HiveOS 6.1r6c Release Notes

Release Version: HiveOS 6.1r6c

Platforms: AP110/120, AP121/141,AP170, AP230, AP320/340, AP330/350, BR100/200/200-WP/200-LTE-VZ, VPN Gateway, VPN Gateway Virtual Appliance, SR2024/2024P

Release Date: April 27, 2015

These are the release notes for HiveOS 6.1r6c firmware.

Known Issues

The following issues are known issues in the HiveOS 6.1r6c release.

Known Issues in HiveOS 6.1r6c

CFD-353	After HiveOS firmware is upgraded in networks where Cisco Model 7925G phones are deployed, APs do not connect to the Cisco phones. WA (Workaround): Reboot the APs to establish connectivity with the Cisco phones.
32060	When an SR2024P device running HiveOS 6.1r3 is upgraded from 6.1r3 to 6.1r6 and you need to roll back to the previous version of HiveOS using the CLI reboot backup command, the 1-Gigabit fiber port connections do not return to their previous UP status. WA: If you need to roll back to the previous version of HiveOS, use the save image command rather than the reboot backup command.
32020	When the SR2124P or the SR2148P is connected to a 10G port on a Dell switch and the Dell port goes down, the corresponding 10G port on the SR2124P or the SR2148P reports a "down event" continuously in the error log.
31844	In some cases, link flapping on a Cisco switch can occur when connecting to an SR2124P or SR2148P switch. WA: Disable link flapping on the Cisco switch by entering the err-disabled command for the port that is experiencing flapping.
31730	The Layer 2 bridge access throughput of the AP230 is less than 500 Mbps.
29880	Enabling a WIPS (wireless intrusion prevention system) policy on an AP121 or AP141 that is set to perform semi-automatic or automatic rogue mitigation or that has rogue client reporting enabled can cause it to reboot intermittently. WA: For AP121 and AP141 devices, set rogue mitigation in manual mode and disable client reporting.
29826	A BR100 is sometimes automatically selected to be the arbitrator for WIPS mitigation although the BR100 platform does not support WIPS, which causes automatic and semi-automatic mitigation processes to fail. WA: Use manual rogue mitigation.
27160	In TeacherView, HiveOS can identify which URLs that teachers access, but it cannot identify which URLs that students access.

25625	Application reporting is affected when a topology consists of a HiveManager connected to a BR200 that is, in turn, connected to one or more APs. When an AP receives client traffic that contains application reporting, it reports this traffic to HiveManager. Then the BR200 reports this same application reporting traffic to HiveManager. This results in HiveManager reporting duplicate application traffic in the widgets on the Application tab.
25297	There is a mismatch in data reporting between the HTTP application in the "All Applications by Usage" and the TCP application in the "Top 20 Watchlist Applications by Usage" widgets in the Dashboard section when HTTP is not included in the "Top 20 Watchlist Applications by Usage" widget. If HTTP is not included in this watchlist, then the HTTP data is reported as TCP because the HTTP protocol runs on TCP. WA: Add HTTP, UDP, and TCP to your "Top 20 Watchlist Applications by Usage" widget. If possible also add SSL to this widget.
24230	An SR2024 in switch mode does not send the user profile ID of hosts connected to it to an Aerohive router upstream. Because the switch does not communicate the user profile ID, an upstream Aerohive router does not apply the user profile settings as expected. WA: Assign a user profile to the port on the router that is physically connected to the switch.
23952	When an SR2024 in router mode reaches maximum throughput capacity and silently begins discarding packets, it does not report them to the dropped packet counter.
23364	Application Visibility and Control does not differentiate the Google Calendar application from other Google applications due to changes made by Google.
20139	Although an SR2024 in router mode marks outbound traffic so that upstream devices can apply QoS, it does not apply QoS itself to the traffic it routes.
18080	An Aerohive router does not apply the same user profile to traffic that an AP forwards to it from a client connected to one of its Ethernet ports in bridge-access mode.
18053	MDM (mobile device management) enrollment does not work with Apple TVs because they cannot complete the enrollment process. Apple TVs do not have a browser to enroll in mobile device management. WA: Connect Apple TVs through SSIDs that do not have MDM enabled.
15474	With its default configuration, an AP mesh point cannot join the hive and then connect to the network using a BR100 as its portal because the BR100 wifi0 interface is in access mode. WA: Deploy the BR100 first and set its wif0 interface in dual mode so that it can provide network access to users and a wireless backhaul link for APs.

Addressed Issues

The following issue was addressed in the HiveOS 6.1r6c.

Addressed Issues in HiveOS 6.1r6c

33858	When Aerohive devices lost their CAPWAP connection to HiveManager, they stopped attempting to reconnect after a period of time. When this occurred, the Aerohive devices required a reboot to regain the CAPWAP connection.

Addressed Issues in HiveOS 6.1r6b

HiveOS vulnerability to CVE-2014-3566 (aka "POODLE") has been addressed in this release. For more details, see http://www.aerohive.com/support/security-center/security-bulletins/psa-cve-2014-3566-poodle.

Addressed Issues in HiveOS 6.1r6a

CFD-556	Newly created ID Manager PPSKs (Private Preshared Keys) sometimes failed to authenticate.
CFD-554	ID Manager relies on RadSec to secure communications on connections through an AP that acts as a RADIUS proxy to authenticate guests. The APs reported as RadSec proxies in HiveManager changed frequently, and those same APs reported as RadSec proxies in HiveManager were sometimes reported differently in their corresponding CLIs.
CFD-469	When a Layer 7 application rule was added to an existing stateful firewall in a user profile, traffic did not reach the Internet. If an ACL (Access Control List) was configured to use NAT (Network Address Translation) for all traffic from an AP and the Layer 7 rule is added, the AP no longer applied NAT to traffic leaving the eth0 interface. Because the traffic contained a source IP of a private subnet that resided behind the AP, return traffic could reach the station; the upstream network dropped the traffic because it did not contain routes for the return traffic.
CFD-366	After the admin classified a rogue AP as a friendly AP in HiveManager, it is possible that the AP will continue to be classified as a rouge AP under certain conditions.
CFD-226	AP330 and AP350 devices might have encountered an operational state where the radio no longer receives frames.
CFD-187	The AP121 became unresponsive on corporate networks when WIPS (wireless intrusion prevention system) was enabled.

Addressed Issues in HiveOS 6.1r6

CFD-255	Although its *Success* page was returned when the captive web portal was configured to display an acceptable use policy in an iOS 7 environment, iOS 7 disconnected the iPhone from the SSID.
CFD-207	HiveOS version 6.1r6 did not support HT40 for country code 392 (Japan) on APs and returned the message, "Radio capability does not support this phymode". To resolve this issue in HiveOS 6.1r6 and later versions, you must update the country code to "(392/4014) Japan". To update the country code, navigate to the *Aerohive APs* page, select the AP120s, AP121s, and AP141s, click **Update > Advanced > Update Country Code**, select (392/4014)Japan from the *New Country Code* drop-down list, and then click **Upload**.

CFD-164	When a captive web portal applied a new user profile to registered users redirecting them to a different VLAN and DHCP server, the Aerohive device did not release their originally assigned IP addresses.
32257	When an AP230 is using wide-channel mode (80-MHz channel width), its upstream and downstream throughput is about 20% lower than where Aerohive expects its performance to be. This issue is not present when operating on 20-MHz and 40-MHz channels.
32168	The default QoS rate control and queuing policies might limit the Layer 2 VPN encryption throughput rate on the VPN Gateway. WA: To increase the throughput, configure a QoS policy using the policing rate limit in Kbps. For example, set the rate limit to 2000000 Kbps.
32133	When the AP230 reported the interfaces, it displayed the incorrect value of -92 dBm for the noise floor.
32101	When both radios were active processing traffic in the wireless to wired direction, the overall AP230 throughput was lower than with 5 GHz traffic only.
31414	When a report was generated, the Transmit Bit Rate Distribution values displayed in HiveManager did not match the values read directly from the AP230.
31206	When band steering was enabled, the AP230 did not steer the configured ratio of dual-band capable clients to the 5 GHz band.
30446	Even when an AP230 required a boost of airtime tokens to meet its minimum targeted throughput level, its SLA status showed it as healthy at 10-minute intervals.
30343	When WIPS and spectrum analysis were both enabled on AP121 and AP141, they conflicted with each other and resulted in an excessively long time to complete the spectrum analysis or did not complete the spectrum analysis.
30285	If you manually cleared the Phase1 SA for an IPsec tunnel on an AP230 (`clear vpn ike sa`) and a wireless client disconnected and reconnected to the AP without reauthenticating itself, the AP230 did not rebuild the GRE tunnel to the VPN server. As a result, the client could not reach any destination requiring its traffic to pass through the tunnel.
30212	Mobile devices connected to an AP230 had their batteries drain faster than expected. This was because when a wireless device was about to go to sleep, it sent a message to the AP230. Then the AP230 responded that it had buffered data to send to the device even when the AP did not have any data. This occurred on both the wifi0 and wifi1 interfaces.
25193	Occasionally, after a reboot, the AP320 or AP340 would apparently be fully booted up but would take several additional minutes before clients could connect tot he 2.4 GHz radio.

Addressed Issues in HiveOS 6.1r4b

32933	The fan control has been enhanced to reduce noise for SR2124P and SR2148P switches.

Addressed Issues in HiveOS 6.1r3b

CFD-227	Disabling transmission at one or more of the default basic data rates caused Aerohive devicesto switch from 802.11n to legacy mode, resulting in much slower throughput.
CFD-53	Clients experienced losses in connectivity when the transmission buffer on an Aerohive device filled up, which occurred sporadically when the device processed IPv6 multicast traffic and which could sometimes take up to several minutes to clear.

Addressed Issues in HiveOS 6.1r3a

30200	When using AVC (Application Visibility and Control) on AP100 series devices, the amount of packet, session, and reporting data stored in memory can be so high that the APs cannot complete a HiveOS image upgrade. WA: Reboot the AP before performing an upgrade to clear the data stored in memory. Also, do not upgrade an AP when the network is busy because memory usage might be particularly high at that time.

Addressed Issues in HiveOS 6.1r3

29610	On a HiveOS Virtual Appliance configured with several BR200 routers, the VPN tunnel connection dropped for one or two minutes every 24 hours, after which each time the VPN was eventually reestablished.
29077 26650 25485 19799	Enabling the Aerohive WIPS (wireless intrusion prevention system) policy under different conditions produced various internal errors and caused the AP devices to reboot frequently and become unresponsive.
29054	While performing a RADIUS re-authentication in HiveManager 6.1r2, user names greater than 31 characters in length were truncated such that only the first part of user-name (31 characters in length) was cleared, and the second part of user name was retained.
28822	When the JSS (JAMF Software Server) was upgraded to version 9.0, the MDM (mobile device management) client appeared as enrolled in the JSS server, but appeared as not enrolled on the Aerohive AP. This is an issue with the JSS that cannot be corrected by Aerohive.
28934 28432	During some periods of time, data was not transmitted or received for several minutes even though clients remained connected to the SSID. After several minutes, the connections resumed without any intervention.
28872	When an AP could not reach the RADIUS server (when the server was on another subnetwork and the default gateway was not configured in the AP), the resulting error message that was supposed to describe this condition was not accurate.
28502	With the Bonjour Gateway enabled on the network policy (the default condition) and bound to Aerohive APs and switches, packets to and from port 5555 on an Aerohive switch flooded the network with UDP packets, rendering the network unusable.
28254	Authentication of multiple clients on single Ethernet port of a captive web portal was no longer supported after HiveOS 6.1r1 was introduced. Only the first client was assigned an IP address and other clients did not have network connectivity.
27721 19801	Some broadcast services were not seen consistently or seen only momentarily by Bonjour devices. Bonjour services became visible across subnets for short periods of time (less than one hour) but then stopped advertising.
27356	The mesh AP link connected only as a one-way connection. This occurred multiple random times during a week. Shutting down and restarting the portal interface reestablished the normal mesh link.

Addressed Issues in HiveOS 6.1r2

27208	Websense could not properly filter anonymous traffic, such as that of unauthenticated guest users, because Aerohive devices did not forward default user names.
27140	When a user with a Samsung Galaxy tablet roams among APs enforcing airtime-based load balancing, the user was prompted to re-enter a password.
27038	In TeacherView, an issue could arise with the list of permitted URLS in the Follow Me list when a teacher and students used different types of devices (mobile devices and PCs). The URLS expected by mobile devices and PCs for the same web site could have differed. For instance, when a teacher permitted the Wikipedia website using a mobile device, the URL was m.wikipedia.org. However, the URL for the same website on a PC was www.wikipedia.org. As a result, a student using a PC was not able to access Wikipedia, even when it was included in the Follow Me list.
26979	When a LAN port on a BR200-WP received a tagged VLAN 1 packet, it treated the packet as an untagged packet and instead matched the packet to the native VLAN configured on that port.
26921	In TeacherView, there was an issue with Internet Explorer not displaying the entire *TeacherView Class* web page.
26844	When using 802.1x or Private PSK authentication with the Websense service, some Aerohive devices did not forward user credentials correctly, which resulted in reports that did not account for users whose credentials were omitted.
26626	When Bonjour Gateway is enabled, there was an issue with client TCP traffic (sent using Telnet, HTTP, HTTPS, SSH, or Web UI) not reaching an AP when the client and AP were assigned to different VLANs.
25703	RADIUS proxy and ID Manager proxy could not function on an AP at the same time. If ID Manager was enabled on an AP that was already acting as the RADIUS proxy, authentications were automatically sent to ID Manager instead.
25698	There was an issue with HiveManager losing track of user names when reporting application data from the Applications perspective on the Dashboard. This issue has been addressed in 6.1r2.
25055	Band steering with the safety net enabled did not distribute clients between the 2.4 GHz and 5 GHz radio bands as expected.
25054	Although iOS devices were able to detect iTunes Home Sharing services that were shared by Bonjour Gateways in different VLANs, the devices were unable to connect to their iTunes libraries because the Bonjour Gateways did not share service subtypes.
23985	Mesh points sometimes lost their wireless backhaul link to their portals as a result of background scanning for WIPS protection.
22975	The AP330 did not auto negotiate or connect at Gigabit speeds with a Cisco 2950 switch unless 802.3az was disabled.
17970	A BR100 in AP mode could not process 802.1X authentication for a new client connected to a LAN port for five minutes after a previously authenticated client disconnects.
16266	The application of an HTTP ALG on an Aerohive device was incompatible with any Websense solution except the web security feature that you can set on Aerohive routers and disrupted HTTP traffic proxied to a Websense server.
15523	If you defined an SSID with private PSK self-registration and the wireless + routing network policy did not contain a network object using VLAN 1 with a subnetwork that had a DHCP server enabled, the clients of unregistered users were unable to get network settings through DHCP.

Addressed Issue in HiveOS 6.1r1a

27542	SR series: Under certain conditions, ports 25-28 were unable to detect a link.

Addressed Issues in HiveOS 6.1r1

25376	After upgrading an Aerohive device to HiveOS 6.0r2, the device did not apply policy-based routing commands properly.
25358	Application Visibility and Control did not always detect and report Netflix video streams.

P/N 330133-02