HiveOS 6.5r3 Release Notes

Release Date: November 21, 2015

Release Versions: HiveOS 6.5r3

Platforms supported: AP110, AP120, AP121, AP130, AP141, AP170, AP230, AP320, AP330, AP340, AP350, AP370, AP390, 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 6.5r3 software. Known issues are described in "Known Issues" on page 2 and "Addressed Issues" on page 3.

Although HiveOS 3.4r4 was the last release for the HiveAP20 series, the current HiveManager can continue to manage all Aerohive platforms. However, you must push full configuration updates to these devices because some commands have been removed, which would cause delta configuration updates to fail. HiveManager can support full and delta configuration updates to APs, BRs, and SR series devices running HiveOS 6.0, and later.

New Features and Enhancements

The following changes to behavior and appearance have been introduced in the 6.5r3 release:

HiveOS 6.5r3 represents the integration of previous HiveOS versions supporting different features and hardware platforms. HiveOS 6.5r3 now supports all Aerohive device platforms, is a unified expression of support for all relevant features, and is the most stable HiveOS release yet.

OpenSSL Improvements: Cypher suites that are commonly used in building TLS tunnels and considered to be weak are no longer supported beginning with this release. As a result, default certificates now use SHA-256.

Diffie-Hellman Key Length: Aerohive devices acting as RADIUS servers now use a 2048-bit Diffie-Hellman key exchange. Formerly, a 512-bit key length was used.

FCC DFS Support for AP130: The AP130 now supports DFS (Dynamic Frequency Selection). DFS is used to detect and make operational allowances for the presence of critical-use transmissions, most commonly radar, by choosing a different frequency to prevent interfering with critical systems.

CAPWAP Discovery Enhancement: When a device is connected to a network and powered on, it begins the process of discovering HiveManager. In this release, Aerohive devices now support the use of DHCP Option 43 (Vendor Class Identifier) to prompt DHCP servers to return the location of HiveManager, which decreases the time required for the device to form a CAPWAP connection. To function properly, the DHCP server must be configured to return the IP address or host name of HiveManager.

iBeacon Support for AP121 and AP141: With this release, the AP121 and AP141 access points can now be configured to act as iBeacon tranmitters and iBeacon location monitors.

HiveOS Accounting and Data Limits: HiveOS 6.5r3 reports client data usage information directly to HiveManager NG, which then tracks usage. When a client reaches its pre-configure data usage limit, HiveManager NG broadcasts a disconnect message to the APs so that the associated AP can force the client off the network and the other APs prevent it from reconnecting elsewhere.

PPSK Authentication Enhancement: When a user authenticates to a network using PPSK, if the user cannot be authenticated on the local access point, then the authentication request is send to the authentication services in the cloud.

SNMP Trap Filter White List: In this release, administrators have the ability to filter SMTP traps, allowing those SNMP traps on the white list to be forwarded to the SNMP server, while disallowing traps that are not on the white list. You can configure SMNP trap white list using the Supplement CLI tool in HiveManager using the following CLI commands:

```
logging trap all [ {emerg|alert|crit|err|warning|notice|info} ]
```

See the full syntax description in the AP330 CLI Reference Guide in the Help system.

```
logging trap white-list category {failure|threshold|statechange|connectionchange
  |idp|powerinfo|channelpower|mitigate|clientinfo|interferencealert|bwsentinel
  |alarmalert} [ {emerg|alert|crit|err|warning|notice|info} ]
```

See the full syntax description in the AP330 CLI Reference Guide in the Help system.

Although the CLI Reference Guide links above are specifically for the AP330 and AP350, this command is available on all devices in the list of supported platforms at the beginning of this document.

Changes in Behavior and Appearance

The following changes to behavior and appearance have been introduced in the 6.5r3 release:

VPN Encryption Enhancement: Aerohive devices running HiveOS 6.5r3 now default to the use of AES-256 encryption for VPN Phase 1 and Phase 2.

Known Issues

The following known issues were found in the HiveOS 6.5r3 release.

Known Issues in HiveOS 6.5r3

HOS-5200	Aerohive devices demonstrate small, but constant packet loss in active VoIP sessions when there is simultaneous lower-priority traffic, for example, background file transfers and streaming video.
HOS-5121	Devices running Bonjour Gateway sometimes generates large amounts of mDNS traffic, which can affect traffic throughput and CPU usage. **Workaround**: Because HiveOS 6.5r3 reduces this behavior, update all devices to HiveOS 6.5r3 or later.

HOS-5024	The AP121 sometimes becomes unresponsive when uploading a configuration containing application signatures. **Workaround**: Do not upload AVC signatures to the AP121 and AP141 access points. In addition, upgrading these devices to HiveOS 6.5r3 uploads the latest AVC signatures on the devices.
HOS-4624	The AP 110 and AP120 report 100% CPU usage immediately after booting. This occasionally causes the AP to become unresponsive. **Workaround**: Update all devices to HiveOS 6.5r3 and consider redeploying AP120 mesh points to act as portal devices instead to reduce processor burden.

Addressed Issues

The following issues were addressed in the HiveOS and HiveManager 6.5r3 releases.

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.

Addressed Issues in HiveOS 6.5r2

HOS-185	If the client device operating system was unknown to the Aerohive device, the Aerohive device was unable to assign an IP address to the client when reassigning it to the prescribed user profile.
35787	Client devices did not appear properly on floor plans within HiveManager with location services enabled.

Addressed Issues in HiveOS 6.5r1a

HOS-185	If the client device operating system was unknown to the Aerohive device, the Aerohive device was unable to assign an IP address to the client when reassigning it to the prescribed user profile.
35787	Client devices did not appear properly on floor plans within HiveManager with location services enabled.

Addressed Issues in HiveManager 6.5r1

CFD-295	The location-based report displayed information for all locations regardless of the filter settings.
CFD-892	Incorrect information was appearing in the csv file for the Client Report.
CFD-924	Planner Map reports were not generating correctly.