HiveOS and HiveManager 6.6r1 Release Notes

Release Date: July 6, 2015

Release Versions: HiveOS 6.6r1 and HiveManager 6.6r1

Platforms supported: AP130, AP230, AP330, AP350, AP1130, BR200, BR200-WP, BR200-LTE-VZ, VPN Gateway Appliance, VPN Gateway Virtual Appliance, SR2024, SR2024P, SR2124P, SR2148P

HiveManager platforms supported: HiveManager Online and on premise HiveManager

These are the release notes for HiveOS firmware and HiveManager 6.6r1 software. Known issues are described in "Known Issues" on page 6 and "Addressed Issues" on page 7.

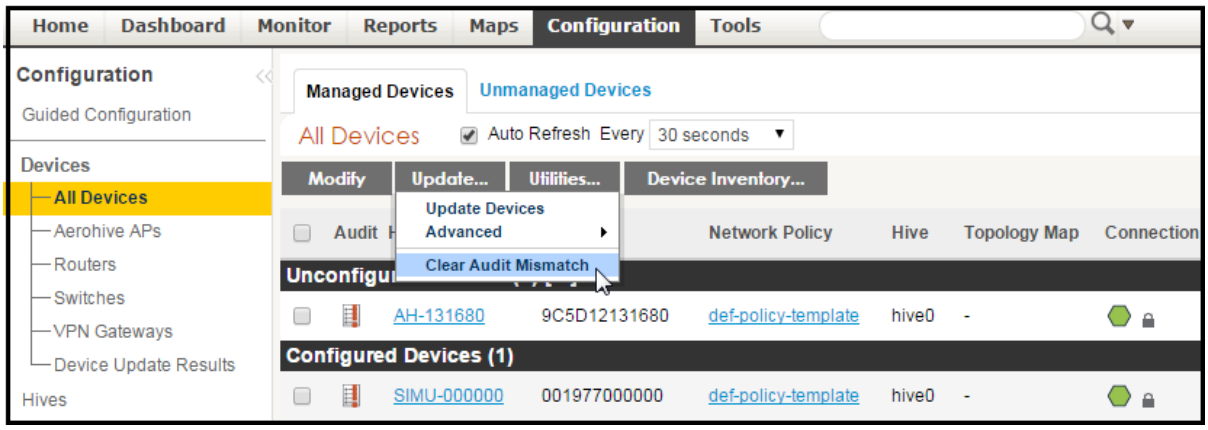
Although HiveOS 3.4r4 was the last release for the HiveAP20 series, the current HiveManager can continue to manage all Aerohive platforms. However, you must push full configuration updates to these devices because some commands have been removed, which would cause delta configuration updates to fail. 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, 6.4 and 6.6.

Changes in Behavior and Appearance

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

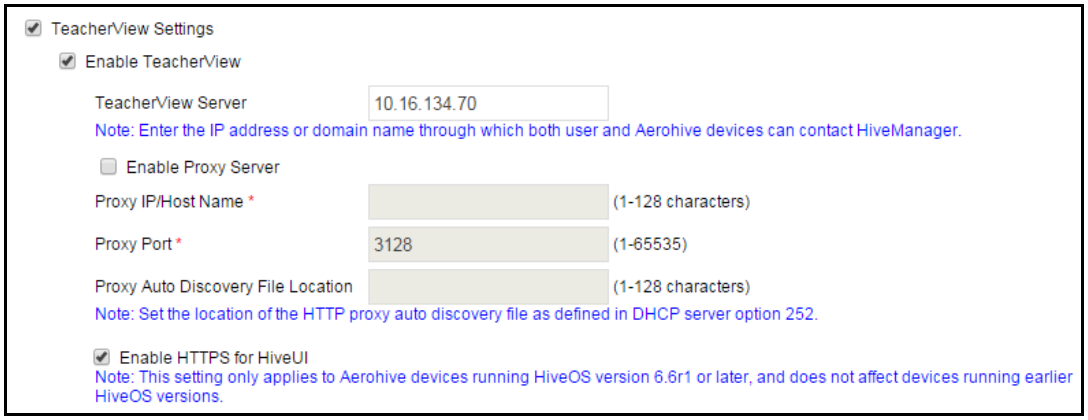
- To close the HiveManager notification bar (that appears at the top of the HiveManager GUI), select **X** to prevent it from displaying during the remainder of your session. For subsequent sessions, the notification bar only appears if one of the following error conditions is met: need to log into an active unit of a high availability pair, need to enter a valid license key, made changes to your policy configuration and need to upload it, performed internal maintenance on Application Visibility and Control and feature has been disabled temporarily, or need to clear critical alarms. Several standard messages that appeared in the Notification bar are no longer displayed.
- When different components associated with an SSID reference several user profiles, you can specify which one you want to apply to the user traffic. If you are upgrading to HiveManager 6.6r1 with the SSID Access Security set to open authentication and expect a user profile ID from MAC authentication, then you need to set the User Profile Application Sequence to "SSID-MAC Authentication- Captive Web Portal". To select this option, navigate to **Configuration > SSIDs > New**. In the *SSID Access Security* section, select **Open** as the authentication option and then select **Enable MAC authentication**. In the *Optional Settings* section, expand **Advanced**. Then open the User Profile Application Sequence drop-down menu, and choose SSID - MAC Authentication - Captive Web Portal. Then click **Save**.
- In the *SSID Access Security* section of the *SSIDs > New* page, select the **Open** and **Enable MAC authentication** check boxes.
- For many cable and DSL Internet connections, ISPs require customers to authenticate using PPPoE by entering a user name and password that the ISP provides. In HiveManager, you can create a PPPoE Authentication object and assign it to your router so that the router automatically connects to the Internet using the credentials required by the ISP. This release supports a PPPoE user name of up to 64 characters and spaces instead of being limited to 32 characters in previous releases. To display the PPPoE dialog box, navigate to **Configuration > ShowNAV > Advanced Configuration > Common Objects > PPPoE** and then click **New**.

- In this release, the admin can manually select one or more Aerohive devices and clear the audit mismatch flag that an on premise HiveManager may apply during configuration.



- In this release of HiveManager, you can now configure TeacherView to use either HTTPS or HTTP when redirecting to HiveOS. When upgrading to HiveManager 6.6r1, devices that are running most of the previous HiveOS releases will continue to run HTTP as the default captive web portal for TeacherView. (There are two exceptions. In HiveManager 6.4r1 and 6.5r1, TeacherView is set to HTTPS by default.) To change the setting to HTTPS, you need to upload the 6.6r1 HiveOS configuration onto your devices and then make the configuration changes described below.

  In HiveManager, navigate to **Home > Administration > HiveManager Services > TeacherView Settings**. On the *HiveManager Services* page, select **TeacherView Settings** and **Enable TeacherView**. Then select the check box next to **Enable HTTPS for HiveUI** and click **Update**.



- In this release of HiveManager, the API key length is now suitable for AirWatch 8.0.
- On Aerohive branch routers, when PPPoE is already enabled on an interface, enter the following command to disable NAT (network address translation):

  `(no) interface <ethx | usbnetx> mode wan nat`

- In this release, RC4 is not supported as a cipher mechanism.

Upgrading HiveManager Software

Aerohive supports upgrading to the 6.6r1 HiveManager 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 before upgrading your system to 6.6r1.

To upgrade the AP230 firmware from HiveOS version 6.1r5 to 6.6r1 or later, you must first upgrade from version 6.1r5 to 6.1r6 followed by a second upgrade from 6.1r6 to 6.6r1.

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 6.6r1

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

From	Action	To
HiveManager 5.1r2 or later	Upgrade to HiveManager 6.6r1.	HiveManager 6.6r1
HiveOS 5.1r2 or later	Use HiveManager running HiveManager 6.6r1to manually upgrade managed devices to HiveOS 6.6r1.	HiveOS 6.6r1

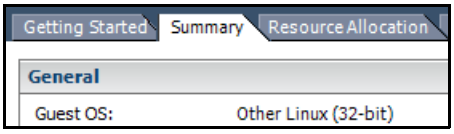
Upgrading the HiveManager Appliance	
1	Back up your database as a safety precaution. Navigate to **Home > Administration > HiveManager Operations > Back Up Database**.
2	Save the 6.6r1 HiveManager software file to a directory on your management system or SCP server. (Log in and download the 6.6r1 HiveManager software file from the Aerohive Support page.)
3	Log in to HiveManager running 5.1r2 or later and then upload the 6.6r1 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

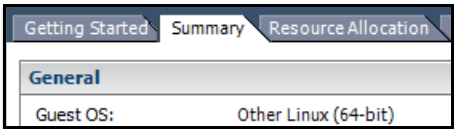
Before you can upgrade a 32-bit HiveManager Virtual Appliance to 6.0 or later, you must increase the memory for it within the ESXi hypervisor to 3 gigabytes, set the number of virtual sockets for its CPU to 2, and change VM params to 1024 megabytes.

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 6.6r1 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.

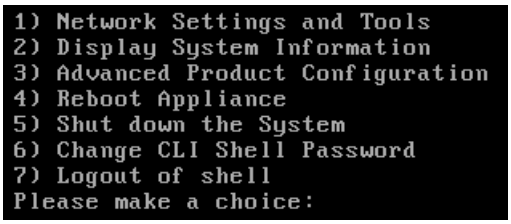


32-bit HiveManager Virtual Appliance

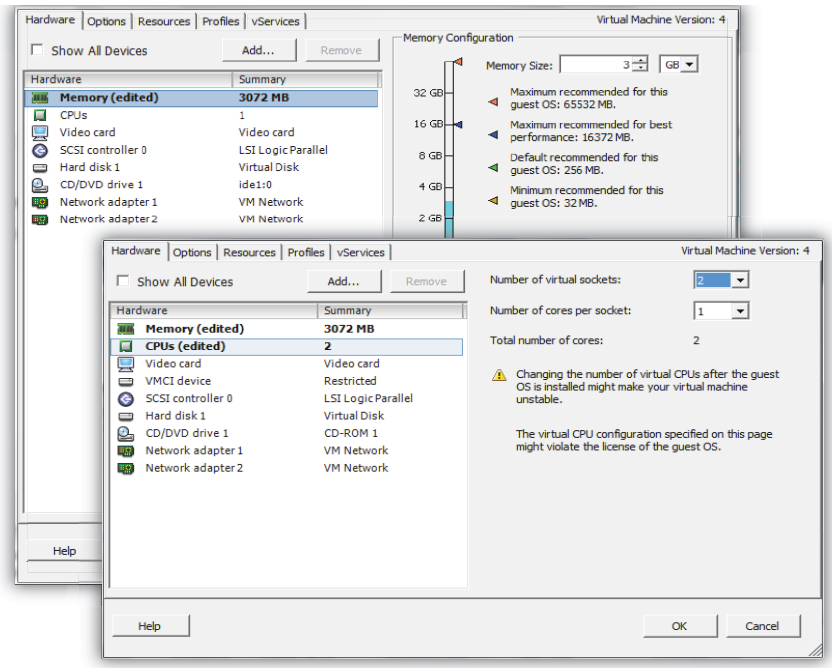


64-bit HiveManager Virtual Appliance

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.



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.)

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 known issues were found in the HiveOS and HiveManager 6.6r1 releases.

Known Issues in HiveOS 6.6r1

CFD-1053	Stations (or clients) that support only long preambles are unable to connect to an AP230 when the Preamble field is configured as Auto (Short/Long). Workaround (WA): Configure the radio profile to use long preambles to allow legacy clients to connect.
HOS-2747	Some third party Beacons (such as those from RADIUS Networks) are not detected by the HiveManager iBeacon Monitor when using their vendor-supplied firmware. WA: Install Aerohive firmware on the third-party Beacon.
HOS-2631	The 802.11r implementation requires client devices that connect to the network to support fast BSS transition in their wireless hardware drivers. There is an issue with clients who are running outdated versions of the Intel 6300N drivers connecting to Aerohive APs when 802.11r is enabled on the APs. WA: There are two workarounds for this issue. Either disable 802.11r on the APs or upgrade the client Wi-Fi drivers to the latest version.
HOS-2570	There is an issue with creating PPSKs (Private Pre-shared Keys) when you enable an AP as an ID Manager authentication proxy and then apply an SSID that includes 802.11r. WA: Disable 802.11r on all APs configured as an ID Manager authentication proxies.
HOS-2454	SR Series switch ports support either HivePort or spanning tree, but not both. WA: Configure either HivePort or spanning tree on a switch port.

Known Issues in HiveManager 6.6r1

CFD-1133	In the Additional Settings > Traffic Filter Settings section of the network policy, the Enable inter-station Traffic check box applies to wired interfaces only and does not affect wireless interface behavior.
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.
HMGR-790	HiveManager on premise expects a slightly different format when you export a .csv file and then import it. In the exported .csv file, the Access Mode, Auto Channel, Country Code, and Wifi0 Admin State rows have text values only. However, HiveManager expects the values for these rows to be a number in the imported file. For example, the Wif0 Admin State row contains “Up" or “Down" in the exported file. The imported file requires "0" or "1" to replace "Up" and "Down" where Up = 0 and Down =1. WA: After you export a .csv file, edit the fields by hand before reimporting it. Click the **View Details** button to see the acceptable format for each field.

Addressed Issues

The following issues were addressed in the HiveOS and HiveManager 6.6r1 releases.

Addressed Issues in HiveOS 6.6r1

CFD-1146	The BR200-LTE-VZ router improperly reported a loss of CAPWAP connectivity to HiveManager while Aerohive devices behind the router remained connected.
CFD-1111	The default user profile attribute was overridden by the HivePass captive web portal.
CFD-1079	When a user was a member of a large number of Active Directory groups, the RADIUS Access-Challenge packets, which contain user group information, exceeded an established size limit and were dropped.
CFD-1078	On networks that required a web proxy server, administrators were unable to update device HiveOS software using the automatic update process in HiveManager. Instead, administrators were required to download HiveOS images manually to update devices.
CFD-1052	Adding a new network to a BR200-WP caused the WAN interface to go down. This issue has been addressed.
CFD-1001	Changes made to the transmit power settings of an AP230 in HiveManager did not persist after a reboot.
CFD-977	In installations in which there were multiple locations, but only one AP per location, APs were not properly electing a designated AP. This issue has been addressed.
CFD-949	Wired 802.1X clients that were directly connected to Aerohive switches were not authenticating after the extended system up time expired.
CFD-900	AP230s sometimes transmitted probe responses at data rates that were disabled in the configuration.
CFD-899	ACSP (Aerohive Channel Selection Protocol) was not reporting non-Aerohive access points in the ACSP neighbor list.
CFD-896	Configuring an Aerohive device acting as a DHCP server to use ARP (Address Resolution Protocol) to detect IP address conflicts caused the device to no longer respond to DHCP discovery packets.
CFD-859	AP330s were transmitting multicast traffic at data rates that were lower than the configured basic data rates.
CFD-848	Clients connecting to an AP230 were sometimes unable to obtain a DHCP address.
CFD-829	An issue with the accuracy of the usage statistics displayed by the *Usage by Location* and *Usage by SSIDs* widgets on the *Dashboard* was corrected.
CFD-796	There was a mismatch when APs reported disconnected clients in SNMP and connected clients in the CLI (command line interface). This issue has been addressed.
CFD-742	Under certain conditions, AP330s sometimes reported incorrectly that interference was higher than it actually was.
CFD-715	Certain legacy 2.4 GHz wireless clients in protection mode experienced high packet loss due to a hidden node issue. This issue has been addressed.

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 *Alarms* instead of *Wireless Clients* 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.

P/N 330182-01, Rev. A