

WLAN 9100

Release Notes

Release Notes for Avaya WLAN 9100 Access Point Operating System (AOS) Release 7.6.1

1. Introduction

This document provides details on the Avaya WLAN 9100 Access Point Operating System (AOS) software release 7.6.1.

AOS Rel 7.6.1 is suitable for the following Access Points

- WAP9132 – Indoor, two radio 2x2 802.11ac Access Point
- WAE9132 - Indoor, two radio 2x2 802.11ac Access Point with External Antennas
- WAP9133 - Indoor, two radio 3x3 802.11ac Access Point
- WAP9172 - Indoor, four radio 2x2 802.11ac Access Point
- WAP9173 - Indoor, four radio 3x3 802.11ac Access Point
- WAO9122 – Outdoor, two radio 2x3 802.11n Access Point
- WAO9132 - Outdoor, two radio 2x3 802.11ac Access Point
- WAP9122 - Indoor, two radio 2x2 802.11n – License Upgradable 802.11ac Access Point
- WAP9123 - Indoor, two radio 3x3 802.11n – License Upgradable 802.11ac Access Point

Note: WAP9112 and WAP9114 – Access Point requires the AOS-Lite Software Images. This release notes document does not cover the AOS-Lite Software Release Notes.

Note: WAP9144 Access Point requires AOS Rel 8.1.0 or above and AOS Rel 7.6.1 is not applicable for WAP9144.

1.1 New in AOS Rel 7.6.1

The following are new features / enhancements introduced in AP Operating System Rel 7.6.1.

- Support of User Name Attribute when the SSID is using Radius MAC authentication.
  - The returned user name in Radius Accept message is populated in client table and used in subsequent Radius Accounting messages.

- Captive Portal / Web Page Redirect (WPR) Login capability within User Groups
  - Allows for specifying unique Captive Portal Pages with Internal or External Login per User Group.
  - Previous releases only supported Landing page and Internal Splash page within User Groups.
  - Feature can only be configured from WOS using the Config Template option

2. Software Image File Details

The following section provides the software image file details for release 7.6.1.

- Access Points delivered from the factory may not be running GA software version. It is recommended to upgrade all the Access Points to the current software version when they are deployed.
- WLAN 9100 APs running 7.0.x software are required to be upgraded to AOS Rel 7.0.7 before upgrading to Rel 7.2.x or later software versions.
- Rev 3 of WAP9132, WAP9133, WAP9122 and WAP9123 APs are required to be upgraded to AOS 7.5.x or later and these APs cannot be downgraded to AOS 7.2.x or older code stream.

Component	File Name	File Size (bytes)
Avaya OS for WLAN 9100 Series Access Points (AOS)	XS-7.6.1-6271.bin	78,180,143

Table 1: Software Image File Details

The AOS 7.6.1 software release can be used with Wireless LAN Orchestration System 7.5.x or later.

WOS 7.5.x can be downloaded from the support portal at https://support.avaya.com/downloads/downloads-landing.action?product_id=P1570&product_name=Wireless+LAN+9100+Series&release_number=releaseId&contentType=Downloads

3. Resolved Issues

Table 2: WLAN 9100 Resolved Issues for AOS 7.6.1

Resolved Issues for WLAN 9100 AOS Access Points
26206 – WAP9132 / WAP9122 – Access Point sometimes reboots after having two disabled SSIDs enabled
26167 – Auto-Channel algorithm updated so non-DFS channels vs DFS channels have same weight.
26105 – Device Classification for Legacy 1x1 windows laptop was erroneously classified as a laptop
26053 – RADIUS Accounting Stop packet contains calling-station-id in the User-name field
26037 –On an SSID using Radius MAC, the session timeout value from the server was not honored
26011 – Filters – Unable to select interface “iap” as filter source or destination
25960 – Intermittently adding filters caused AP to reboot during the configuration push.
25953 – In some instances Preset Filter could not be added to a filter list
25926 – WMI – Pinging a host in the WMI produces an error
25842 – Intermittently Radio in monitor mode was not initialized correctly, affecting radio assurance and rogue detection.
25744 – Occasionally WAP9133 Access Point restarts with GPC Error with “Unable to handle kernel paging request at virtual address c00000000333f008, epc == ffffffff8060fa6c, ra == ffffffff8060fffc” error message.
25704 – Netflow / IPFIX – Some Output flows are in little Endian and other are in Big Endian.
25709 – Statefull Filter setting is sometimes not updated correctly when Application Control is disabled
25007 – Access Points sometimes become unreachable on the network and AP MAC address is aged out on the PoE Switch port and AP stops servicing clients.
24397 – ACL entries added by intrusion detection cannot be deleted successfully
24208 – MDNS filtering is not blocking Apple TV discovery correctly
12818 – Application Control – Packet count displays zero for an Application Control entry with a QoS value of 1

4. Known Issues

Table 3: Known Limitations for WLAN 9100 AOS Rel 7.5.4

Known Limitations for WLAN 9100 AOS Access Points
26412 – WPA/TKIP only SSID – For SSIDs using WPA/TKIP encryption, changes in the SSID settings could cause the station to fail association. As a workaround a radio need to be enabled and disabled.
25830- With Country Code Bahamas (BS) AP does not support DFS channels and association rates are very low on non-DFS channels as well
25605 – When logged into WMI using Google Chrome, sort Rogues APs by “Last Active” result in a reverse order.
25562 – With WMM – Admission Control for Voice and Video enabled, voice quality issues may be observed using Avaya Communicator application on certain smartphones. Recommendation is to disable ACM Voice and Video when using Avaya Communicator application over iOS and Android devices.
24999 –When Layer3 roaming is enabled, changes to OKC settings are not being saved automatically. The unit needs to be rebooted for the changes to take effect
24381 - Because IDS defaults are updated with AOS rel 7.5.4, Previous IDS configuration will not be preserved when upgrading from earlier release to AOS 7.5.4 or above. A Profile sync is required if any of the IDS configuration was previously modified from defaults.
24241 – Rebooting an AP sometimes takes a long time to complete the boot-up.
23467 - Intermittently, some Wireless Clients fail to complete the 4-way EAP handshake with OKC enabled as part of the re-association process. A new CLI configuration option is introduced to enable/disable OKC if the environment has clients that experience these issues.
23440 - In WMI, the Filter page may take long time to display
23270 – Some of the hyperlinks in application control page do not function
23195 - Firmware Upgrade can sometimes fail using TFTP. As a workaround use FTP or http-get
23058 - Radius Admin Shared Secret does not support special characters :!$&()|\"`;<>?. on WLAN 9100 Access Points
23012 - Internal Splash Page configuration for Captive Portal (WPR) may be lost in some cases when upgrading from previous AOS versions to 7.5.x or above. WOS Profile Sync may be required after the upgrade to resolve this issue.
22978 – WMI – Active Directory Secret shows failure when should be success
22756 - Layer 3 roaming with internal DHCP with NAT is not recommended in this release.
22003 - Radius Admin Authentication only supports PAP, CHAP and MS-CHAPv1.
21651 - Some of the newer Samsung and Motorola phones are not classified as Phone under the device types

Known Limitations for WLAN 9100 AOS Access Points
21321 - Attempting to upgrade AOS on multiple APs using cluster mode results in some APs not being upgraded. Workaround is to upgrade APs individually or use WOS.
21216 - RADIUS Accounting packets have incorrect Das Event Timestamp. The timestamp is also sent when it is configured to not include it.
19824 – User Group station limit is not enforced correctly.
19362 – WPR – using a non-standard HTTPS/SSL ports for WPR redirect-url does not work. Use port 443 for HTTPS/SSL support
16435 - Wireless Packet Capture is not supported on the 802.11ac WLAN 9100 Access Point models. Only WAO9122 supports remote wireless packet capture with the current release.
14826 – WMI – Filters cannot be added to filters list if name has a special character.
In WMI for an AP in cluster mode (Configuration > IAPs > IAP Settings), IAP channels cannot be changed at this time. The dropdown menu shows only the channel selected.
WMI Security page is not properly aligned when using Internet explorer browser. Use Chrome, Safari and Firefox as a work around since they don't exhibit this issue.
Doing a bulk configuration of more than 30 rogues does not work. Workaround is to limit bulk rogue configuration to less than 30.