

HiveManager 6.6r3 Release Notes

Release Date: November 21, 2015

Release Versions: HiveManager 6.6r3

Platforms supported: AP110/120, AP121/141, AP130, AP230, AP330/350, AP370/AP390, AP1130, BR100, BR200, BR200-WP, BR200-LTE-VZ, SR2024P, SR2124P, SR2048P, VPN Gateway Virtual Appliance

These are the release notes for HiveManager 6.6r3 software. Known issues are described in ["Known Issues"](#) on page 4 and ["Addressed Issues"](#) on page 5.

Current Features Extended to Devices

The following existing features have been extended to the respective devices.

Existing Supported Feature	Introduced	Extended to Devices
KDDR	HiveManager 6.1r2	AP110
Stateless Bonjour Gateway	HiveManager 6.4r1	AP320 and AP340
Sensor Mode	HiveManager 6.4r1	AP320 and AP340
iBeacon	HiveManager 6.6r1	AP141
Self-registration using PPSK or 802.1X	ID Manager	AP370 and AP390
Client Management	ID Manager	AP370 and AP390
Social Login	ID Manager	AP370 and AP390

Features and Enhancements

This release adds the following new features to all supported platforms.

Dual Image Support on AP121 and AP141: Access points can store two HiveOS images so that you can choose one of the other to be the boot image. In this release, HiveManager extends this capability to the AP121 and AP141.

DHCP Vendor Class Option 43: 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.

Bypass Apple Devices: In this release, HiveManager allows you to control under what conditions an Apple CNA (Captive Network Assistant) generates a popup mini-browser for the user to log in. Because limitations in the CNA mini-browser as a login interface can create issues with implementation that use captive web portals, allowing some captive web portals to bypass the CNA facilitates the login process.

Changes in Behavior and Appearance

The following changes to behavior and appearance have been introduced in the 6.6r1 releases:

- HiveManager and Aerohive HiveOS devices now default to the use of AES-128 encryption.
- The maximum length of a PPPoE user name has been increased to 64 characters.
- Accounting Interim Interval is now set to 600 seconds. You can find this setting in *AAA Client Settings* page of a new or existing AAA client.
- This release resolves the Logjam vulnerability, an exploit of which can result in the negotiation of cryptographically weak keys and subsequent loss of data integrity.

Upgrading HiveManager Software

Aerohive supports upgrading to the 6.6r3 HiveManager software from 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 before upgrading your system to 6.6r3.

Upgrade HiveManager 5.1r2 or later to 6.6r3

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

From	Action	To
HiveManager 5.1r2 or later	Upgrade to HiveManager 6.6r3.	HiveManager 6.6r3

Upgrading the HiveManager Appliance

1	Back up your database as a safety precaution. Navigate to Home > Administration > HiveManager Operations > Back Up Database .
2	Save the 6.6r3 HiveManager software file to a directory on your management system or SCP server. (Log in and download the 6.6r3 HiveManager software file from the Aerohive Support page.)
3	Log in to HiveManager running 5.1r2 or later and then upload the 6.6r3 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 HiveManager 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

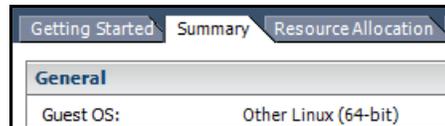
Before you can upgrade a 32-bit HiveManager Virtual Appliance to 6.0 or later, you must increase the memory for it within the ESXi hypervisor to 3 gigabytes, set the number of virtual sockets for its CPU to 2, and change VM params to 1024 megabytes.

“” 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 6.6r3 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.



32-bit HiveManager Virtual Appliance



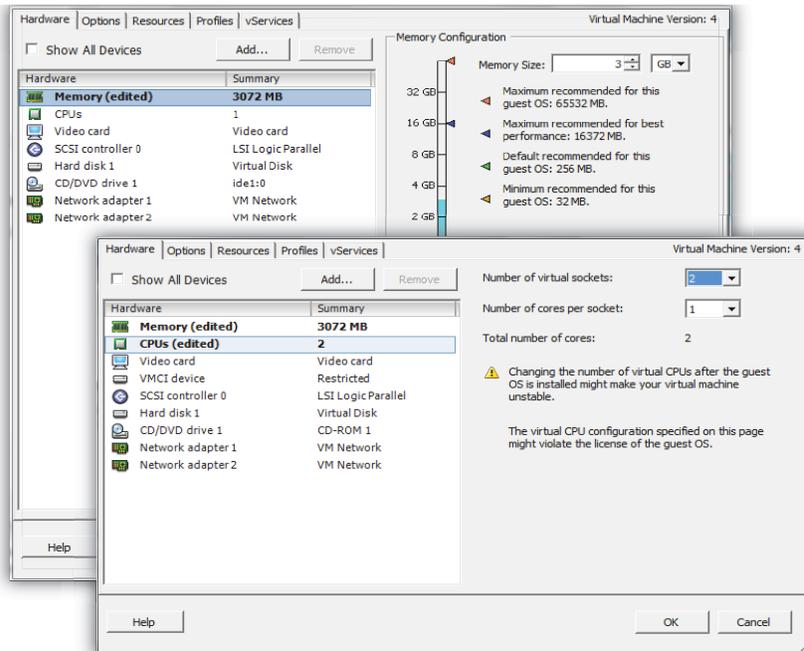
64-bit HiveManager Virtual Appliance

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, select **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 in the HiveManager 6.6r3 releases.

Known Issues in HiveManager 6.6r3

CFD-1128	HiveManager sometimes calculates the number of selected devices incorrectly when a filter is used and there are more devices selected than the page can display.
----------	--

Addressed Issues

The following issues were addressed in the current and previous HiveManager releases.

Addressed Issues in HiveManager 6.6r3

CFD-1133	In the Additional Settings > Traffic Filter Settings section of the network policy, the Enable inter-station Traffic check box applied to wired interfaces only and does not affect wireless interface behavior.
HMGR-790	HiveManager on premise expected a slightly different format when you exported a .csv file and then imported it. In the exported .csv file, the Access Mode, Auto Channel, Country Code, and Wifi0 Admin State rows had text values only. However, HiveManager expected the values for these rows to be a number in the imported file. For example, the Wifi0 Admin State row contained "Up" or "Down" in the exported file. The imported file required "0" or "1" to replace "Up" and "Down" where Up = 0 and Down = 1.

Addressed Issues in HiveManager 6.6r1

CFD-1171	The description of HivePass on the Reports > HivePass page was incorrect.
CFD-1152	The Tunisia/North Africa timezone setting was adjusted for DST (Daylight Savings Time). However, Tunisia no longer observes DST. This issue has been addressed.
CFD-1148	When virtual HiveManager (VHM) systems with registered HivePass configurations were moved to new servers, the HivePass configurations did not transfer properly. As a result, HivePass configurations did not show up in the HiveManager interface and could not be re-registered because HiveManager was still reporting it as registered.
CFD-1116	The time that a device was disconnected from HiveManager, as reported in the table of managed devices, was not consistent with time zone configuration in HiveManager.
CFD-1103	When configuring an AP230 in HiveManager, administrators could not choose channels 120, 124, or 128 when DFS (Dynamic Frequency Selection) was enabled.
CFD-1064	Topology maps that were populated with any planned devices were slow to render.
CFD-1058	Rogue clients were reported on the wireless network even if the APs were configured to not report them.
CFD-1048	It was not possible to enable the OpenDNS Server Settings if it was not previously enabled. This issue has been corrected.
CFD-1028	When HA (High Availability) mode was enabled (Home > Administration > HA Monitoring) and a HiveManager super user created a map for a VHM system, the map was displayed in the root topology tree, but not in the VHM system.
CFD-1011	Captive web portals did not save changes that were made to self-registration user accounts created in ID Manager. This issue has been addressed.
CFD-995	It was not possible to create, edit, or view IP firewall policies after upgrading to HiveManager 6.4r1 due to an invalid apostrophe character in an IP object name. This issue has been corrected.
CFD-965	When navigating to Monitor > Clients > Wireless Clients using Firefox, the navigation menu sometimes incorrectly indicated the current page as <i>Alarms</i> instead of <i>Wireless Clients</i> although the page displayed the correct contents.

CFD-951	HiveManager was unable to display channels, stations, or RSSI heat maps from topology maps.
CFD-872	Client devices connected to an AP230 were able to associate and to obtain an IP address, but were sometimes unable to pass traffic.
CFD-871	The number of distinct channels displayed on a topology map exceeded 12, some APs appeared gray, and their channel numbers were not displayed.
CFD-861	HiveManager was not saving changes in the radio profile backhaul failover settings unless the radio profile was removed from the AP configuration first.
CFD-716	When user profile redirection was in use and a client classification was enabled on the re-assigned user profile, HiveManager did not generate service commands properly, and was unable to push configurations to devices.
CFD-170	When using a network policy that included wireless, switching, and routing features, making a change in the network policy resulted in the audit flag indicating that the device configuration required updating, even when the device did not support the feature, and the policy change did not affect the device.

2015 ©Aerohive Networks, Inc.
Aerohive is a U.S. registered trademark of Aerohive Networks, Inc.