



WLAN 9100

Release Notes

Release Notes for Avaya WLAN 9100
Access Point Operating System (AOS)
Release 8.2.0

1. Introduction

This document provides details on the Avaya WLAN 9100 Access Point Operating System (AOS) software release 8.2.0.

AOS Rel 8.2.0 is suitable for the following Access Points

- WAP9144 – Indoor, two radio 4x4 802.11ac Wave 2 Access Point
- WAP9133 - Indoor, two radio 3x3 802.11ac Access Point
- WAP9132 – Indoor, two radio 2x2 802.11ac Access Point
- WAE9132 - Indoor, two radio 2x2 802.11ac Access Point with External Antennas
- 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.

1.1 New in AOS Rel 8.2.0

The following are new features / enhancements introduced in AP Operating System Rel 8.2.0.

- WAO9122 support in the AOS 8.x code train, including all AOS 8.1.x features.
- WPR / Captive Portal redirection for HTTPS
 - Intercept first URL requested traffic (either HTTP or HTTPS) for unauthenticated users and redirect to the different WPR options
- LLDP daemon to start before other daemons in the AP.
 - the traffic will not flow until the AP is authenticated against the identity engines.
- RADIUS primary to secondary fail-over enhancement
 - Added a fail-over timeout (available globally and per SSID) with a default value of 60 seconds and a configurable range of 10 to 600 seconds.
 - When the timeout is reached the AP will switch to the secondary radius server.
- Hard Enforcement (UPSK– Easy Pass Onboarding)
 - Supports a clear authentication command that will clear cache of the station record when connected to an SSID that uses UPSK (Easy Pass Onboarding).
- Create policies per device class in an SSID (Configurable via CLI, XMS Cloud profile, or XMS Enterprise config template)
 - Configure a device class as a source and or a destination for a specific filter
 - Modify the device in the group policy to include only the device's class and not individual device types.

- Support of DFS Channels on the WAP9144
- Enable Weather Band Channels 120, 124 and 128 in US only
- Country code list was updated:
 - Added Ecuador
 - Added Algeria
 - Added Vietnam
 - Updated Qatar channel list (100-140 out 149-165 indoor only)

2. Software Image File Details

The following section provides the software image file details for release 8.2.0.

- AOS 8.2.0 is the GA software for WAP9144 and it is recommended that all WAP9144 APs should be upgraded to AOS 8.2.0 or above for improved reliability and performance.
- Access Points delivered from the factory may not be running the 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-8.2.0-6852.bin	8,379,328

Table 1: Software Image File Details

The AOS 8.2.0 software release can be used with Wireless LAN Orchestration System 8.0.x or later.

WOS 8.0.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=releaseld&contentType=Downloads

3. Resolved Issues

Table 2: WLAN 9100 Resolved Issues for AOS 8.2.0

Resolved Issues for WLAN 9100 AOS Access Points
14826 - WMI only - cannot add filters to a filter-list if the filter-list has special characters in the name.
25637 - WAP9144 reports Android devices as Apple iPhone and Linux Notebook
25948 - CLI - user experiences General Error when they attempt to disable autonegotiation on Gig1.
26984 - Application control on a WAP9123 & WAP9133 is unable to block Facebook video whether in the Facebook app or browser when using fb_video as the application to block.
27055 - Radio Resets - excessive radio resets on WAP9144 with 200 Stations - MI_MACSSPND and Fatal Error.
27079 - SSID WEP - on a Broadcom processor, WEP does not work. STA can associate and pass traffic but connection is ENC None.
27142 - Block Apple Update AppCon rule does not block iOS updates.
27276 - DHCP daemon and other daemons are delayed from starting when Fabric Attached is disabled.
27280 - Apple TV - not visible to stations on neighboring APs when on an WAP9144 set to MCST isolation AP+Neighbors (B1 only)
27374 - WMI SSID Management page locks up when using special characters for PSK.
27387 - Radius-Failover - doesn't work when the SSID is set as WPA or WPA2 EAP.
27596 - Xbox One Systems were not recognized as device class "game console"
27693 – On a WAP91x2, significant performance impact caused by inactive filters.
27734 - Change the Radius failover default value from 60s to 10s
28189 - AP goes offline due to failed health check and high CPU utilization.
TKT-80893 – WAP9144 does not support the 5 Gig DFS channels. Must update the OS to AOS 8.2.0.

4. Known Issues

Table 3: Known Issues for WLAN 9100 AOS Rel 8.2.0

Known Issues for WLAN 9100 AOS Access Points
24598 - Radius- must use quotes "" to add the word "secret" as a password.
25558 - Standby Mode – Enabling standby mode on an SSID could cause a General Error. It is not recommended to use this feature with this release
25665 - When running MuMiMo with 10STA, the WAP9144 does not group stations
25764 - Association – In noisy environments, clients may be slow connecting to 80Mhz bonded channels
26045 - Admin RADIUS – Admin RADIUS is not working with IPv6
26222 - RADIUS – No RADIUS packets are sent to server from PEAP client when primary server is using IPv6
26606 - Console Timeout – Console timeout value is not respected. Workaround is to set the Xircon timeout and the console timeout to the same value. As designed.
26635 - L3 Roaming – Layer 3 roaming using Spectralink 8440 and WPA2-PSK is not working. Works with WPA2 Enterprise
26771 - Spectralink 8020 – Spectralink 8020/30 cannot associate in the 2.4G band on WAP9144.
27041 - Radio Assurance – Radio assurance feature is not functional on the WAP9144.
27310 - Loss of IP connectivity on the WAP9144 radios, after station associates to UPSK SSID
27376 - WPR SSL Redirect - Chrome does not allow the user to accept the SSL Certificate
27400 - Factory reset via AP WMI result discovery and default profile assignment with a failure in the configuration push.
28104 - On the WAP9144, the QoS UP bit in QoS Control Field is always set to whatever QoS setting is set on the SSID
28490 - Protected Management Frames not fully supported on the WAP9144.
28711 - APs may occasionally crash and reset when station to station blocking is set.
28493 - LLDP displays the XRP tunnel IP address as the Management address versus displaying AP Management IP.

Known Issues for WLAN 9100 AOS Access Points

28532 - "40MHz Auto bond" off and "auto-channel power-up" on the WAP9144 5GHz radio stops beaconing after auto-channel completes after boot-up

28534 - On the WAP9144 5GHz radio, with "40MHz Auto bond" off, when auto-channel is performed twice, the 5GHz channel stops beaconing.