HiveOS 8.0r1 Release Notes

Release date: April 28, 2017

Release versions: HiveOS 8.0r1

Hardware platforms supported: AP122, AP130, AP230, AP245X, AP250, AP550, and AP1130

Managed by: HiveManager Classic 8.0r1and later, and HiveManager NG 11.20 and later

Enhancements and Changes in Behavior

This release adds the following enhancements and changes in behavior:

ACSP (Automatic Channel Selection Protocol) Improvements:

- Access points now store the last-used channel and power settings across a reboot, speeding up the restoration of the previous radio environment.
- With this release, SDR (Software-Defined Radio) disables redundant 2.4 GHz radios when it detects sufficient coverage from neighboring 2.4 GHz radios.
- For dual 5 GHz-capable platforms, you can now let ACSP decide whether to run in 2.4 and 5 GHz mode or in dual 5 GHz mode.

Enhancements applicable to all supported platforms:

- This release improves multi-client bandwidth distribution, resulting in improved fairness and increased aggregate performance.
- The Aerohive WIPS mitigation process has been enhanced to ensure that WIPs behavior is consistent for all client types. The interval between deauthentication packets sent to all clients has been decreased.
- With this release, AP radios (with the exception of the AP122) can automatically adjust bandwidth based on the OBSS (overlapping BSS) threshold by expanding or shrinking the channel width.
- This release adds support for non-ASCII characters in SSID strings.
- This release lets you create individualized success pages with redirect URLs for logins on external captive web portals.
- This release lets you control whether an Apple Captive Network Assistant displays a log-in window when using IP firewall redirect.
- This release allows Client Monitor 2.0 to send realtime data through TLV parameters to HiveManager Classic.
- The channel width for the default radio profile radio_ac0 has been reduced to 20MHz for a better out-of-box experience in production environments.

Platform-specific enhancements:

- This release adds the ability to automatically switch the wifi0 radio band of Dual-5G APs, whenever RF is significantly redundant for the current band.
- The limit for concurrent associated clients on 2.4 GHz and 5 GHz radios has been increased from 100 to 200+ for the AP130, AP1130, AP230, AP250, AP245X, and AP550. The default remains at 100. AP122 remains at a 100 client limit.
- This release introduces support for Hotspot 2.0 in AP245X, AP250, and AP550 for secure and automatic Wi-Fi connectivity to carrier or subscriber networks.
- This release adds voice enterprise support (with official certification) for the AP250, AP245X, and AP550.
- WMM-AC is supported in this release on AP250, AP245X, and AP550.
- This release adds support for smart antennas for the AP550 and AP250.
- This release supports 4 spatial streams per radio for MU-MIMO-capable clients on the AP550.

- Zero-wait DFS handling is now available for the AP250, AP245X, and AP550.
- This release adds FCC DFS (dynamic frequency selection) support for the AP122, AP245X, and AP550.
- This release enables APs to restore the last-used DFS static channel after the NOL (non-occupancy-list) timeout.
- Sector antennas (in addition to omnidirectional) are supported for the AP1130.
- With this release, users can no longer make channel and power changes that do not meet the new CE regulatory compliance requirements. This applies to the AP122, AP130, AP230, AP245X, AP250, AP550, and AP1130.

Known issues in HiveOS 8.0r1

This is the inaugural release of HiveOS 8.0r1,there are no known issues.

Addressed Issues in HiveOS 8.0r1

The following issues were addressed in the HiveOS 8.0r1 release.

CFD-2438	AP550 and AP250 access point erroneously deauthenticated nearby client devices when the APs were deployed in environments containing both Qualcom and Broadcom radio chipsets.
CFD-2382	Captive web portal changes were not being uploaded to AP130s.
CFD-2377	AP130 and AP230 devices were truncating initiate-session and terminate-session commands for a network policy that was configured to perform logging. As a result, logging did not occur.
CFD-2343	When multiple PSK SSIDs were configured, RSN (Robust Security Network) information was missing on beacon or probe response packets for some SSIDs, preventing clients from connecting through the affected SSIDs.
CFD-2309	HiveOS ACSP (Automatic Channel Selection Protocol) was blacklisting iOS clients when invoked by scheduled scanning or when an interference threshold was reached.
CFD-2248	Although WMM (Wi-Fi Multimedia) was disabled, the 802.11e load element was still advertised in frames.
CFD-2247	Cisco 7925G phones were experiencing difficulties making and receiving calls.
CFD-2245	The Available Admission Capacity was always displayed as 0.
CFD-2207	When configuring MAC-based authentication, invoking the `fallback-to-ecwp` command resulted in an HTTP 500 error.
CFD-2200	Reconnection and display issues occurred when using a user policy acceptance captive web portal (eCWP).
CFD-2158	An override of the VLAN defined in the user profile did not work using RADIUS CoA (Change of Authorization), but did work with 802.1x authentication.
CFD-2135	The time accrued against a session timeout was resetting after a client roamed.
CFD-2120	After a restart, users with revoked PPSKs could still connect to the network.
CFD-2119	AP130s were responding to probes with invalid AIFS (Arbitration Inter-frame Spacing) values.
CFD-2118	Acct-Session-ID and Acct-Multi-Session IDs were missing from RADIUS Access-Request packets.
CFD-2105	AP130s were unable to connect using the Colombia country code and channel 13.
CFD-2100	Multi-cast DNS frames were using excessive CPU cycles.
CFD-2060	French language characters were not displaying correctly.
CFD-2024	HiveOS was reserving the incorrect maximum PoE power settings.

CFD-1921	Packet MTU increased on the tunnel0 interface on the HiveManager Virtual Appliance.
CFD-1790	AP230 devices experienced false radar detection.
HOS-9968	Spectrum analysis was not functioning properly on the AP122.
HOS-8851	iPhone and iPad clients continuously reconnected due to an unsuccessful 4-way handshake.
HOS-6308	QoS airtime did not take effect even though it was enabled.