# HiveOS 6.1r5b Release Notes

**Release Date**: August 3, 2015

**Release Versions**: HiveOS 6.1r5b

**HiveOS Platforms supported**: AP230

These are the release notes for HiveOS 6.1r5b firmware. This release contains numerous new and enhanced features, summaries of which are described in the following section. Known issues are described in the "Known Issues" on page 2 and "Addressed Issues" on page 3 sections near the end of this document.

# Changes in the HiveOS 6.1r5b Release

The following changes have been made with the HiveOS 6.1r5b release:

## Status LED Behavior

Aerohive access points include LEDs that can be used to assist installation, monitoring, and troubleshooting. Prior to this release, the default behavior of the AP130 and AP230 LED was to be on and illuminated at all times during normal AP operation. The new behavior of the AP130 and AP230 LED is to exhibit a long-period blink: The LED illuminates for 4 seconds, and then remains off for about one minute. There are no other changes to the operation of the access point.

This change is in response to a manufacturing defect reported by some customers that might cause the LEDs on the access point to become increasingly dim over time. This defect is largely cosmetic and does not alter or cause any loss of functionality to the product. That is, regardless of the condition of the LED over time, the performance and connectivity provided by your Aerohive network remains unchanged.

Customers who have reported this issue report a significant visual difference between the brightness of the LEDs on their units after nine to twelve months of continuous operation as compared to when the units were originally installed. This issue only exists in AP130s and AP230s, and, to date, has only been reported by AP230 customers, although not all units have been affected. The change in LED behavior allows the LED to continue to provide a visual indicator of the AP's health for those customers who use this feature, while significantly extending the life expectancy of the LEDs, in many cases to beyond the expected service life of the access point.

## What You Need to Do

Aerohive recommends that you take steps to extend the life of the LEDs on your access points. Even if you do not typically rely on the LEDs for ongoing operations, taking action now will ensure that the LEDs are available to you if you need them in the future. This requires you to install an updated version of HiveOS. See "Updating Your Devices" on page 2 for instructions on how to update your devices.

By updating HiveOS by September 1, 2015, you ensure the continued, full protection of your Aerohive warranty. For further protection, customers who do not typically use the LEDs as part of ongoing operations can turn the LEDs off completely, then turn them on when needed for troubleshooting.

## Updating Your Devices

### *HiveManager Online*

To update your AP230s to HiveOS 6.1r5b, log in to HiveManager Online, and then do the following:

1. Navigate to **Monitor > Devices > Access Points > Aerohive APs**, and the select the AP230s you want to update, and then click **Update > Advanced > Upload and Activate HiveOS Firmware**.
2. Choose the 6.1r5b image from the HiveOS Image drop-down list, and then click **Upload.**

### *HiveManager NG*

To update your AP230s to HiveOS 6.1r5b, log in to HiveManager NG, and then do the following:

1. Navigate to **Monitor > Devices**, select the AP230s you want to update, and then click **Update Devices**.
2. In the Device Update dialog, select **Upgrade HiveOS** and **Upgrade even if the versions are the same**, choose your preferred activation parameter, and then click **Upload**.

### *HiveManager Appliances and Virtual Appliances*

To update your AP230s to HiveOS 6.1r5b, log in to your HiveManager appliance running HiveManager 6.1r5 or later, and then do the following:

1. Navigate to **Monitor > Devices > Access Points > Aerohive APs**, and the select the AP230s you want to update.
2. Click **Update > Advanced > Upload and Activate HiveOS Firmware**.
3. Choose the 6.1r5b image from the HiveOS Image drop-down list, and then click **Upload**.

   If the image you want does not appear in the drop-down list, you can obtain the image from the HiveOS Update server. To do this, click **Add/Remove**, choose **HiveOS latest images from update server**, select the image you want from the list, and then click **Upload**. HiveManager transfers the requested HiveOS image to your local appliance, after which time it is available in the HiveOS Image drop-down list. When the transfer is complete, return to step 2 above.

# Known Issues

The following are known issues at the time of the following Aerohive releases. If a section for known issues of a release does not appear, then there are no known issues for that release.

## Known Issues in HiveOS 6.1r5b

| | |
|---|---|
| 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. |
| | Workaround: 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 reports the interfaces, it displays the incorrect value of -92 dBm for the noise floor. |

| 32101 | When simultaneously passing uplink traffic from two Macbook Pros to the AP230, one connected to the 2.4 GHz radio and the other connected to the 5 GHz radio, the throughput is lower than when passing uplink traffic from only one Macbook Pro that is connected to the 5GHz radio. |
|---|---|
| 31730 | The Layer 2 bridge access throughput of the AP230 is less than 500 Mbps. |
| 31414 | When generating a report, the Transmit Bit Rate Distribution values displayed in HiveManager do not match the values read directly from the AP230. |
| 31206 | When band steering is enabled, the AP230 does not steer the configured ratio of dual-band capable clients to the 5 GHz band. |
| 30446 | Even when an AP230 requires a boost of airtime tokens to meet its minimum targeted throughput level, its SLA status shows it as healthy at 10-minute intervals. |
| 30285 | If you manually clear the Phase1 SA for an IPsec tunnel on an AP230 (`clear vpn ike sa`) and a wireless client disconnects and reconnects to the AP without reauthenticating itself, the AP230 does not rebuild the GRE tunnel to the VPN server. As a result, the client cannot reach any destination requiring its traffic to pass through the tunnel. |
| 30212 | When a wireless device is about to go to sleep, it sends a message to the AP230. Then the AP230 responds that it has buffered data to send to the device even when the AP does not have any data. This occurs on both the wifi0 and wifi1 interfaces. |

# Addressed Issues

The following issues were addressed in the HiveOS and HiveManager 6.1 releases, ID Manager, and Client Management releases. If a section for addressed issues of a release does not appear, then there were no issues addressed for that release.

## 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. |