HiveOS 6.5r4 Release Notes

Release Date: May 10, 2016

Release Versions: HiveOS 6.5r4

Platforms supported: AP110, AP120, AP121, AP130, AP141, AP170, AP230, AP320, AP330, AP340, AP350, AP370, AP390, AP1130, BR100, BR200, BR200-WP, BR200-LTE-VZ, SR2024, SR2024P, SR2124P, SR2148P, VPN Gateway Appliance, VPN Gateway Virtual Appliance

HiveManager platforms supported: HiveManager NG, HiveManager Online, HiveManager Appliance

These are the release notes for HiveOS 6.5r4 software. Known issues are described in "Known Issues" on page 1 and "Addressed Issues" on page 2.

New Features and Enhancements

The following changes to behavior and appearance have been introduced in the 6.5r4 release:

HiveOS 6.5r4 represents the integration of previous HiveOS versions supporting different features and hardware platforms. HiveOS 6.5r4 now supports all Aerohive device platforms, is a unified expression of support for all relevant features, and is the most stable HiveOS release yet.

LED Behavior: Additional flexibility in the behavior of the status LED on all devices running HiveOS 6.5r4 has been enhanced, and now provides added continuity in default behavior across devices, as well as the ability to configure custom blink behavior.

Changes in Behavior and Appearance

The following changes to behavior and appearance have been introduced in the 6.5r4 release:

FCC DFS Compliance: Some devices based on older radio chipsets are unable to comply with new FCC rules that take effect on June 1, 2016. HiveOS 6.5r4 prevents the non-compliant use of DFS channels on the AP121/141, AP330/350, and AP370/390 hardware platforms sold after June 1, 2016.

Devices sold before June 1, 2016 are not bound by the new regulations and can continue to use DFS channels.

Known Issues

No major known issues were found in HiveOS 6.5r4.

Addressed Issues

The following issues were addressed in the HiveOS and HiveManager 6.5r4 releases.

Addressed Issues in HiveOS 6.5r4

CFD-1750	UDP CAPWAP connections would sometimes close, and then renegotiate a CAPWAP connection over HTTP. When this occurred, client devices could no communicate with the network.
CFD-1722	After upgrading AP230 access points to HiveOS 6.5r3, some client devices would intermittently not receive DHCP offers, despite the DHCP offers 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 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 HiveManager 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 associate afterward.
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 HiveManager during the configuration upload process, which resulted in HiveManager reporting an error and preventing a successful configuration upload.
CFD-1374	Clock drift of some HiveOS devices would sometimes cause sufficient disparity to cause VPN tunnels to close and need to be renegotiated, causing 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 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) would result in an error.
HOS-1680	The Troubleshooting tool within HiveManager NG was incorrectly reporting that clients configured an incorrect static IP address or gateway when the clients were properly configured and functioning correctly on the network.