HiveOS 6.5r5 Release Notes

Release date: August 31, 2016

Release versions: HiveOS 6.5r5

Hardware platforms supported: AP110/120, AP121/141, AP130, AP230, AP330/350, AP370/AP390, AP1130, BR100, BR200, BR200-WP, BR200-LTE-VZ, SR2024P, SR2124P, SR2048P, VPN Gateway Virtual Appliance.

Managed by: HiveManager 6.8r3 and later, and HiveManager NG 11.16.1.10 and later

Features and Enhancements

This release adds support for the following features and enhancements:

- This release adds three new system OIDs (Object Identifiers) for CPU, memory, and connected client count to legacy QCA platforms. The OIDs are defined in the file "ah_system_mib.txt", included with HiveManager at Home > Administration > Auxiliary File > MIB files.

Changes in Behavior and Appearance

Due to memory constraints, the AVC (Applications Visibility and Control) subsystem (on AP121 and AP141 devices only) has been reverted to version 4.x. The main change is a less-granular identification of applications, with the implication that some applications recognized by other HiveOS 6.5r5 devices may not be recognized by AP121and AP141 devices, or the application may be mis-identified.

Known Issues in HiveOS 6.5r5

There are no known issues for this release.

Addressed Issues

The following issues were addressed in the current and previous HiveOS releases.

Addressed Issues in HiveOS 6.5r5

CFD-1947	The AeroScout server was not able to process data sent by a tag through an AP230.
CFD-1928	Previously, HiveOS misinterpreted an NTP server message intended to signify that the correct time was not available or was not yet set on the server, resulting in time stamps indicating the year 2036. This also affected services such as ID Manager and IPSec tunneling.
CFD-1905	SNMP traps sent by an AP230 with embedded IP addresses reversed the IP addresses.
CFD-1860	AP IP sessions increased significantly after a classifier map was pushed to the configuration.

CFD-1833	The `show vpn ike sa` and `show vpn ipsec sa` commands were not displaying data for the VPN Gateway Virtual Appliance.
CFD-1820	DHCP packets were using invalid client MAC address for Bonjour Gateway.
CFD-1811	The transmit (Tx) power for AP130 devices was displayed as 31 dBm after a reboot.
CFD-1805	There were inconsistencies in the `show ACSP neighbor` and `show hive neighbor` RSSI output.
CFD-1801	AP370 devices were spontaneously rebooting.
CFD-1798	MAC authentication and 802.1x authentication were not using the same action when the user-profile-mapping function was enabled.
CFD-1795	RADIUS class attributes were no longer available after a BSS transition.
CFD-1759	Legacy clients could not be authenticated with LEAP (Lightweight Extensible Authentication Protocol).
CFD-1719	The list of friendly APs that appeared on non-DA APs did not include all the information that appeared on the list for DA APs.
CFD-1706	APs were incorrectly recognizing themselves as rogues.
CFD-1195	AP121 access points were returning a page allocation error after experiencing high memory usage.
HOS-7525 (14158)	Under certain circumstances, hardware TCP checksums were incorrectly calculated, resulting in the AP320 and AP340 corrupting forwarded frames.
HOS-7478	Weak (96-bit or shorter) ciphers and the SHA-1 MAC algorithm, retained for backwards compatibility with old client devices that did not support modern crypto ciphers or MAC algorithms, have been removed, to prevent false positives from security scanners.
HOS-7312	The event-timestamp field was missing from the Accounting-On, Accounting-Off, and Start forms of the Accounting-Request packets.
HOS-7311	The Acct-Delay-Time RADIUS attribute was missing from Accounting-Request packets.
HOS-7310	Accounting-Off Accounting-Request packets were not being sent by HiveOS when a reboot command was issued.
HOS-7220	Self-signed certificates, used for securing HTTPS access to the HiveOS device, have been updated to use the SHA-256 algorithm for signing.
HOS-7134	Enabling <b>Redirect to the initially requested page</b> using the access web server's page as the first URL created an endless loop of login requests.
HOS-6261	The Filter ID was unable to assign a user profile correctly.

Addressed Issues in HiveOS 6.5r4

CFD-1750	UDP CAPWAP connections would sometimes close and then reopen over HTTP. When this occurred, client devices could not communicate with the network.
CFD-1722	After upgrading AP230 access points to HiveOS 6.5r3, some client devices would intermittently not receive DHCP offers that were being sent by the DHCP server.
CFD-1703	The SR2024P switch operating in router mode becomes unresponsive during bootup when using the Huawei E8372 modem as the backup WAN port and the primary WAN connection is removed.
CFD-1693	The four-way handshake process was sometimes unsuccessful because of unexpected WPA key data returned by the supplicant.

CFD-1686	SR2024P switches were reporting the IP address octets of connected hosts to HiveOS in reverse order.
CFD-1647	Macbooks sometimes did not process the 802.11h power constraint value correctly, which resulted in a transmit power setting that was too low. This version of HiveOS introduces Client Transmit Power Control, now disabled by default, which instructs the client device to match the AP transmit power.
CFD-1581	The RADIUS failover process was taking several seconds, causing some clients to disassociate, and then be unable to re-associate after the process completed.
CFD-1550	VPN tunnels being negotiated by the BR200-WP router would sometimes take several minutes because the xauth-request packet was not received when expected.
CFD-1502	BR200 routers sometimes reported an incorrect vendor ID to HiveOS during the configuration upload process, which resulted in HiveOS reporting an error and preventing a successful configuration upload.
CFD-1374	Clock drift of some HiveOS devices would sometimes create sufficient disparity to cause VPN tunnels to close and then need to be renegotiated, producing data transfer interruptions.
CFD-1383	After upgrading to HiveOS 6.6r1, devices were unable to execute the DHCP option commands properly.
HOS-6723	Although there is no method to exploit CVE-2015-7547 within HiveOS, Aerohive has updated HiveOS to prevent false positive responses being generated by security software.

Addressed Issues in HiveOS 6.5r3a

HOS-5200	Aerohive devices demonstrated small, but constant packet loss in active VoIP sessions when there was simultaneous lower-priority traffic, for example, background file transfers and streaming video.

Addressed Issues in HiveOS 6.5r3

CFD-1331 CFD-1245	The VPN daemon running on the HiveOS Virtual Appliance spontaneously restarted, causing all active VPN tunnels to reset unexpectedly.
CFD-1289	The AP230 was reporting the incorrect transmit and receive airtime counts.
CFD-1111	When authenticating through a HivePass captive web portal, the user profile was assigned an incorrect user profile attribute value.
CFD-1097	The byte order of the IP address was reversed as reported by SNMP v2C traps on the AP230, which resulted in the apparent failure of applications due to firewalls dropping packets with bad reverse IP addresses.
CFD-897	NetConfig UI reported a validation error when a password was configured to end in the letter z.
HOS-2635	On Aerohive SR-series switches, performing an SNMP walk (snmpwalk) resulted in an error.
HOS-1680	The Troubleshooting tool within HiveOS NG was incorrectly reporting that clients configured an incorrect static IP address or gateway although the clients were properly configured and functioning correctly on the network.