



Aerohive Release Notes

Release: HiveOS 6.1r3b

Platforms: All AP and BR series devices (except the AP370 and AP390)

Release Date: March 28, 2014

These are the release notes for HiveOS 6.1r3b. This release contains two addressed issues described in the ["Addressed Issues" on page 6](#) section near the end of this document.

Upgrading HiveManager and HiveOS

Aerohive supports upgrading to 6.1r3 HiveManager software and 6.1r3b HiveOS firmware from HiveManager 5.1r3 and HiveOS 5.1r3 releases or later. If your systems are running images earlier than 5.1r3, follow the steps in the 5.1r3 Aerohive release notes to upgrade HiveManager software and HiveOS firmware to 5.1r3 first before upgrading them to 6.1r3 and 6.1r3b.

Memory Increase Required before Upgrading to HiveManager 6.0 or Later

Before upgrading HiveManager software on existing 32-bit HiveManager physical appliances and HiveManager Virtual Appliances to 6.0r1 or later, you must first increase their memory to 3 gigabytes. For 64-bit HiveManager Virtual Appliances, you must increase the memory to 8 gigabytes. For instructions about increasing the memory for a physical HiveManager appliance, see the instructions in [Memory Upgrade for 1U HiveManager Appliances](#). For instructions about increasing the memory for a HiveManager Virtual Appliance, see ["Increasing Memory, CPU, and VM Param Settings for the HiveManager Virtual Appliance" on page 3](#).

Step 1: Upgrade 5.1r3 or later to 6.1r3 and 6.1r3b

When upgrading HiveManager to 6.1r3 and HiveOS to 6.1r3b, upgrade HiveManager first and then the devices second. Use the following procedure to upgrade a HiveManager standalone or HA pair.

From	Action	To
HiveManager 5.1r3 or later	Upgrade to HiveManager 6.1r3.	HiveManager 6.1r3
HiveOS 5.1r3 or later	Use HiveManager running HiveManager 6.1r3 to upgrade managed devices to HiveOS 6.1r3b.	HiveOS 6.1r3b

Upgrading the HiveManager Appliance and Aerohive Devices

1	Back up your database as a safety precaution (Home > Administration > HiveManager Operations > Back Up Database).
2	Save the following files to a directory on your management system: (Log in and download these files from the Aerohive Support page.) <ul style="list-style-type: none"> • 6.1r3 HiveManager software file • 6.1r3b HiveOS firmware files for all the managed device platforms being updated
3	Log in to HiveManager running 5.1r3 or later and upload the 6.1r3b HiveOS files for all the types of Aerohive devices that you are managing to HiveManager. Click Monitor > Devices > All Devices > Update > Advanced > Upload and Activate HiveOS Software > Add/Remove . In the <i>Add/Remove HiveOS Image</i> dialog box that appears, select Local File , click Browse , navigate to one of the HiveOS image files you saved to your local management system in the previous step, select it, click Open , and then click Upload . Repeat this to upload a HiveOS image file for each type of Aerohive device that you want to update.
4	To update HiveManager, click Home > HiveManager Operations > Update Software , select the method to upload the 6.1r3 HiveManager software, and then click OK . When the upload is complete, HiveManager automatically reboots to activate its new software.
5	To update the HiveOS image on the managed devices, log back in to HiveManager and navigate back to Monitor > Devices > All Devices . Click the device or devices of the same type for which you want to update the HiveOS firmware, click Update > Advanced > Upload and Activate HiveOS Software , select the appropriate file from the HiveOS Image drop-down list, and then click Upload .

Step 2: Reload the HiveOS Configurations

1. Check that the firmware upgrade is complete (see Configuration > Devices > Device Update Results).
2. Upload the full configurations from HiveManager to the devices, and then reboot them to activate the 6.1r3-compatible configurations.

(i) *HiveManager running HiveManager 6.1r3 can support Aerohive devices running HiveOS 5.1r3-6.1r3b. Based on the HiveOS version that each device is running, HiveManager generates different configurations. Therefore, it is necessary to activate the HiveOS 6.1r3b firmware on managed devices before updating their configurations so that the updated configurations use the new 6.1r3 format.*

Increasing Memory, CPU, and VM Param Settings for the HiveManager Virtual Appliance

Before you can upgrade a 32-bit HiveManager Virtual Appliance to 6.0 or later, you must increase the memory for it within the ESXi hypervisor to 3 gigabytes, set the number of virtual sockets for its CPU to 2, and change VM params to 1024 megabytes.

ⓘ Upgrading the 64-bit HiveManager Virtual Appliance to 6.0 or later does not require any changes to its default memory (4 GB), CPU (4 virtual sockets), and VM param settings (1480 MB). A new 6.1r1 installation of a 64-bit HiveManager Virtual Appliance .ova file has a new default memory size of 8 GB.

1. From the vSphere Client on your management system, log in to the ESXi hypervisor hosting the HiveManager Virtual Appliance whose memory you want to increase.
2. To check which type of system you have, select the name of the HiveManager Virtual Appliance, click **Summary**, and check whether the Guest OS indicates that it is 32 or 64 bits.

ⓘ You can also check the system type in the HiveManager GUI. In the HiveManager 5.0 and 5.1 releases, click **Home > Dashboard**, and view the model number in the HiveManager System Information widget. The VM 1U model is 32 bits, and the VM 2U model is 64.



32-bit HiveManager Virtual Appliance



64-bit HiveManager Virtual Appliance

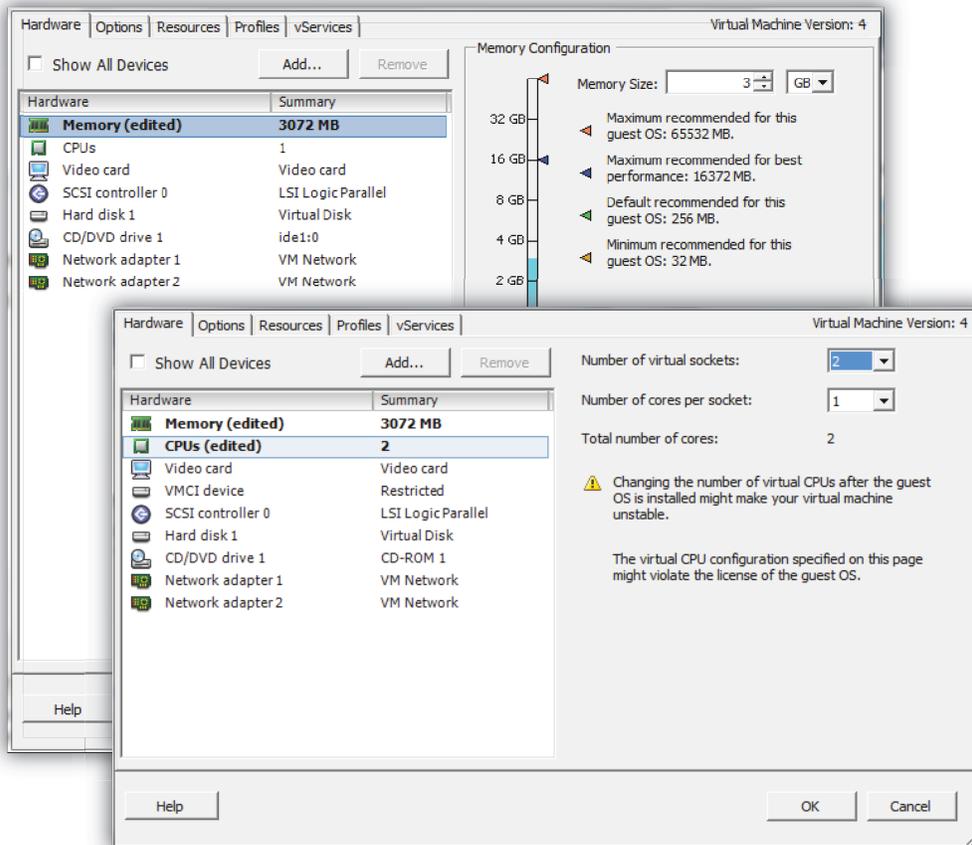
3. If it is a 32-bit system, keep the name of the HiveManager Virtual Appliance selected, click the **Console** tab, click in the console window, and then log in to the HiveManager CLI shell. If it is a 64-bit system and is still using the default settings, you are not required to change them. However, if you want to, you can increase the memory from 4 GB to 8 GB by performing the following steps.

```

1) Network Settings and Tools
2) Display System Information
3) Advanced Product Configuration
4) Reboot Appliance
5) Shut down the System
6) Change CLI Shell Password
7) Logout of shell
Please make a choice:

```

4. To shut down the virtual appliance, enter **5** (Shut down the system) and then enter **Y** when prompted to confirm the action.
5. In the vSphere Client GUI, right-click the HiveManager Virtual Appliance name in the left navigation panel, and then click **Edit Settings**.
6. On the **Hardware** tab, click **Memory**, change the value in the Memory Size field to **3 GB** for a 32-bit system or up to **8 GB** for a 64-bit system, and then click **OK**. (For a 64-bit system using its default values, there is no need to change any other settings.)
7. For a 32-bit system, select **CPUs**, from the Number of virtual sockets drop-down list, choose **2**, and then click **OK**.



8. With the name of the HiveManager Virtual Appliance still selected, click **Power on the virtual machine**.
9. After the HiveManager Virtual Appliance is powered back on, click the **Console** tab, click in the console window, and log in to the HiveManager CLI shell.
10. Enter **3 - 2 - 2** to navigate to Advanced Product Configuration > Configure VM Params > Change VM Params, and then enter **1024** (for 1 GB).
11. Reboot the HiveManager Virtual Appliance to apply this setting. (You can navigate back to the home menu, and enter **4** for Reboot Appliance.)
12. After the HiveManager Virtual Appliance finishes rebooting, check that it recognizes its increased memory size by returning to the console window, logging back in to the HiveManager CLI shell, and entering **2 - 4** (Display System Information > Display Hardware Information). To complete the memory upgrade procedure, check that the MemTotal value for a 32-bit system is approximately 3,000,000 KB. (The MemTotal value for a 64-bit system is approximately 8,000,000 KB.)

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 6.1r3b

30343	When WIPS (wireless intrusion prevention system) is not enabled, all channels are rapidly scanned in the spectrum analysis scan cycle. However, when WIPS is enabled, there is a delay in the scanning time of some channels and other channels are not scanned at all during the scan cycle.
30200	<p>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.</p> <p>WA (work around): 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.</p>
29880	<p>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.</p> <p>WA: For AP121 and AP141 devices, set rogue mitigation in manual mode and disable client reporting.</p>
29826	<p>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.</p> <p>WA: Use manual rogue mitigation.</p>
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.
25193	After an AP320 or AP340 reboots, it can occasionally take 3-5 minutes to begin providing wireless services.
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.
14603	<p>If you enable OSPF route advertisements on both the eth0 and eth1 interfaces of the CVG, traffic from hosts in the corporate site might be routed through the CVG to the public network instead of taking a different path.</p> <p>WA: Only advertise routes on one interface, either eth0 or eth1.</p>

Known Issues in HiveManager 6.1r3

28720	The Aerohive Application Visibility and Control Feature might only be able to recognize the "Facebook" and "Facebook Messages" applications in the applications watchlist due to a recent change by Facebook, Inc which makes HTTPS the default connection protocol. The other six Facebook applications, "Facebook Apps", "Facebook Event", "Facebook Post", "Facebook Search", "Facebook Video", and "Facebook Video Chat", might be recognized if the Facebook user connects to Facebook using HTTP instead of HTTPS, which is the new default secure connection protocol. These applications are available from the Reports > Report Settings page, from the System Defined Applications tab in the section.
27123	In ID Manager, the email and phone fields on the <i>Self Registration</i> page accept special characters that are not related to email or phone numbers, and then return illegible data because of these characters. WA: Make sure to enter only the characters that are valid for email and phone numbers.
20947	In Bonjour Gateway, you cannot set a static VLAN when you create a wireless network policy. WA: Configure a device as a DHCP server instead of configuring a static VLAN.
15162	Although Wi-Fi statistical reports show data at one-minute intervals accurately, they do not normalize the data for ten-minute intervals, which causes the data to appear exaggerated in the charts.

Addressed Issues

The following issues were addressed in the HiveOS and HiveManager 6.1 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 6.1r3b

CFD-227	Disabling transmission at one or more of the default basic data rates caused Aerohive devices to 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 6.1r3

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 will be prompted to re-enter a password. WA: Disable load balancing.
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.

Addressed Issues in HiveManager 6.1r3

30196	In the <i>Admin Account Manager</i> dialog box, the User Manager Administrators or Operators options did not appear in the Group Name drop-down list.
30101	The database was losing the device template classification settings.
30100	Device template classification settings disappeared from a cloned network policy.
29965	The list of network policies appeared in the order they were created and did not appear in alphabetical order in the Create New Filter menu.
29765	Some APs could not be updated over the CAPWAP connection after an upgrade was performed from version 6.1r1 to 6.1r2a.

29664	When creating a new Bonjour Gateway within a network policy, the table for configuring Bonjour services was missing. The window became unresponsive and the Save and Cancel buttons became unusable. You had to reload the page to continue.
29544	When attempting to log in to TeacherView using HiveManager Online, a CAS (central authentication service) authentication error appeared.
29444	The Location field of the BR series devices was correctly disabled (because they do not support certain SNMP features), but it retained legacy text content, which caused confusion as to the status of SNMP support in Aerohive BR series routers.
29142	HiveManager would sometimes set the VLAN of a wireless-only network policy to be a VLAN other than the VLAN configured.
29101	In HiveManager 6.1r2, the data in the Client Device SLA Compliance over Time and Aerohive Device SLA Compliance over Time widgets in the dashboard erroneously indicated alarm conditions.
29074	HiveManager sometimes unnecessarily performed a complete configuration update, which requires a device reboot, instead of performing a delta configuration update, which does not.
29063	After being upgraded to 6.1r1 or 6.1r2, HiveManager did not display multiple VLAN ID object definitions (distinguished by topology node, device name, and device tag classifier).
29062	An alarm stating that the default DTLS passphrase was in use frequently appeared after uploading configurations to devices and rebooting them.
28996	If a network policy included a captive web portal using self-registration or both (auth/self-reg) and did not reference a management options profile, uploading the configuration to devices caused an error because the devices were unable to check if reports about captive web portal clients was enabled.
28953	HiveManager permitted the inclusion of an SSID and a port type with the same name in the same network policy, which caused configuration uploads to devices with both Wi-Fi and Ethernet interfaces to fail.
28938	HiveManager Online: Erasing the database caused the Device Inventory button and <i>Unmanaged Devices</i> tab to disappear, making it impossible to synchronize the inventory list in the VHM with that in the redirector.
28904	After authentication using Private PSKs, some users were being placed into VLAN 1 and the incorrect user profile was being applied.
28856	When a .csv file of IP objects with a global value was imported into HiveManager, all tags were marked as having a value even though the tags were empty.
28836	When the USB port was configured as backup WAN interface on a BR100, there was no CLI available to configure its WAN priority.
28834	When the Chrome browser was used to view the HiveManager Dashboard data and memory usage was high, the <i>Application Usage over Time</i> widget did not display any data. Note: <i>This issue appeared when an earlier version of the Chrome browser was used to view the dashboard. It does not appear if you use the latest version of the Chrome browser.</i>
28817	When a device configuration was successfully updated to 6.1r2, and the device image was rolled back to a previous version, a warning message appeared in the Update Result column of the <i>Device Update Results</i> page.

28790	After the HiveManager Online administrator logged in to a VHM (virtual HiveManager) and added or removed a device using the <i>Device Inventory</i> drop-down menu (Monitor > All Devices), the login session expired due to inactivity, and you logged in again to add or remove another device, the <i>Device Inventory</i> drop-down menu no longer appeared.
28770	When the LED brightness was changed from Bright to Soft, an error was generated during a delta configuration upload, and the upload failed.
28736	If the number of characters in the URL of the mobile device management and captive web portal was greater than 32 characters, the configuration upload failed.
28715	When cloning a network policy that contains device templates, the device templates were deleted from both the original and cloned network policy if the cloned policy was not saved properly.
28541	During the auto provisioning process as the BR100 function was changed from a router to an AP, the same static IP address was used for the new AP, which did not match the IP network and would cause it to lose its connection to HiveManager.
28407	The colors shown in the topology maps were not indicating the correct alarm severity of APs, most of which were AP mesh points.
27140	The Samsung Tab 2 GT-P3100 device had connectivity issues during AP high-density load balancing.
25962	In the <i>Applications</i> perspective on the Dashboard, the "All Applications by Usage" widget displayed "failed to request date" for the first twenty-four hours after the initial installation or upgrade of HiveManager. The first roll up of information to this widget occurred twenty-four hours after installation. This issue does not occur when upgrading from HiveManager 6.1r1 to later versions.
25410	After disabling client learning on an SR2024 Ethernet port, HiveManager continued to display previously learned MAC addresses instead of removing them from the client list for that port.
24332	In the <i>Monitor</i> section, you could not distinguish between ports that were available (but not configured) and ports that were shut down because both port states were shown in red.
22897	A device configured as a Bonjour Gateway did not retain any realm name previously defined for it after a reboot.
21815	When zooming in to a topology map containing clients, the clients would disappear because the Show Clients check box became cleared.
15225	For a VHM on a physical HiveManager appliance or HiveManager Virtual Appliance, it was not possible to auto provision devices by specifying their subnetworks. Note: <i>This is not a valid issue. Auto provisioning using an IP subnet was only intended for VHMs with non-overlapping IP subnets. You must not use this feature if there are overlapping subnetworks.</i>

Addressed Issues in HiveManager 6.1r2a

29074	Sometimes devices unnecessarily rebooted after a simple incremental configuration update was performed.
29062	Aerohive devices displayed the "Default DTLS passphrase is in use" alarm message without any changes or configuration pushes being initiated to these devices.

Addressed Issues in HiveManager 6.1r2

28891	HiveManager Online: It was not possible to upload a delta or complete configuration if the VHM name contained "view" in it.
28541	When the BR100 configuration was changed from a router to an AP during the auto provisioning process, the same static IP address that was used for the new AP did not match the IP network. This caused the AP to lose connection with HiveManager and, after 15 minutes, the configuration was rolled back to that of a router.
27483	A user assigned to only have access to the Redirector could not access the Redirector or HiveManager.
27249	When the HiveManager web-based SSH client was used to establish an SSH session with an Aerohive device, the connection attempt failed and an error message appeared.
26922	In HiveManager Express Mode with ID Manager enabled, there was an issue with creating and adding a Captive Web Portal Use Policy Acceptance to an SSID. This setting could be changed in the GUI, but it was not saved.
26738	If the HiveManager database was too large (over 1G, for example), performance was degraded, and the AP locked and required a reboot. This fix added the maximum size limitations for performance data and client history in the HiveManager database.
26737	When users authenticated to a network through a captive web portals using Use Policy Acceptance, the use policy text did not appear in the use policy area.
25698	User names associated with wireless clients that APs reported correctly to HiveManager were changed to "unknown" when the switch to which the APs connected sent client update events.
25272, 24281	In the <i>System Details</i> section of the Monitor > Devices > Routers > <i>router_name</i> page, HiveManager displayed the external WAN IP address that an upstream NAT device applied to an SR2024 instead of the IP address of the WAN interface itself.
25407	Wi-Fi client mode (Wi-Fi as a WAN interface) was not supported in HiveManager auto provisioning.
24768	AP330 and AP350: Performing off-channel rogue mitigation sometimes caused the AP to become unresponsive.
24309	An HTTP Status 500 error appeared on the primary HiveManager Virtual Appliance running in high-availability mode, and the primary HiveManager needed to be restarted using an SSH connection to recover.
24294	You were not able to create a new TeacherView account in HiveManager when you also had an ID Manager account. In the <i>TeacherView > Classes > New</i> page, clicking the New (+) icon launches the <i>New Teacher Account</i> dialog box. With the implementation of centralized user management through MyHive, the <i>New Teacher Account</i> dialog box did not appear in VHMs that were linked to ID Manager.
23205	HiveManager was unable to manage APs using UDP, and uploading configurations failed because there is an SSH key mismatch between HiveManager and the APs.
23008	Under certain conditions, there were delays when generating a PDF report from the Maps GUI section.
19295	When a client whose OS type was determined through DHCP snooping to be "unknown" roams to another AP, HiveManager changed the OS type it displayed from "unknown" to blank because APs did not include DHCP option 55 information in their roaming cache updates.
19081	You could not import a list of client OS types into one VHM if it contained an OS type that already existed in another VHM.

18618	HiveManager allowed you to upload a network policy that had the Bonjour Gateway feature enabled to a BR100 although that platform did not support Bonjour Gateway functionality.
18067	A HiveManager operating in Express mode could not manage a CVG functioning as a Layer 2 VPN gateway and erroneously displayed any CVG that had formed a CAPWAP connection with it as an AP110.

Addressed Issues in HiveManager 6.1r1

25784	When you upgraded HiveManager from 5.1 to 6.0r2 or later, upgraded the managed devices, and then uploaded a complete configuration to the devices, reported data might not have appeared in the widgets in the Network Summary and Troubleshooting perspectives. However, the data was displayed in the System Summary perspective.
25701	When attempting to perform an LDAP lookup from the HiveManager GUI against an Aerohive RADIUS server joined to Active Directory, the request kept processing and never completed.
25368	When a VHM admin created an application watchlist and then an admin with super user privileges logged in to that VHM from the home system, the admin with super user privileges could not see the previously added applications in the watchlist.
25351	When upgrading the software from 5.1r5 to 6.0r2 or later, a network policy did not reference any policy-based routing profile that was a part of the policy before the upgrade. This issue has been addressed.
24942	In the "Channel Usage over Time" and "Errors over Time" graphs that appear on drill-down pages in the dashboard, HiveManager displayed the 2.4 GHz and 5 GHz data averaged together instead of separately. In the "Airtime Usage over Time" graphs, HiveManager displayed the 2.4 GHz and 5 GHz data combined together instead of separately.

2014 Aerohive Networks, Inc.

Aerohive is a U.S. registered trademark of Aerohive Networks, Inc.

P/N 330104-03b, Rev. A