functionality is offered by Bluetooth® to enable devices to run for long durations with low power consumption.

BMC

Beacon Management Console. BMC manages and monitors beacons from the BLE devices. The BLE devices are used for location tracking and proximity detection.

BPDU

Bridge Protocol Data Unit. A BPDU is a data message transmitted across a local area network to detect loops in network topologies.

BRE

Basic Regular Expression. The BRE syntax standards designed by the IEEE provides extension to the traditional Simple Regular Expressions syntax and allows consistency between utility programs such as grep, sed, and awk.

BSS

Basic Service Set. A BSS is a set of interconnected stations that can communicate with each other. BSS can be an independent BSS or infrastructure BSS. An independent BSS is an ad hoc network that does not include APs, whereas the infrastructure BSS consists of an AP and all its associated clients.

BSSID

Basic Service Set Identifier. The BSSID identifies a particular BSS within an area. In infrastructure BSS networks, the BSSID is the MAC address of the AP. In independent BSS or ad hoc networks, the BSSID is generated randomly.

BYOD

Bring Your Own Device. BYOD refers to the use of personal mobile devices within an enterprise network infrastructure.

CA

Certificate Authority or Certification Authority. Entity in a public key infrastructure system that issues certificates to clients. A certificate signing request received by the CA is converted into a certificate when the CA adds a signature generated with a private key. See digital certificate.

CAC

Call Admission Control. CAC regulates traffic volume in voice communications. CAC can also be used to ensure or maintain a certain level of audio quality in voice communications networks.

CALEA

Communications Assistance for Law Enforcement Act. To comply with the CALEA specifications and to allow lawful interception of Internet traffic by the law enforcement and intelligence agencies, the telecommunications carriers and manufacturers of telecommunications equipment are required to modify and design their equipment, facilities, and services to ensure that they have built-in surveillance capabilities.

Campus AP

Campus APs are used in private networks where APs connect over private links (LAN, WLAN, WAN or MPLS) and terminate directly on controllers. Campus APs are deployed as part of the indoor campus solution in enterprise office buildings, warehouses, hospitals, universities, and so on.

captive portal

A captive portal is a web page that allows the users to authenticate and sign in before connecting to a public-access network. Captive portals are typically used by business centers, airports, hotel lobbies, coffee shops, and other venues that offer free Wi-Fi hotspots for the guest users.

CCA

Clear Channel Assessment. In wireless networks, the CCA method detects if a channel is occupied or clear, and determines if the channel is available for data transmission.

CDP

Cisco Discovery Protocol. CDP is a proprietary Data Link Layer protocol developed by Cisco Systems. CDP runs on Cisco devices and enables networking applications to learn about the neighboring devices directly connected to the network.

CDR

Call Detail Record. A CDR contains the details of a telephone or VoIP call, such as the origin and destination addresses of the call, the start time and end time of the call, any toll charges that were added through the network or charges for operator services, and so on.

CEF

Common Event Format. The CEF is a standard for the interoperability of event or log-generating devices and applications. The standard syntax for CEF includes a prefix and a variable extension formatted as key-value pairs.

CGI

Common Gateway Interface. CGI is a standard protocol for exchanging data between the web servers and executable programs running on a server to dynamically process web pages.

CHAP

Challenge Handshake Authentication Protocol. CHAP is an authentication scheme used by PPP servers to validate the identity of remote clients.

CIDR

Classless Inter-Domain Routing. CIDR is an IP standard for creating and allocating unique identifiers for networks and devices. The CIDR IP addressing scheme is used as a replacement for the older IP addressing scheme based on classes A, B, and C. With CIDR, a single IP address can be used to designate many unique IP addresses. A CIDR IP address ends with a slash followed by the IP network prefix, for example, 192.0.2.0/24.

ClearPass

ClearPass is an access management system for creating and enforcing policies across a network to all devices and applications. The ClearPass integrated platform includes applications such as Policy Manager, Guest, Onboard, OnGuard, Insight, Profile, QuickConnect, and so on.

ClearPass Guest

ClearPass Guest is a configurable ClearPass application for secure visitor network access management.

ClearPass Policy Manager

ClearPass Policy Manager is a baseline platform for policy management, AAA, profiling, network access control, and reporting. With ClearPass Policy Manager, the network administrators can configure and manage secure network access that accommodates requirements across multiple locations and multivendor networks, regardless of device ownership and connection method.

CLI

Command-Line Interface. A console interface with a command line shell that allows users to execute text input as commands and convert these commands to appropriate functions.

CN

Common Name. CN is the primary name used to identify a certificate.

CNA

Captive Network Assistant. CNA is a popup page shown when joining a network that has a captive portal.

CoA

Change of Authorization. The RADIUS CoA is used in the AAA service framework to allow dynamic modification of the authenticated, authorized, and active subscriber sessions.

CoS

Class of Service. CoS is used in data and voice protocols for classifying packets into different types of traffic (voice, video, or data) and setting a service priority. For example, voice traffic can be assigned a higher priority over email or HTTP traffic.

CPE

Customer Premises Equipment. It refers to any terminal or equipment located at the customer premises.

CPsec

Control Plane Security. CPsec is a secure form of communication between a controller and APs to protect the control plane communications. This is performed by means of using public-key self-signed certificates created by each master controller.

CPU

Central Processing Unit. A CPU is an electronic circuitry in a computer for processing instructions.

CRC

Cyclic Redundancy Check. CRC is a data verification method for detecting errors in digital data during transmission, storage, or retrieval.

CRL

Certificate Revocation List. CRL is a list of revoked certificates maintained by a certification authority.

cryptobinding

Short for cryptographic binding. A procedure in a tunneled EAP method that binds together the tunnel protocol and the tunneled authentication methods, ensuring the relationship between a collection of data assets. Cryptographic binding focuses on protecting the server; mutual cryptographic binding protects both peer and server.

CSA

Channel Switch Announcement. The CSA element enables an AP to advertise that it is switching to a new channel before it begins transmitting on that channel. This allows the clients, which support CSA, to transition to the new channel with minimal downtime.

CSMA/CA

Carrier Sense Multiple Access / Collision Avoidance. CSMA/CA is a protocol for carrier transmission in networks using the 802.11 standard. CSMA/CA aims to prevent collisions by listening to the broadcasting nodes, and informing devices not to transmit any data until the broadcasting channel is free.

CSR

Certificate Signing Request. In PKI systems, a CSR is a message sent from an applicant to a CA to apply for a digital identity certificate.

CSV

Comma-Separated Values. A file format that stores tabular data in the plain text format separated by commas.

CTS

Clear to Send. The CTS refers to the data transmission and protection mechanism used by the 802.11 wireless networking protocol to prevent frame collision occurrences. See RTS.

CW

Contention Window. In QoS, CW refers to a window set for access categories based on the type of traffic. Based on the type and volume of the traffic, the minimum and maximum values can be calculated to provide a wider window when necessary.

DAI

Dynamic ARP inspection. A security feature that validates ARP packets in a network.

DAS

Distributed Antenna System. DAS is a network of antenna nodes strategically placed around a geographical area or structure for additional cellular coverage.

dB

Decibel. Unit of measure for sound or noise and is the difference or ratio between two signal levels.

dBm

Decibel-Milliwatts. dBm is a logarithmic measurement (integer) that is typically used in place of mW to represent receive-power level. AMP normalizes all signals to dBm, so that it is easy to evaluate performance between various vendors.

DCB

Data Center Bridging. DCB is a collection of standards developed by IEEE for creating a converged data center network using Ethernet.

DCE

Data Communication Equipment. DCE refers to the devices that establish, maintain, and terminate communication network sessions between a data source and its destination.

DCF

Distributed Coordination Function. DCF is a protocol that uses carrier sensing along with a four-way handshake to maximize the throughput while preventing packet collisions.

DDMO

Distributed Dynamic Multicast Optimization. DDMO is similar to Dynamic Multicast Optimization (DMO) where the multicast streams are converted into unicast streams on the AP instead of the controller, to enhance the quality and reliability of streaming videos, while preserving the bandwidth available to non-video clients.

DES

Data Encryption Standard. DES is a common standard for data encryption and a form of secret key cryptography, which uses only one key for encryption and decryption.

designated router

Designated router refers to a router interface that is elected to originate network link advertisements for networks using the OSPF protocol.

destination NAT

Destination Network Address Translation. Destination NAT is a process of translating the destination IP address of an end route packet in a network. Destination NAT is used for redirecting the traffic destined to a virtual host to the real host, where the virtual host is identified by the destination IP address and the real host is identified by the translated IP address.

DFS

Dynamic Frequency Selection. DFS is a mandate for radio systems operating in the 5 GHz band to be equipped with means to identify and avoid interference with Radar systems.

DFT

Discrete Fourier Transform. DFT converts discrete-time data sets into a discrete-frequency representation. See FFT.

DHCP

Dynamic Host Configuration Protocol. A network protocol that enables a server to automatically assign an IP address to an IP-enabled device from a defined range of numbers configured for a given network.

DHCP snooping

DHCP snooping enables the switch to monitor and control DHCP messages received from untrusted devices that are connected to the switch.

digital certificate

A digital certificate is an electronic document that uses a digital signature to bind a public key with an identity—information such as the name of a person or an organization, address, and so forth.

Digital wireless pulse

A wireless technology for transmitting large amounts of digital data over a wide spectrum of frequency bands with very low power for a short distance. Ultra Wideband radio can carry a huge amount of data over a distance up to 230 ft at very low power (less than 0.5 mW), and has the ability to carry signals through doors and other obstacles that tend to reflect signals at more limited bandwidths and a higher power.

Disconnect-Ack

Disconnect-Ack is a NAS response packet to a Disconnect-Request, which indicates that the session was disconnected.

Disconnect-Nak

Disconnect-Nak is NAS response packet to a Disconnect-Request, which indicates that the session was not disconnected.

Disconnect-Request

Disconnect-Request is a RADIUS packet type sent to a NAS requesting that a user or session be disconnected.

distribution certificate

Distribution certificate is used for digitally signing iOS mobile apps to enable enterprise app distribution. It verifies the identity of the app publisher.

DLNA

Digital Living Network Alliance. DLNA is a set of interoperability guidelines for sharing digital media among multimedia devices.

DMO

Dynamic Multicast Optimization. DMO is a process of converting multicast streams into unicast streams over a wireless link to enhance the quality and reliability of streaming videos, while preserving the bandwidth available to non-video clients.

DN

Distinguished Name. A series of fields in a digital certificate that, taken together, constitute the unique identity of the person or device that owns the digital certificate. Common fields in a DN include country, state, locality, organization, organizational unit, and the “common name”, which is the primary name used to identify the certificate.

DNS

Domain Name System. A DNS server functions as a phone book for the intranet and Internet users. It converts human-readable computer host names into IP addresses and IP addresses into host names. It stores several records for a domain name such as an address 'A' record, name server (NS), and mail exchanger (MX) records. The Address 'A' record is the most important record that is stored in a DNS server, because it provides the required IP address for a network peripheral or element.

DOCSIS

Data over Cable Service Interface Specification. A telecommunication standard for Internet access through cable modem.

DoS

Denial of Service. DoS is any type of attack where the attackers send excessive messages to flood traffic and thereby preventing the legitimate users from accessing the service.

DPD

Dead Peer Detection. A method used by the network devices to detect the availability of the peer devices.

DPI

Deep Packet Inspection. DPI is an advanced method of network packet filtering that is used for inspecting data packets exchanged between the devices and systems over a network. DPI functions at the Application layer of the Open Systems Interconnection (OSI) reference model and enables users to identify, categorize, track, reroute, or stop packets passing through a network.

DRT

Downloadable Regulatory Table. The DRT feature allows new regulatory approvals to be distributed for APs without a software upgrade or patch.

DS

Differentiated Services. The DS specification aims to provide uninterrupted quality of service by managing and controlling the network traffic, so that certain types of traffic get precedence.

DSCP

Differentiated Services Code Point. DSCP is a 6-bit packet header value used for traffic classification and priority assignment.

DSL

Digital Subscriber Line. The DSL technology allows the transmission of digital data over telephone lines. A DSL modem is a device used for connecting a computer or router to a telephone line that offers connectivity to the Internet.

DSSS

Direct-Sequence Spread Spectrum. DSSS is a modulation technique used for reducing overall signal interference. This technique multiplies the original data signal with a pseudo random noise spreading code. Spreading of this signal makes the resulting wideband channel more noisy, thereby increasing the resistance to interference. See FHSS.

DST

Daylight Saving Time. DST is also known as summer time that refers to the practice of advancing clocks, so that evenings have more daylight and mornings have less. Typically clocks are adjusted forward one hour near the start of spring and are adjusted backward in autumn.

DTE

Data Terminal Equipment. DTE refers to a device that converts user information into signals or re-converts the received signals.

DTIM

Delivery Traffic Indication Message. DTIM is a kind of traffic indication map. A DTIM interval determines when the APs must deliver broadcast and multicast frames to their associated clients in power save mode.

DTLS

Datagram Transport Layer Security. DTLS communications protocol provides communications security for datagram protocols.

dynamic authorization

Dynamic authorization refers to the ability to make changes to a visitor account's session while it is in progress. This might include disconnecting a session or updating some aspect of the authorization for the session.

dynamic NAT

Dynamic Network Address Translation. Dynamic NAT maps multiple public IP addresses and uses these addresses with an internal or private IP address. Dynamic NAT helps to secure a network by masking the internal configuration of a private network.

EAP

Extensible Authentication Protocol. An authentication protocol for wireless networks that extends the methods used by the PPP, a protocol often used when connecting a computer to the Internet. EAP can support multiple authentication mechanisms, such as token cards, smart cards, certificates, one-time passwords, and public key encryption authentication.

EAP-FAST

EAP – Flexible Authentication Secure Tunnel (tunneled).

EAP-GTC

EAP – Generic Token Card. (non-tunneled).

EAP-MD5

EAP – Method Digest 5. (non-tunneled).

EAP-MSCHAP

EAP Microsoft Challenge Handshake Authentication Protocol.

EAP-MSCHAPv2

EAP Microsoft Challenge Handshake Authentication Protocol Version 2.

EAP-PEAP

EAP–Protected EAP. A widely used protocol for securely transporting authentication data across a network (tunneled).

EAP-PWD

EAP-Password. EAP-PWD is an EAP method that uses a shared password for authentication.

EAP-TLS

EAP–Transport Layer Security. EAP-TLS is a certificate-based authentication method supporting mutual authentication, integrity-protected ciphersuite negotiation and key exchange between two endpoints. See RFC 5216.

EAP-TTLS

EAP–Tunneled Transport Layer Security. EAP-TTLS is an EAP method that encapsulates a TLS session, consisting of a handshake phase and a data phase. See RFC 5281.

EAPoL

Extensible Authentication Protocol over LAN. A network port authentication protocol used in IEEE 802.1X standards to provide a generic network sign-on to access network resources.

ECC

Elliptical Curve Cryptography or Error correcting Code memory. Elliptical Curve Cryptography is a public-key encryption technique that is based on elliptic curve theory used for creating faster, smaller, and more efficient cryptographic keys. Error Correcting Code memory is a type of computer data storage that can detect and correct the most common kinds of internal data corruption. ECC memory is used in most computers where data corruption cannot be tolerated under any circumstances, such as for scientific or financial computing.

ECDSA

Elliptic Curve Digital Signature Algorithm. ECDSA is a cryptographic algorithm that supports the use of public or private key pairs for encrypting and decrypting information.

EDCA

Enhanced Distributed Channel Access. The EDCA function in the IEEE 802.11e Quality of Service standard supports differentiated and distributed access to wireless medium based on traffic priority and Access Category types. See WMM and WME.

EIGRP

Enhanced Interior Gateway Routing Protocol. EIGRP is a routing protocol used for automating routing decisions and configuration in a network.

EIRP

Effective Isotropic Radiated Power or Equivalent Isotropic Radiated Power. EIRP refers to the output power generated when a signal is concentrated into a smaller area by the Antenna.

ESI

External Services Interface. ESI provides an open interface for integrating security solutions that solve interior network problems such as viruses, worms, spyware, and corporate compliance.

ESS

Extended Service Set. An ESS is a set of one or more interconnected BSSs that form a single sub network.

ESSID

Extended Service Set Identifier. ESSID refers to the ID used for identifying an extended service set.

Ethernet

Ethernet is a network protocol for data transmission over LAN.

EULA

End User License Agreement. EULA is a legal contract between a software application publisher or author and the users of the application.

FCC

Federal Communications Commission. FCC is a regulatory body that defines standards for the interstate and international communications by radio, television, wire, satellite, and cable.

FFT

Fast Fourier Transform. FFT is a frequency analysis mechanism that aims at faster conversion of a discrete signal in time domain into a discrete frequency domain representation. See also DFT.

FHSS

Frequency Hopping Spread Spectrum. FHSS is transmission technique that allows modulation and transmission of a data signal by rapidly switching a carrier among many frequency channels in a random but predictable sequence. See also DSSS.

FIB

Forwarding Information Base. FIB is a forwarding table that maps MAC addresses to ports. FIB is used in network bridging, routing, and similar functions to identify the appropriate interface for forwarding packets.

FIPS

Federal Information Processing Standards. FIPS refers to a set of standards that describe document processing, encryption algorithms, and other information technology standards for use within non-military government agencies, and by government contractors and vendors who work with these agencies.

firewall

Firewall is a network security system used for preventing unauthorized access to or from a private network.

FQDN

Fully Qualified Domain Name. FQDN is a complete domain name that identifies a computer or host on the Internet.

FQLN

Fully Qualified Location Name. FQLN is a device location identifier in the format: APname.Floor.Building.Campus.

frequency allocation

Use of radio frequency spectrum as regulated by governments.

FSPL

Free Space Path Loss. FSPL refers to the loss in signal strength of an electromagnetic wave that would result from a line-of-sight path through free space (usually air), with no obstacles nearby to cause reflection or diffraction.

FTP

File Transfer Protocol. A standard network protocol used for transferring files between a client and server on a computer network.

GARP

Generic Attribute Registration Protocol. GVRP is a LAN protocol that allows the network nodes to register and de-register attributes, such as network addresses, with each other.

GAS

Generic Advertisement Service. GAS is a request-response protocol, which provides Layer 2 transport mechanism between a wireless client and a server in the network prior to authentication. It helps in determining a wireless network infrastructure before associating clients, and allows clients to send queries to multiple 802.11 networks in parallel.

gateway

Gateway is a network node that allows traffic to flow in and out of the network.

Gbps

Gigabits per second.

GBps

Gigabytes per second.

GET

GET refers HTTP request method or an SNMP operation method. The GET HTTP request method submits data to be processed to a specified resource. The GET SNMP operation method obtains information from the Management Information Base (MIB).

GHz

Gigahertz.

GMT

Greenwich Mean Time. GMT refers to the mean solar time at the Royal Observatory in Greenwich, London. GMT is the same as Coordinated Universal Time (UTC) standard, written as an offset of UTC +/- 00:00.

goodput

Goodput is the application level throughput that refers to the ratio of the total bytes transmitted or received in the network to the total air time required for transmitting or receiving the bytes.

GPS

Global Positioning System. A satellite-based global navigation system.

GRE

Generic Routing Encapsulation. GRE is an IP encapsulation protocol that is used to transport packets over a network.

GTC

Generic Token Card. GTC is a protocol that can be used as an alternative to MSCHAPv2 protocol. GTC allows authentication to various authentication databases even in cases where MSCHAPv2 is not supported by the database.

GVRP

GARP VLAN Registration Protocol or Generic VLAN Registration Protocol. GARP is an IEEE 802.1Q-compliant protocol that facilitates VLAN registration and controls VLANs within a larger network.

H2QP

Hotspot 2.0 Query Protocol.

hot zone

Wireless access area created by multiple hotspots that are located in close proximity to one another. Hot zones usually combine public safety APs with public hotspots.

hotspot

Hotspot refers to a WLAN node that provides Internet connection and virtual private network (VPN) access from a given location. A business traveler, for example, with a laptop equipped for Wi-Fi can look up a local hotspot, contact it, and get connected through its network to reach the Internet.

HSPA

High-Speed Packet Access.

HT

High Throughput. IEEE 802.11n is an HT WLAN standard that aims to achieve physical data rates of close to 600 Mbps on the 2.4 GHz and 5 GHz bands.

HTTP

Hypertext Transfer Protocol. The HTTP is an application protocol to transfer data over the web. The HTTP protocol defines how messages are formatted and transmitted, and the actions that the w servers and browsers should take in response to various commands.

HTTPS

Hypertext Transfer Protocol Secure. HTTPS is a variant of the HTTP that adds a layer of security on the data in transit through a secure socket layer or transport layer security protocol connection.

IAS

Internet Authentication Service. IAS is a component of Windows Server operating systems that provides centralized user authentication, authorization, and accounting.

ICMP

Internet Control Message Protocol. ICMP is an error reporting protocol. It is used by network devices such as routers, to send error messages and operational information to the source IP address when network problems prevent delivery of IP packets.

IDS

Intrusion Detection System. IDS monitors a network or systems for malicious activity or policy violations and reports its findings to the management system deployed in the network.

IEEE

Institute of Electrical and Electronics Engineers.

IGMP

Internet Group Management Protocol. Communications protocol used by hosts and adjacent routers on IP networks to establish multicast group memberships.

IGMP snooping

IGMP snooping prevents multicast flooding on Layer 2 network by treating multicast traffic as broadcast traffic. Without IGMP snooping, all streams could be flooded to all ports on that VLAN. When multicast flooding occurs, end-hosts that happen to be in the same VLAN would receive all the streams only to be discarded without snooping.

IGP

Interior Gateway Protocol. IGP is used for exchanging routing information between gateways within an autonomous system (for example, a system of corporate local area networks).

IGRP

Interior Gateway Routing Protocol. IGRP is a distance vector interior routing protocol used by routers to exchange routing data within an autonomous system.

IKE

Internet Key Exchange. IKE is a key management protocol used with IPsec protocol to establish a secure communication channel. IKE provides additional feature, flexibility, and ease of configuration for IPsec standard.

IKEv1

Internet Key Exchange version 1. IKEv1 establishes a secure authenticated communication channel by using either the pre-shared key (shared secret), digital signatures, or public key encryption. IKEv1 operates in Main and Aggressive modes. See RFC 2409.

IKEv2

Internet Key Exchange version 2. IKEv2 uses the secure channel established in Phase 1 to negotiate Security Associations on behalf of services such as IPsec. IKEv2 uses pre-shared key and Digital Signature for authentication. See RFC 4306.

IoT

Internet of Things. IoT refers to the internetworking of devices that are embedded with electronics, software, sensors, and network connectivity features allowing data exchange over the Internet.

IPM

Intelligent Power Monitoring. IPM is a feature supported on certain APs that actively measures the power utilization of an AP and dynamically adapts to the power resources.

IPS

Intrusion Prevention System. The IPS monitors a network for malicious activities such as security threats or policy violations. The main function of an IPS is to identify suspicious activity, log the information, attempt to block the activity, and report it.

IPsec

Internet Protocol security. IPsec is a protocol suite for secure IP communications that authenticates and encrypts each IP packet in a communication session.

IPSG

Internet Protocol Source Guard. IPSG restricts IP address from untrusted interface by filtering traffic based on list of addresses in the DHCP binding database or manually configured IP source bindings. It prevents IP spoofing attacks.

IrDA

An industry-sponsored organization set up in 1993 to create international standards for the hardware and software used in infrared communication links. In this special form of radio transmission, a focused ray of light in the infrared frequency spectrum, measured in terahertz (THz), or trillions of hertz (cycles per second), is modulated with information and sent from a transmitter to a receiver over a relatively short distance.

ISAKMP

Internet Security Association and Key Management Protocol. ISAKMP is used for establishing Security Associations and cryptographic keys in an Internet environment.

ISP

Internet Service Provider. An ISP is an organization that provides services for accessing and using the Internet.

JSON

JavaScript Object Notation. JSON is an open-standard, language-independent, lightweight data-interchange format used to transmit data objects consisting of attribute–value pairs. JSON uses a "self-describing" text format that is easy for humans to read and write, and that can be used as a data format by any programming language.

Kbps

Kilobits per second.

KBps

Kilobytes per second.

keepalive

Signal sent at periodic intervals from one device to another to verify that the link between the two devices is working. If no reply is received, data will be sent by a different path until the link is restored. A keepalive can also be used to indicate that the connection should be preserved so that the receiving device does not consider it timed out and drop it.

L2TP

Layer-2 Tunneling Protocol. L2TP is a networking protocol used by the ISPs to enable VPN operations.

LACP

Link Aggregation Control Protocol. LACP is used for the collective handling of multiple physical ports that can be seen as a single channel for network traffic purposes.

LAG

Link Aggregation Group . A LAG combines a number of physical ports together to make a single high-bandwidth data path. LAGs can connect two switches to provide a higher-bandwidth connection to a public network.

LAN

Local Area Network. A LAN is a network of connected devices within a distinct geographic area such as an office or a commercial establishment and share a common communications line or wireless link to a server.

LCD

Liquid Crystal Display. LCD is the technology used for displays in notebook and other smaller computers. Like LED and gas-plasma technologies, LCDs allow displays to be much thinner than the cathode ray tube technology.

LDAP

Lightweight Directory Access Protocol. LDAP is a communication protocol that provides the ability to access and maintain distributed directory information services over a network.

LDPC

Low-Density Parity-Check. LDPC is a method of transmitting a message over a noisy transmission channel using a linear error correcting code. An LDPC is constructed using a sparse bipartite graph.

LEAP

Lightweight Extensible Authentication Protocol. LEAP is a Cisco proprietary version of EAP used in wireless networks and Point-to-Point connections.

LED

Light Emitting Diode. LED is a semiconductor light source that emits light when an electric current passes through it.

LEEF

Log Event Extended Format. LEEF is a type of customizable syslog event format. An extended log file contains a sequence of lines containing ASCII characters terminated by either the sequence LF or CRLF.

LI

Lawful Interception. LI refers to the procedure of obtaining communications network data by the Law Enforcement Agencies for the purpose of analysis or evidence.

LLDP

Link Layer Discovery Protocol. LLDP is a vendor-neutral link layer protocol in the Internet Protocol suite used by network devices for advertising their identity, capabilities, and neighbors on an IEEE 802 local area network, which is principally a wired Ethernet.

LLDP-MED

LLDP–Media Endpoint Discovery. LLDP-MED facilitates information sharing between endpoints and network infrastructure devices.

LMS

Local Management Switch. In multi-controller networks, each controller acts as an LMS and terminates user traffic from the APs, processes, and forwards the traffic to the wired network.

LNS

L2TP Network Server. LNS is an equipment that connects to a carrier and handles the sessions from broadband lines. It is also used for dial-up and mobile links. LNS handles authentication and routing of the IP addresses. It also handles the negotiation of the link with the equipment and establishes a session.

LTE

Long Term Evolution. LTE is a 4G wireless communication standard that provides high-speed wireless communication for mobile phones and data terminals. See 4G.

MAB

MAC Authentication Bypass. Endpoints such as network printers, Ethernet-based sensors, cameras, and wireless phones do not support 802.1X authentication. For such endpoints, MAC Authentication Bypass mechanism is used. In this method, the MAC address of the endpoint is used to authenticate the endpoint.

MAC

Media Access Control. A MAC address is a unique identifier assigned to network interfaces for communications on a network.

MAM

Mobile Application Management. MAM refers to software and services used to secure, manage, and distribute mobile applications used in enterprise settings on mobile devices like smartphones and tablet computers. Mobile Application Management can apply to company-owned mobile devices as well as BYOD.

Mbps

Megabits per second

MBps

Megabytes per second

MCS

Modulation and Coding Scheme. MCS is used as a parameter to determine the data rate of a wireless connection for high throughput.

MD4

Message Digest 4. MD4 is an earlier version of MD5 and is an algorithm used to verify data integrity through the creation of a 128-bit message digest from data input.

MD5

Message Digest 5. The MD5 algorithm is a widely used hash function producing a 128-bit hash value from the data input.

MDAC

Microsoft Data Access Components. MDAC is a framework of interrelated Microsoft technologies that provides a standard database for Windows OS.

MDM

Mobile Device Management. MDM is an administrative software to manage, monitor, and secure mobile devices of the employees in a network.

mDNS

Multicast Domain Name System. mDNS provides the ability to perform DNS-like operations on the local link in the absence of any conventional unicast DNS server. The mDNS protocol uses IP multicast User Datagram Protocol (UDP) packets, and is implemented by the Apple Bonjour and Linux NSS-mDNS services. mDNS works in conjunction with DNS Service Discovery (DNS-SD), a companion zero-configuration technique specified. See RFC 6763.

MFA

Multi-factor Authentication. MFA lets you require multiple factors, or proofs of identity, when authenticating a user. Policy configurations define how often multi-factor authentication will be required, or conditions that will trigger it.

MHz

Megahertz

MIB

Management Information Base. A hierarchical database used by SNMP to manage the devices being monitored.

microwave

Electromagnetic energy with a frequency higher than 1 GHz, corresponding to wavelength shorter than 30 centimeters.

MIMO

Multiple Input Multiple Output. An antenna technology for wireless communications in which multiple antennas are used at both source (transmitter) and destination (receiver). The antennas at each end of the communications circuit are combined to minimize errors and optimize data speed.

MISO

Multiple Input Single Output. An antenna technology for wireless communications in which multiple antennas are used at the source (transmitter). The antennas are combined to minimize errors and optimize data speed. The destination (receiver) has only one antenna.

MLD

Multicast Listener Discovery. A component of the IPv6 suite. It is used by IPv6 routers for discovering multicast listeners on a directly attached link.

MPDU

MAC Protocol Data Unit. MPDU is a message exchanged between MAC entities in a communication system based on the layered OSI model.

MPLS

Multiprotocol Label Switching. The MPLS protocol speeds up and shapes network traffic flows.

MPPE

Microsoft Point-to-Point Encryption. A method of encrypting data transferred across PPP-based dial-up connections or PPTP-based VPN connections.

MS-CHAP

Microsoft Challenge Handshake Authentication Protocol. MS-CHAP is Password-based, challenge-response, mutual authentication protocol that uses MD4 and DES encryption.

MS-CHAPv1

Microsoft Challenge Handshake Authentication Protocol version 1. MS-CHAPv1 extends the user authentication functionality provided on Windows networks to remote workstations. MS-CHAPv1 supports only one-way authentication.

MS-CHAPv2

Microsoft Challenge Handshake Authentication Protocol version 2. MS-CHAPv2 is an enhanced version of the MS-CHAP protocol that supports mutual authentication.

MSS

Maximum Segment Size. MSS is a parameter of the options field in the TCP header that specifies the largest amount of data, specified in bytes, that a computer or communications device can receive in a single TCP segment.

MSSID

Mesh Service Set Identifier. MSSID is the SSID used by the client to access a wireless mesh network.

MSTP

Multiple Spanning Tree Protocol. MSTP configures a separate Spanning Tree for each VLAN group and blocks all but one of the possible alternate paths within each spanning tree.

MTU

Maximum Transmission Unit. MTU is the largest size packet or frame specified in octets (eight-bit bytes) that can be sent in networks such as the Internet.

MU-MIMO

Multi-User Multiple-Input Multiple-Output. MU-MIMO is a set of multiple-input and multiple-output technologies for wireless communication, in which users or wireless terminals with one or more antennas communicate with each other.

MVRP

Multiple VLAN Registration Protocol. MVRP is a Layer 2 network protocol used for automatic configuration of VLAN information on switches.

mW

milliWatts. mW is 1/1000 of a Watt. It is a linear measurement (always positive) that is generally used to represent transmission.

NAC

Network Access Control. NAC is a computer networking solution that uses a set of protocols to define and implement a policy that describes how devices can secure access to network nodes when they initially attempt to connect to a network.

NAD

Network Access Device. NAD is a device that automatically connects the user to the preferred network, for example, an AP or an Ethernet switch.

NAK

Negative Acknowledgement. NAK is a response indicating that a transmitted message was received with errors or it was corrupted, or that the receiving end is not ready to accept transmissions.

NAP

Network Access Protection. The NAP feature in the Windows Server allows network administrators to define specific levels of network access based on identity, groups, and policy compliance. The NAP Agent is a service that collects and manages health information for NAP client computers. If a client is not compliant, NAP provides a mechanism to automatically bring the client back into compliance and then dynamically increase its level of network access.

NAS

Network Access Server. NAS provides network access to users, such as a wireless AP, network switch, or dial-in terminal server.

NAT

Network Address Translation. NAT is a method of remapping one IP address space into another by modifying network address information in Internet Protocol (IP) datagram packet headers while they are in transit across a traffic routing device.

NetBIOS

Network Basic Input/Output System. A program that lets applications on different computers communicate within a LAN.

netmask

Netmask is a 32-bit mask used for segregating IP address into subnets. Netmask defines the class and range of IP addresses.

NFC

Near-Field Communication. NFC is a short-range wireless connectivity standard (ECMA-340, ISO/IEC 18092) that uses magnetic field induction to enable communication between devices when they touch or are brought closer (within a few centimeters of distance). The standard specifies a way for the devices to establish a peer-to-peer (P2P) network to exchange data.

NIC

Network Interface Card. NIC is a hardware component that allows a device to connect to the network.

Nmap

Network Mapper. Nmap is an open-source utility for network discovery and security auditing. Nmap uses IP packets to determine such things as the hosts available on a network and their services, operating systems and versions, types of packet filters/firewalls, and so on.

NMI

Non-Maskable Interrupt. NMI is a hardware interrupt that standard interrupt-masking techniques in the system cannot ignore. It typically occurs to signal attention for non-recoverable hardware errors.

NMS

Network Management System. NMS is a set of hardware and/or software tools that allow an IT professional to supervise the individual components of a network within a larger network management framework.

NOE

New Office Environment. NOE is a proprietary VoIP protocol designed by Alcatel-Lucent Enterprise.

NTP

Network Time Protocol. NTP is a protocol for synchronizing the clocks of computers over a network.

OAuth

Open Standard for Authorization. OAuth is a token-based authorization standard that allows websites or third-party applications to access user information, without exposing the user credentials.

OCSP

Online Certificate Status Protocol. OCSP is used for determining the current status of a digital certificate without requiring a CRL.

OFDM

Orthogonal Frequency Division Multiplexing. OFDM is a scheme for encoding digital data on multiple carrier frequencies.

OID

Object Identifier. An OID is an identifier used to name an object. The OIDs represent nodes or managed objects in a MIB hierarchy. The OIDs are designated by text strings and integer sequences and are formally defined as per the ASN.1 standard.

OKC

Opportunistic Key Caching. OKC is a technique available for authentication between multiple APs in a network where those APs are under common administrative control. Using OKC, a station roaming to any AP in the network will not have to complete a full authentication exchange, but will instead just perform the 4-way handshake to establish transient encryption keys.

onboarding

The process of preparing a device for use on an enterprise network, by creating the appropriate access credentials and setting up the network connection parameters.

OpenFlow

OpenFlow is an open communications interface between control plane and the forwarding layers of a network.

OpenFlow agent

OpenFlow agent. OpenFlow is a software module in Software-Defined Networking (SDN) that allows the abstraction of any legacy network element, so that it can be integrated and managed by the SDN controller. OpenFlow runs on network devices such as switches, routers, wireless controllers, and APs.

Optical wireless

Optical wireless is combined use of conventional radio frequency wireless and optical fiber for telecommunication. Long-range links are provided by using optical fibers; the links from the long-range endpoints to end users are accomplished by RF wireless or laser systems. RF wireless at Ultra High Frequencies and microwave frequencies can carry broadband signals to individual computers at substantial data speeds.

OSI

Open Systems Interconnection. OSI is a reference model that defines a framework for communication between the applications in a network.

OSPF

Open Shortest Path First. OSPF is a link-state routing protocol for IP networks. It uses a link-state routing algorithm and falls into the group of interior routing protocols that operates within a single Autonomous System (AS).

OSPFv2

Open Shortest Path First version 2. OSPFv2 is the version 2 of the link-state routing protocol, OSPF. See RFC 2328.

OUI

Organizationally Unique Identifier. Synonymous with company ID or vendor ID, an OUI is a 24-bit, globally unique assigned number, referenced by various standards. The first half of a MAC address is OUI.

OVA

Open Virtualization Archive. OVA contains a compressed installable version of a virtual machine.

OVF

Open Virtualization Format. OVF is a specification that describes an open-standard, secure, efficient, portable and extensible format for packaging and distributing software for virtual machines.

PAC

Protected Access Credential. PAC is distributed to clients for optimized network authentication. These credentials are used for establishing an authentication tunnel between the client and the authentication server.

PAP

Password Authentication Protocol. PAP validates users by password. PAP does not encrypt passwords for transmission and is thus considered insecure.

PAPI

Process Application Programming Interface. PAPI controls channels for ARM and Wireless Intrusion Detection System (WIDS) communication to the master controller. A separate PAPI control channel connects to the local controller where the SSID tunnels terminate.

PBR

Policy-based Routing. PBR provides a flexible mechanism for forwarding data packets based on polices configured by a network administrator.

PDU

Power Distribution Unit or Protocol Data Unit. Power Distribution Unit is a device that distributes electric power to the networking equipment located within a data center. Protocol Data Unit contains protocol control Information that is delivered as a unit among peer entities of a network.

PEAP

Protected Extensible Authentication Protocol. PEAP is a type of EAP communication that addresses security issues associated with clear text EAP transmissions by creating a secure channel encrypted and protected by TLS.

PEF

Policy Enforcement Firewall. PEF also known as PEFNG provides context-based controls to enforce application-layer security and prioritization. The customers using Aruba mobility controllers can avail PEF features and services by obtaining a PEF license. PEF for VPN users—Customers with PEF for VPN license can apply firewall policies to the user traffic routed to a controller through a VPN tunnel.

PEFNG

Policy Enforcement Firewall. PEF also known as PEFNG provides context-based controls to enforce application-layer security and prioritization. The customers using Aruba mobility controllers can avail PEF features and services by obtaining a PEF license. PEF for VPN users—Customers with PEF for VPN license can apply firewall policies to the user traffic routed to a controller through a VPN tunnel.

PEFV

Policy Enforcement Firewall. PEF also known as PEFNG provides context-based controls to enforce application-layer security and prioritization. The customers using Aruba mobility controllers can avail PEF features and services by obtaining a PEF license. PEF for VPN users—Customers with PEF for VPN license can apply firewall policies to the user traffic routed to a controller through a VPN tunnel.

PFS

Perfect Forward Secrecy. PFS refers to the condition in which a current session key or long-term private key does not compromise the past or subsequent keys.

PHB

Per-hop behavior. PHB is a term used in DS or MPLS. It defines the policy and priority applied to a packet when traversing a hop (such as a router) in a DiffServ network.

PIM

Protocol-Independent Multicast. PIM refers to a family of multicast routing protocols for IP networks that provide one-to-many and many-to-many distribution of data over a LAN, WAN, or the Internet.

PIN

Personal Identification Number. PIN is a numeric password used to authenticate a user to a system.

PKCS#n

Public-key cryptography standard n. PKCS#n refers to a numbered standard related to topics in cryptography, including private keys (PKCS#1), digital certificates (PKCS#7), certificate signing requests (PKCS#10), and secure storage of keys and certificates (PKCS#12).

PKI

Public Key Infrastructure. PKI is a security technology based on digital certificates and the assurances provided by strong cryptography. See also certificate authority, digital certificate, public key, private key.

PLMN

Public Land Mobile Network. PLMS is a network established and operated by an administration or by a Recognized Operating Agency for the specific purpose of providing land mobile telecommunications services to the public.

PMK

Pairwise Master Key. PMK is a shared secret key that is generated after PSK or 802.1X authentication.

PoE

Power over Ethernet. PoE is a technology for wired Ethernet LANs to carry electric power required for the device in the data cables. The IEEE 802.3af PoE standard provides up to 15.4 W of power on each port.

PoE+

Power over Ethernet+. PoE+ is an IEEE 802.3at standard that provides 25.5W power on each port.

POST

An HTTP request method that requests data from a specified resource.

PPP

Point-to-Point Protocol. PPP is a data link (layer 2) protocol used to establish a direct connection between two nodes. It can provide connection authentication, transmission encryption, and compression.

PPPoE

Point-to-Point Protocol over Ethernet. PPPoE is a method of connecting to the Internet, typically used with DSL services, where the client connects to the DSL modem.

PPTP

Point-to-Point Tunneling Protocol. PPTP is a method for implementing virtual private networks. It uses a control channel over TCP and a GRE tunnel operating to encapsulate PPP packets.

private key

The part of a public-private key pair that is always kept private. The private key encrypts the signature of a message to authenticate the sender. The private key also decrypts a message that was encrypted with the public key of the sender.

PRNG

Pseudo-Random Number Generator. PRNG is an algorithm for generating a sequence of numbers whose properties approximate the properties of sequences of random numbers.

PSK

Pre-shared key. A unique shared secret that was previously shared between two parties by using a secure channel. This is used with WPA security, which requires the owner of a network to provide a passphrase to users for network access.

PSU

Power Supply Unit. PSU is a unit that supplies power to an equipment by converting mains AC to low-voltage regulated DC power.

public key

The part of a public-private key pair that is made public. The public key encrypts a message and the message is decrypted with the private key of the recipient.

PVST

Per-VLAN Spanning Tree. PVST provides load balancing of VLANs across multiple ports resulting in optimal usage of network resources.

PVST+

Per-VLAN Spanning Tree+. PVST+ is an extension of the PVST standard that uses the 802.1Q trunking technology.

QoS

Quality of Service. It refers to the capability of a network to provide better service and performance to a specific network traffic over various technologies.

RA

Router Advertisement. The RA messages are sent by the routers in the network when the hosts send multicast router solicitation to the multicast address of all routers.

Radar

Radio Detection and Ranging. Radar is an object-detection system that uses radio waves to determine the range, angle, or velocity of objects.

RADIUS

Remote Authentication Dial-In User Service. An Industry-standard network access protocol for remote authentication. It allows authentication, authorization, and accounting of remote users who want to access network resources.

RAM

Random Access Memory.

RAPIDS

Rogue Access Point identification and Detection System. An AMP module that is designed to identify and locate wireless threats by making use of all of the information available from your existing infrastructure.

RARP

Reverse Address Resolution Protocol. RARP is a protocol used by a physical machine in a local area network for determining the IP address from the ARP table or cache of the gateway server.

Regex

Regular Expression. Regex refers to a sequence of symbols and characters defining a search pattern.

Registration Authority

Type of Certificate Authority that processes certificate requests. The Registration Authority verifies that requests are valid and comply with certificate policy, and authenticates the user's identity. The Registration Authority then forwards the request to the Certificate Authority to sign and issue the certificate.

Remote AP

Remote APs extend corporate network to the users working from home or at temporary work sites. Remote APs are deplyed at branch office sites and are connected to the central network on a WAN link.

REST

Representational State Transfer. REST is a simple and stateless architecture that the web services use for providing interoperability between computer systems on the Internet. In a RESTful web service, requests made to the URI of a resource will elicit a response that may be in XML, HTML, JSON or some other defined format.

RF

Radio Frequency. RF refers to the electromagnetic wave frequencies within a range of 3 kHz to 300 GHz, including the frequencies used for communications or Radar signals.

RFC

Request For Comments. RFC is a commonly used format for the Internet standards documentss.

RFID

Radio Frequency Identification. RFID uses radio waves to automatically identify and track the information stored on a tag attached to an object.

RIP

Routing Information Protocol. RIP prevents the routing loops by limiting the number of hops allowed in a path from source to destination.

RJ45

Registered Jack 45. RJ45 is a physical connector for network cables.

RMA

Return Merchandise Authorization. RMA is a part of the product returning process that authorizes users to return a product to the manufacturer or distributor for a refund, replacement, or repair. The customers who want to return a product within its Warranty period contact the manufacturer to initiate the product returning process. The manufacturer or the seller generates an authorization number for the RMA, which is used by the customers, when returning a product to the warehouse.

RMON

Remote Monitoring. RMON provides standard information that a network administrator can use to monitor, analyze, and troubleshoot a group of distributed LANs.

RoW

Rest of World. RoW or RW is an operating country code of a device.

RSA

Rivest, Shamir, Adleman. RSA is a cryptosystem for public-key encryption, and is widely used for securing sensitive data, particularly when being sent over an insecure network such as the Internet.

RSSI

Received Signal Strength Indicator. RSSI is a mechanism by which RF energy is measured by the circuitry on a wireless NIC (0-255). The RSSI is not standard across vendors. Each vendor determines its own RSSI scale/values.

RSTP

Rapid Spanning Tree Protocol. RSTP provides significantly faster spanning tree convergence after a topology change, introducing new convergence behaviors and bridge port roles to do this.

RTCP

RTP Control Protocol. RTCP provides out-of-band statistics and control information for an Real-Time Transport Protocol session.

RTLS

Real-Time Location Systems. RTLS automatically identifies and tracks the location of objects or people in real time, usually within a building or other contained area.

RTP

Real-Time Transport Protocol. RTP is a network protocol used for delivering audio and video over IP networks.

RTS

Request to Send. RTS refers to the data transmission and protection mechanism used by the 802.11 wireless networking protocol to prevent frame collision occurrences. See CTS.

RTSP

Real Time Streaming Protocol. RTSP is a network control protocol designed for use in entertainment and communications systems to control streaming media servers.

RVI

Routed VLAN Interface. RVI is a switch interface that forwards packets between VLANs.

RW
: Rest of World. RoW or RW is an operating country code of a device.

SA
: Security Association. SA is the establishment of shared security attributes between two network entities to support secure communication.

SAML
: Security Assertion Markup Language. SAML is an XML-based framework for communicating user authentication, entitlement, and attribute information. SAML enables single sign-on by allowing users to authenticate at an identity provider and then access service providers without additional authentication.

SCEP
: Simple Certificate Enrollment Protocol. SCEP is a protocol for requesting and managing digital certificates.

SCP
: Secure Copy Protocol. SCP is a network protocol that supports file transfers between hosts on a network.

SCSI
: Small Computer System Interface. SCSI refers to a set of interface standards for physical connection and data transfer between a computer and the peripheral devices such as printers, disk drives, CD-ROM, and so on.

SD-WAN
: Software-Defined Wide Area Network. SD-WAN is an application for applying SDN technology to WAN connections that connect enterprise networks across disparate geographical locations.

SDN
: Software-Defined Networking. SDN is an umbrella term encompassing several kinds of network technology aimed at making the network as agile and flexible as the virtualized server and storage infrastructure of the modern data center.

SDR
: Server Derivation Rule. An SDR refers to a role assignment model used by the controllers running ArubaOS to assign roles and VLANs to the WLAN users based on the rules defined under a server group. The SDRs override the default authentication roles and VLANs defined in the AAA and Virtual AP profiles.

SDU
: Service Data Unit. SDU is a unit of data that has been passed down from an OSI layer to a lower layer and that has not yet been encapsulated into a PDU by the lower layer.

SFP

The Small Form-factor Pluggable. SFP is a compact, hot-pluggable transceiver that is used for both telecommunication and data communications applications.

SFP+

Small Form-factor Pluggable+. SFP+ supports up to data rates up to 16 Gbps.

SFTP

Secure File Transfer Protocol. SFTP is a network protocol that allows file access, file transfer, and file management functions over a secure connection.

SHA

Secure Hash Algorithm. SHA is a family of cryptographic hash functions. The SHA algorithm includes the SHA, SHA-1, SHA-2 and SHA-3 variants.

SIM

Subscriber Identity Module. SIM is an integrated circuit that is intended to securely store the International Mobile Subscriber Identity (IMSI) number and its related key, which are used for identifying and authenticating subscribers on mobile telephony devices.

SIP

Session Initiation Protocol. SIP is used for signaling and controlling multimedia communication session such as voice and video calls.

SIRT

Security Incident Response Team. SIRT is responsible for reviewing as well as responding to computer security incident reports and activity.

SKU

Stock Keeping Unit. SKU refers to the product and service identification code for the products in the inventory.

SLAAC

Stateless Address Autoconfiguration. SLAAC provides the ability to address a host based on a network prefix that is advertised from a local network router through router advertisements.

SMB

Server Message Block or Small and Medium Business. Server Message Block operates as an application-layer network protocol mainly used for providing shared access to files, printers, serial ports, and for miscellaneous communications between the nodes on a network.

SMS

Short Message Service. SMS refers to short text messages (up to 140 characters) sent and received through mobile phones.

SMTP

Simple Mail Transfer Protocol. SMTP is an Internet standard protocol for electronic mail transmission.

SNIR

Signal-to-Noise-Plus-Interference Ratio. SNIR refers to the power of a central signal of interest divided by the sum of the interference power and the power of the background noise. SINR is defined as the power of a certain signal of interest divided by the sum of the interference power (from all the other interfering signals) and the power of some background noise.

SNMP

Simple Network Management Protocol. SNMP is a TCP/IP standard protocol for managing devices on IP networks. Devices that typically support SNMP include routers, switches, servers, workstations, printers, modem racks, and more. It is used mostly in network management systems to monitor network-attached devices for conditions that warrant administrative attention.

SNMPv1

Simple Network Management Protocol version 1. SNMPv1 is a widely used network management protocol.

SNMPv2

Simple Network Management Protocol version 2. SNMPv2 is an enhanced version of SNMPv1, which includes improvements in the areas of performance, security, confidentiality, and manager-to-manager communications.

SNMPv2c

Community-Based Simple Network Management Protocol version 2. SNMPv2C uses the community-based security scheme of SNMPv1 and does not include the SNMPv2 security model.

SNMPv3

Simple Network Management Protocol version 3. SNMPv3 is an enhanced version of SNMP that includes security and remote configuration features.

SNR

Signal-to-Noise Ratio. SNR is used for comparing the level of a desired signal with the level of background noise.

SNTP

Simple Network Time Protocol. SNTP is a less complex implementation of NTP. It uses the same , but does not require the storage of state over extended periods of time.

SOAP

Simple Object Access Protocol. SOAP enables communication between the applications running on different operating systems, with different technologies and programming languages. SOAP is an XML-based messaging protocol for exchanging structured information between the systems that support web services.

SoC

System on a Chip. SoC is an Integrated Circuit that integrates all components of a computer or other electronic system into a single chip.

source NAT

Source NAT changes the source address of the packets passing through the router. Source NAT is typically used when an internal (private) host initiates a session to an external (public) host.

SSH

Secure Shell. SSH is a network protocol that provides secure access to a remote device.

SSID

Service Set Identifier. SSID is a name given to a WLAN and is used by the client to access a WLAN network.

SSL

Secure Sockets Layer. SSL is a computer networking protocol for securing connections between network application clients and servers over the Internet.

SSO

Single Sign-On. SSO is an access-control property that allows the users to log in once to access multiple related, but independent applications or systems to which they have privileges. The process authenticates the user across all allowed resources during their session, eliminating additional login prompts.

STBC

Space-Time Block Coding. STBC is a technique used in wireless communications to transmit multiple copies of a data stream across a number of antennas and to exploit the various received versions of the data to improve the reliability of data transfer.

STM

Station Management. STM is a process that handles AP management and user association.

STP

Spanning Tree Protocol. STP is a network protocol that builds a logical loop-free topology for Ethernet networks.

SU-MIMO

Single-User Multiple-Input Multiple-Output. SU-MIMO allocates the full bandwidth of the AP to a single high-speed device during the allotted time slice.

subnet

Subnet is the logical division of an IP network.

subscription

A business model where a customer pays a certain amount as subscription price to obtain access to a product or service.

SVP

SpectraLink Voice Priority. SVP is an open, straightforward QoS approach that has been adopted by most leading vendors of WLAN APs. SVP favors isochronous voice packets over asynchronous data packets when contending for the wireless medium and when transmitting packets onto the wired LAN.

SWAN

Structured Wireless-Aware Network. A technology that incorporates a Wireless Local Area Network (WLAN) into a wired Wide Area Network (WAN). SWAN technology can enable an existing wired network to serve hundreds of users, organizations, corporations, or agencies over a large geographic area. SWAN is said to be scalable, secure, and reliable.

TAC

Technical Assistance Center.

TACACS

Terminal Access Controller Access Control System. TACACS is a family of protocols that handles remote authentication and related services for network access control through a centralized server.

TACACS+

Terminal Access Controller Access Control System+. TACACS+ provides separate authentication, authorization, and accounting services. It is derived from, but not backward compatible with, TACACS.

TCP

Transmission Control Protocol. TCP is a communication protocol that defines the standards for establishing and maintaining network connection for applications to exchange data.

TCP/IP

Transmission Control Protocol/ Internet Protocol. TCP/IP is the basic communication language or protocol of the Internet.

TFTP

Trivial File Transfer Protocol. The TFTP is a software utility for transferring files from or to a remote host.

TIM

Traffic Indication Map. TIM is an information element that advertises if any associated stations have buffered unicast frames. APs periodically send the TIM within a beacon to identify the stations that are using power saving mode and the stations that have undelivered data buffered on the AP.

TKIP

Temporal Key Integrity Protocol. A part of the WPA encryption standard for wireless networks. TKIP is the next-generation Wired Equivalent Privacy (WEP) that provides per-packet key mixing to address the flaws encountered in the WEP standard.

TLS

Transport Layer Security. TLS is a cryptographic protocol that provides communication security over the Internet. TLS encrypts the segments of network connections above the Transport Layer by using asymmetric cryptography for key exchange, symmetric encryption for privacy, and message authentication codes for message integrity.

TLV

Type-length-value or Tag-Length-Value. TLV is an encoding format. It refers to the type of data being processed, the length of the value, and the value for the type of data being processed.

ToS

Type of Service. The ToS field is part of the IPv4 header, which specifies datagrams priority and requests a route for low-delay, high-throughput, or a highly reliable service.

TPC

Transmit Power Control. TPC is a part of the 802.11h amendment. It is used to regulate the power levels used by 802.11a radio cards.

TPM

Trusted Platform Module. TPM is an international standard for a secure cryptoprocessor, which is a dedicated microcontroller designed to secure hardware by integrating cryptographic keys into devices.

TSF

Timing Synchronization Function. TSF is a WLAN function that is used for synchronizing the timers for all the stations in a BSS.

TSPEC

Traffic Specification. TSPEC allows an 802.11e client or a QoS-capable wireless client to signal its traffic requirements to the AP.

TSV

Tab-Separated Values. TSV is a file format that allows the exchange of tabular data between applications that use different internal data formats.

TTL

Time to Live. TTL or hop limit is a mechanism that sets limits for data expiry in a computer or network.

TTY

TeleTypeWriter. TTY-enabled devices allow telephones to transmit text communications for people who are deaf or hard of hearing as well as transmit voice communication.

TXOP

Transmission Opportunity. TXOP is used in wireless networks supporting the IEEE 802.11e Quality of Service (QoS) standard. Used in both EDCA and HCF Controlled Channel Access modes of operation, TXOP is a bounded time interval in which stations supporting QoS are permitted to transfer a series of frames. TXOP is defined by a start time and a maximum duration.

U-APSD

Unscheduled Automatic Power Save Delivery. U-APSD is a part of 802.11e and helps considerably in increasing the battery life of VoWLAN terminals.

UAM

Universal Access Method. UAM allows subscribers to access a wireless network after they successfully log in from a web browser.

UCC

Unified Communications and Collaboration. UCC is a term used to describe the integration of various communications methods with collaboration tools such as virtual whiteboards, real-time audio and video conferencing, and enhanced call control capabilities.

UDID

Unique Device Identifier. UDID is used to identify an iOS device.

UDP

User Datagram Protocol. UDP is a part of the TCP/IP family of protocols used for data transfer. UDP is typically used for streaming media. UDP is a stateless protocol, which means it does not acknowledge that the packets being sent have been received.

UDR

User Derivation Rule. UDR is a role assignment model used by the controllers running ArubaOS to assign roles and VLANs to the WLAN users based on MAC address, BSSID, DHCP-Option, encryption type, SSID, and the location of a user. For example, for an SSID with captive portal in the initial role, a UDR can be configured for scanners to provide a role based on their MAC OUI.

UHF

Ultra high frequency. UHF refers to radio frequencies between the range of 300 MHz and 3 GHz. UHF is also known as the decimeter band as the wavelengths range from one meter to one decimeter.

UI

User Interface.

UMTS

Universal Mobile Telecommunication System. UMTS is a third generation mobile cellular system for networks. See 3G.

UPnP

Universal Plug and Play. UPnp is a set of networking protocols that permits networked devices, such as personal computers, printers, Internet gateways, Wi-Fi APs, and mobile devices to seamlessly discover each other's presence on the network and establish functional network services for data sharing, communications, and entertainment.

URI

Uniform Resource Identifier. URI identifies the name and the location of a resource in a uniform format.

URL

Uniform Resource Locator. URL is a global address used for locating web resources on the Internet.

USB

Universal Serial Bus. USB is a connection standard that offers a common interface for communication between the external devices and a computer. USB is the most common port used in the client devices.

UTC

Coordinated Universal Time. UTC is the primary time standard by which the world regulates clocks and time.

UWB

Ultra-Wideband. UWB is a wireless technology for transmitting large amounts of digital data over a wide spectrum of frequency bands with very low power for a short distance.

VA

Virtual Appliance. VA is a pre-configured virtual machine image, ready to run on a hypervisor.

VBR

Virtual Beacon Report. VBR displays a report with the MAC address details and RSSI information of an AP.

VHT

Very High Throughput. IEEE 802.11ac is an emerging VHT WLAN standard that could achieve physical data rates of close to 7 Gbps for the 5 GHz band.

VIA

Virtual Intranet Access. VIA provides secure remote network connectivity for Android, Apple iOS, Mac OS X, and Windows mobile devices and laptops. It automatically scans and selects the best secure connection to the corporate network.

VLAN

Virtual Local Area Network. In computer networking, a single Layer 2 network may be partitioned to create multiple distinct broadcast domains, which are mutually isolated so that packets can only pass between them through one or more routers; such a domain is referred to as a Virtual Local Area Network, Virtual LAN, or VLAN.

VM

Virtual Machine. A VM is an emulation of a computer system. VMs are based on computer architectures and provide functionality of a physical computer.

VoIP

Voice over IP. VoIP allows transmission of voice and multimedia content over an IP network.

VoWLAN

Voice over WLAN. VoWLAN is a method of routing telephone calls for mobile users over the Internet using the technology specified in IEEE 802.11b. Routing mobile calls over the Internet makes them free, or at least much less expensive than they would be otherwise.

VPN

Virtual Private Network. VPN enables secure access to a corporate network when located remotely. It enables a computer to send and receive data across shared or public networks as if it were directly connected to the private network, while benefiting from the functionality, security, and management policies of the private network. This is done by establishing a virtual point-to-point connection through the use of dedicated connections, encryption, or a combination of the two.

VRD

Validated Reference Design. VRDs are guides that capture the best practices for a particular technology in field.

VRF

VisualRF. VRF is an AirWave Management Platform (AMP) module that provides a real-time, network-wide views of your entire Radio Frequency environment along with floor plan editing capabilities. VRF also includes overlays on client health to help diagnose issues related to clients, floor plan, or a specific location.

VRF Plan

VisualRF Plan. A stand-alone Windows client used for basic planning procedures such as adding a floor plan, provisioning APs, and generating a Bill of Materials report.

VRRP

Virtual Router Redundancy Protocol. VRRP is an election protocol that dynamically assigns responsibility for a virtual router to one of the VRRP routers on a LAN.

VSA

Vendor-Specific Attribute. VSA is a method for communicating vendor-specific information between NASs and RADIUS servers.

VTP

VLAN Trunking Protocol. VTP is a Cisco proprietary protocol for propagating VLANs on a LAN.

W-CDMA

Wideband Code-Division Multiple Access. W-CDMA is a third-generation (3G) mobile wireless technology that promises much higher data speeds to mobile and portable wireless devices.

walled garden

Walled garden is a feature that allows blocking of unauthorized users from accessing network resources.

WAN

Wide Area Network. WAN is a telecommunications network or computer network that extends over a large geographical distance.

WASP

Wireless Application Service Provider. WASP provides a web-based access to applications and services that would otherwise have to be stored locally and makes it possible for customers to access the service from a variety of wireless devices, such as a smartphone or Personal Digital Assistant (PDA).

WAX

Wireless abstract XML. WAX is an abstract markup language and a set of tools that is designed to help wireless application development as well as portability. Its tags perform at a higher level of abstraction than that of other wireless markup languages such as HTML, HDML, WML, XSL, and more.

web service

Web services allow businesses to share and process data programmatically. Developers who want to provide integrated applications can use the API to programmatically perform actions that would otherwise require manual operation of the user interface.

WEP

Wired Equivalent Privacy. WEP is a security protocol that is specified in 802.11b and is designed to provide a WLAN with a level of security and privacy comparable to what is usually expected of a wired LAN.

WFA

Wi-Fi Alliance. WFA is a non-profit organization that promotes Wi-Fi technology and certifies Wi-Fi products if they conform to certain standards of interoperability.

Wi-Fi

Wi-Fi is a technology that allows electronic devices to connect to a WLAN network, mainly using the 2.4 GHz and 5 GHz radio bands. Wi-Fi can apply to products that use any 802.11 standard.

WIDS

Wireless Intrusion Detection System. WIDS is an application that detects the attacks on a wireless network or wireless system.

WiMAX

Worldwide Interoperability for Microwave Access. WiMAX refers to the implementation of IEEE 802.16 family of wireless networks standards set by the WiMAX forum.

WIP

Wireless Intrusion Protection. The WIP module provides wired and wireless AP detection, classification, and containment. It detects Denial of Service (DoS) and impersonation attacks, and prevents client and network intrusions.

WIPS

Wireless Intrusion Prevention System. WIPS is a dedicated security device or integrated software application that monitors the radio spectrum of WLAN network for rogue APs and other wireless threats.

WISP

Wireless Internet Service Provider. WISP allows subscribers to connect to a server at designated hotspots using a wireless connection such as Wi-Fi. This type of ISP offers broadband service and allows subscriber computers called stations, to access the Internet and the web from anywhere within the zone of coverage provided by the server antenna, usually a region with a radius of several kilometers.

WISPr

Wireless Internet Service Provider Roaming. The WISPr framework enables the client devices to roam between the wireless hotspots using different ISPs.

WLAN

Wireless Local Area Network. WLAN is a 802.11 standards-based LAN that the users access through a wireless connection.

WME

Wireless Multimedia Extension. WME is a Wi-Fi Alliance interoperability certification, based on the IEEE 802.11e standard. It provides basic QoS features to IEEE 802.11 networks. WMM prioritizes traffic according to four ACs: voice (AC_VO), video (AC_VI), best effort (AC_BE) and background (AC_BK). See WMM.

WMI

Windows Management Instrumentation. WMI consists of a set of extensions to the Windows Driver Model that provides an operating system interface through which instrumented components provide information and notification.

WMM

Wi-Fi Multimedia. WMM is also known as WME. It refers to a Wi-Fi Alliance interoperability certification, based on the IEEE 802.11e standard. It provides basic QoS features to IEEE 802.11 networks. WMM prioritizes traffic according to four ACs: voice (AC_VO), video (AC_VI), best effort (AC_BE), and background (AC_BK).

WPA

Wi-Fi Protected Access. WPA is an interoperable wireless security specification subset of the IEEE 802.11 standard. This standard provides authentication capabilities and uses TKIP for data encryption.

WPA2

Wi-Fi Protected Access 2. WPA2 is a certification program maintained by IEEE that oversees standards for security over wireless networks. WPA2 supports IEEE 802.1X/EAP authentication or PSK technology, but includes advanced encryption mechanism using CCMP that is referred to as AES.

WSDL

Web Service Description Language. WSDL is an XML-based interface definition language used to describe the functionality provided by a web service.

WSP

Wireless Service Provider. The service provider company that offers transmission services to users of wireless devices through Radio Frequency (RF) signals rather than through end-to-end wire communication.

WWW

World Wide Web.

X.509

X.509 is a standard for a public key infrastructure for managing digital certificates and public-key encryption. It is an essential part of the Transport Layer Security protocol used to secure web and email communication.

XAuth

Extended Authentication. XAuth provides a mechanism for requesting individual authentication information from the user, and a local user database or an external authentication server. It provides a method for storing the authentication information centrally in the local network.

XML

Extensible Markup Language. XML is a markup language that defines a set of rules for encoding documents in a format that is both human-readable and machine-readable.

XML-RPC

XML Remote Procedure Call. XML-RPC is a protocol that uses XML to encode its calls and HTTP as a transport mechanism. Developers who want to provide integrated applications can use the API to programmatically perform actions that would otherwise require manual operation of the user interface.

ZTP

Zero Touch Provisioning. ZTP is a device provisioning mechanism that allows automatic and quick provisioning of devices with a minimal or at times no manual intervention.