HiveManager 6.4r2 Release Notes

Release Date: February 14, 2015

Release Versions: HiveManager 6.4r2

Platforms supported: AP121, AP141, AP330, AP350, BR200-WP

These are the release notes for HiveManager 6.4r2 firmware. Known issues are described in "Known Issues" on page 6 and "Addressed Issues" on page 6.

((¡)) *Although HiveOS 3.4r4 was the last release for the HiveAP 20 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 6.1, 6.2, 6.3 and 6.4.*

New Features and Enhancements in the 6.4 Releases

The following are the new features and feature enhancements in the HiveOS and HiveManager 6.0 releases.

New and Enhanced HiveManager 6.4r2 Features

HivePass: Aerohive, in partnership with Passforce, now offers the HivePass feature. HivePass is an easy-to-implement loyalty program that retail customers can use to attract and retain customers. HivePass removes the burden of costly custom retail applications, and thereby minimizes the risks associate with their implementation. HivePass uses the Passbook application, which is pre-installed on modern iOS devices, and numerous free apps that are available for Android devices. You can deliver HivePass passes directly to devices that attach to your wireless network.

New and Enhanced HiveOS 6.4r1 Features

The following new features and feature enhancements have been added in the HiveOS 6.4r1 release:

AP230 Location Services: AP230 devices can now discover the received signal strength (RSSI) values of client transmissions and report these values to HiveManager, which uses them to calculate the probable location of the client, and display an icon for the client on a map. For a complete description of location services, see the HiveManager Online Help.

AP230 Protected Management Frames: AP230 devices now support the use of protected management frames (PMF) established with 802.11w, which prevents the malicious use of spoofed management frames to disrupt the operation of the wireless network.

AP230 Spectrum Analysis: AP230 devices now support spectrum analysis. This feature extracts RF interference information and classifies the cause based on spectrum signatures on both the 2.4 GHz and 5 GHz bands. For a complete description of spectrum analysis, see the HiveManager Online Help.

Asynchronous RADIUS Accounting Update: A RADIUS accounting update interval is a repeating, 20 second period of time during which APs report DHCP-snooped IP addresses of associated clients to the RADIUS server, so they can be recorded and be properly authorized for network access. This enhancement removes the requirement that the AP waits until the end of the interval to update the RADIUS server. The AP now provides updated IP addresses of clients to an external RADIUS server immediately as soon as this information is obtained.

MAC address bypass for captive web portal: The MAC address bypass enhancement allows administrators to configure a whitelist containing specific client MAC addresses. When paired with an SSID profile, these clients can bypass the normal captive web portal authentication and interaction process. This allows "headless" or embedded devices, such as ATMs and vending machines, to connect to the WLAN network without admin intervention.

New and Enhanced HiveManager 6.4r1 Features

The following are the new features and feature enhancements in the HiveManager 6.4r1 release.

AP230 as iBeacon: Bluetooth Low Energy (BLE) wireless technology provides many new applications for retail and commercial enterprises. With this release, you can enable an AP230 to behave as an iBeacon transmitter by connecting a Bluetooth dongle to the external USB port interface. iBeacon functions are configured in HiveManager.

FCC DFS support for AP230: AP230 devices now support dynamic frequency selection (DFS), which is required when wireless devices are operating in the same regions as active radar systems. Because radar systems use part of the 5 GHz band, devices must be able to detect the radar activity and select an unoccupied channel automatically.

Delegate remote deployment of Aerohive devices: Aerohive currently supports the HiveManager capability to upload a specific HiveOS image and configuration to all automatically discovered devices as soon as they make an initial CAPWAP connection with HiveManager. This release introduces enhancements to the provisioning process, and eliminates any additional manual input that was previously required by the remote deployment administrator. All device-specific settings are now imported to devices using the CSV import file, the device auto provisioning network policy is automatically created based on the CSV import file, and the device firmware upgrade is performed as defined in the policy.

Unified IP Firewall Policy extended to switches: In this release, the unified IP firewall policy extends to the SR Series switches, covering both inbound and outbound traffic on wireless and wired clients. Previously, the IP firewall policy only supported Aerohive APs.

Hong Kong area support for DFS for the AP230: When operating in the Hong Kong geographic area, AP230 devices now support the use of dynamic frequency selection (DFS) where radar systems are in use. This allows the devices to select a radar-free channel automatically when a radar presence is detected. For a complete description of DFS, see the HiveManager Online Help.

AP230 support for the China country code: AP230 devices now support for the China country code.

AP1130 support for the Korea country code: AP1130 devices now support the Korea country code. Support Enhancements for NAC: This release extends support for Network Access Control (NAC) applications. NAC Change of Authorization (CoA) messages can now redirect bring your own device (BYOD) users to an external captive web portal (in addition to the Aerohive internal web portal) for firs-time credential entry, or remediation, such as anti-virus software installation or other updates required to bring the user device into compliance with the network policy.

Technology Preview: Cooperative-Application Visibility and Control Extended to SR Series Switches: Cooperative-Application Visibility and Control (C-AVC) extends AVC to the SR Series switches, enabling you to monitor traffic patterns on wired and wireless networks. Using C-AVC, Aerohive switches and access points leverage Cooperative Control protocols to analyze application usage data from wired clients, while HiveManager provides monitoring and reporting of Layer 7 application data gathered from both wired and

wireless clients. C-AVC is available on SR2024, SR2024P, SR2124P, and SR2148P switches when a supported AP230, AP330, or AP350 is connected directly to the switch. For more information about C-AVC, including currently supported features, supported configurations, and setup instructions, please see the C-AVC Technology Preview.

Upgrading HiveManager Software

Aerohive supports upgrading to the 6.4r2 HiveOS software from the HiveManager 5.1r2 releases or later. If your system is running an image earlier than 5.1r2, follow the steps in the 5.1r2 Aerohive release notes to upgrade HiveManager to 5.1r2 first before upgrading them to 6.r42.

("i") *To upgrade the AP230 firmware from HiveOS version 6.1r5 to 6.4r1b or later, you must first upgrade from version 6.1r5 to 6.1r6 followed by a second upgrade from 6.1r6 to 6.4r2.*

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 4.

Upgrade HiveManager 5.1r2 or later to 6.4r2

Use the following procedure to up grade a HiveManager standalone or HA pair.

From	Action	To
HiveManager 5.1r2 or later	Upgrade to HiveManager 6.4r2.	HiveManager 6.4r2
HiveOS 5.1r2 or later	Use HiveManager running HiveManager 6.4r1to manually upgrade managed devices to HiveOS 6.4r1	HiveOS 6.r41

Upgrading the HiveManager Appliance
1	Back up your database as a safety precaution (Home > Administration > HiveManager Operations > Back Up Database).
2	Save the 6.4r2 HiveManager software file to a directory on your management system or SCP server. (Log in and download the 6.4r2 HiveManager software file from the Aerohive Support page.)
3	Log in to HiveManager running 5.1r2 or later and then upload the 6.4r2 HiveManager software file. To update HiveManager, click **Home > HiveManager Operations > Update Software**, select the method to upload the HiveManager software, and then click **OK**. When the upload is complete, HiveManager automatically reboots to activate its new software.
4	HiveManager periodically checks for new HiveOS firmware releases that it can download to itself for distribution to managed devices. If HiveManager is connected to the Internet, it automatically obtains HiveOS firmware image files for every type of managed device from the Aerohive update server and makes the image files available in about 15-30 minutes, depending on how many image files it is downloading and its connection speed to the server. To update the HiveOS firmware image files manually, log back in to HiveManager, select the device or devices of the same type for which you want to update the HiveOS firmware, click **Update > Advanced > Upload and Activate HiveOS Firmware**, select the appropriate HiveOS image from the list for the selected device type, and then click **Upload**. If the firmware is not available in the list of HiveOS images, click **Add/Remove** and obtain the HiveOS image you want from the update server, your local directory, or SCP server. If you are managing various Aerohive device types, repeat the upload process for all your managed devices, and then reboot them to activate their new firmware.

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.
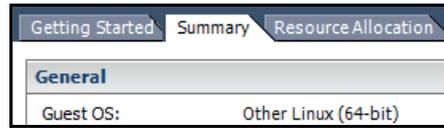
((¡)) Upgrading the 64-bit HiveManager Virtual Appliance to 6.0 or later does not require any changes to its default memory (4 GB), CPU (4 virtual sockets), and VM param settings (1480 MB). A new 6.4r1b installation of a 64-bit HiveManager Virtual Appliance .ova file has a new default memory size of 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.*
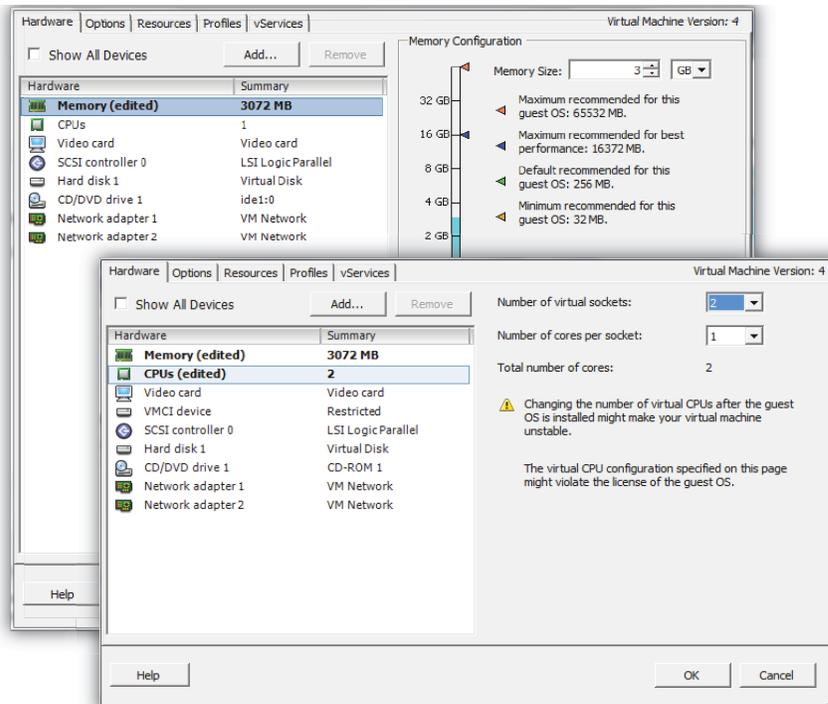
32-bit HiveManager Virtual Appliance

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.

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.)

Documentation

Product documentation is still in progress at the time of these releases and is not yet available. However, the Help for HiveOS CLI commands are ready. To use the CLI Help, enter `keyword-SPACE-?` (for example: **qos ?**). In addition, there are online CLI reference guides that provide the syntax and explanations for every command in the CLI. They also include information on accessing the CLI through console, Telnet, and SSH connections, tips on using the CLI, and some keyboard shortcuts.

Help System for Mobile Devices

Aerohive provides a way for you to view the Help system on a mobile device. The Aerohive Help is designed to be responsive, so in cases where viewing the Help system in a browser is inconvenient or impossible, you can view the Help content on your smart phone or tablet.

Known Issues

The following is a known issue in the HiveManager 6.4r2 release:

Known Issues in HiveManager 6.4r2

35361	In rare instances, when a client device joins the wireless network using HivePass, the captive web portal page continues to display "Downloading Pass", even after the authentication process has completed.
	WA (Workaround): Refresh the current page or navigate to another web page.

Addressed Issues

The following issues were addressed in the HiveOS and HiveManager 6.4r1 releases.

Addressed Issues in HiveOS 6.4r1b

CFD-693	If the transmit power on an AP230 was manually configured below 9 dB and saved, this setting would be lost after a reboot, or when an interface was brought down and then back up. If the AP230 transmit power was configured for 9 dB or higher, or the AP was configured so that ACSP automatically set the transmit power, the setting would remain stable.

Addressed Issues in HiveOS 6.4r1

CFD-666	Show commands were not generating output for AP230 devices, resulting in an inability to troubleshoot connectivity issues.
CFD-723	After upgrading an AP230 from 6.1r6a to 6.2r1, the APs incorrectly broadcast the names of hidden SSIDs.
CFD-701	A switch port configured with "auth fail" and a user profile with device classification did not work for multiple devices.

Addressed Issues in HiveManager 6.4r1

34407	The AP121 was not responding to a command to change the Wi-Fi channel width from 40 MHz Above to 40 MHz Below.
CFD-678	Topology maps were not displayed.
CFD-631	A HiveManager configuration audit showed that configuration changes were synchronized, when they actually were not synchronized.
CFD-736	In WIPS, the Stop Mitigation option for rogue APs was not working correctly. Mitigation could be started but not stopped.
CFD-520	When images containing special characters were uploaded to topology maps, the image would not appear on the topology map, and could not be deleted.