Aerohive Release Notes

Release Versions: HiveOS 6.1r6 and HiveManager 6.1r6a, StudentManager 1.1r5

Platforms: AP110, AP120, AP121, AP141, AP170, AP230, AP320, AP330, AP340, AP350, BR100, BR200, BR200-WP, BR200-LTE-VZ, SR 2024 series devices; VPN Gateway Appliance, and VPN Gateway Virtual Appliance; HiveManager Online, and all HiveManager Physical and Virtual Appliances.

Release Date: June 30, 2014

These are the release notes for HiveOS 6.1r6 firmware, HiveManager 6.1r6a software, and StudentManger 1.1r5 software. These releases contain numerous new and enhanced features, summaries of which are described in the following section. For more detailed descriptions, see the *Aerohive New Features Guide*. Known issues are described in the "Known Issues" on page 18 section and "Addressed Issues" on page 20 section near the end of this document.

> ⓘ *Although HiveOS 3.4r4 was the last release for the HiveAP 20 series, HiveManager 6.1r6a can continue to manage all Aerohive platforms. However, you must push full configuration updates to them 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 5.0, 5.1, 6.0, and 6.1.*

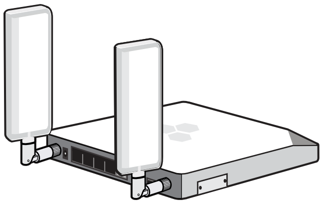
Memory Increase Required before Upgrading to HiveManager 6.0 or Later

Before upgrading HiveManager software on existing HiveManager physical appliances and HiveManager Virtual Appliances to 6.0r1 or later, you must first increase their memory to 3 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 15.

> ⓘ *Before upgrading HiveManager, it is always a good precaution to do a full backup of the database.*

New 6.1r6 Hardware Platform and Hardware Enhancements

BR200-LTE-VZ: This release introduces the BR200-LTE-VZ router. The BR200-LTE-VZ allows enterprises to provision branch office networks and teleworkers quickly and easily. This router provides LAN and WLAN connectivity and PoE (power over Ethernet) support. The router has a single dual band 2.4/5 GHz (802.11a/b/g/n) radio, an embedded LTE modem for use with the Verizon 4G LTE network, two external diversity antennas, one WAN port (ETH0), four LAN ports (ETH1 through ETH4), a Console port, and an LTE USB port for WAN connection redundancy (reserved for future use). Routers support up to 16 SSIDs, 16 VLANs, 16 networks, and 64 user profiles across both wired and wireless interfaces.



New Features and Enhancements in the 6.1 Releases

The following are the new features and feature enhancements in the HiveOS and HiveManager 6.1 releases:

New and Enhanced HiveOS 6.1r6 and HiveManager 6.1r6a Features

The following are the new features and feature enhancements in the HiveOS 6.1r6 and HiveManager 6.1r6a releases. For more information about these new and enhanced features, see the *Aerohive New Features Guide*.

New and Enhanced HiveOS 6.1r6 Features

The following are the new features and feature enhancements in the HiveOS 6.1r6 release.

ⓘ *There is no 6.1r6 firmware image for the SR2124P or SR2148P devices.*

Enhancements to NetConfig UI Security: The NetConfig UI in HiveOS 6.1r6 now displays a message that notifies you if Internet connectivity is unavailable rather than simply displaying the *WAN Interface Settings* page.

DHCP Option 43 Support: In HiveOS 6.1r5 and earlier, Aerohive devices were unable to fully support DHCP Option 43 because the maximum number of configurable hex digits was limited to 32. This release increases the number of configurable hex digits to 254, making it easier to deploy applications such as Microsoft Lync Server.

Additional USB Modem Support: This release adds the following USB modems to the supported modems list:

- AT&T Beam AC340U
- Verizon Pantech 4G LTE UML295
- T-Mobile Rocket 3.0 4G ZTE MF683
- Franklin C-Spire Wireless 4G LTE U772

Devices Supporting KDDR Logging: The KDDR (Kernel Diagnostic Data Recorder) logs capture run-time statistical data about unexpected events and difficult-to-predict or unwanted situations that might occur with the ongoing processes and services of an Aerohive device. The KDDR logs are disabled by default in both the on-premises HiveManager appliances and HiveManager Online. With this release, KDDR logging support is available for all Aerohive access points that can run HiveOS version 6.1r6.

New Certification for Aerohive devices: In the 6.1r6 release, several Aerohive devices have been newly certified for the following regulatory specifications and DFS (dynamic frequency selection):

Platform	**Regulatory Certification in:**	**DFS Certification in:**
AP121	China, India, Saudi Arabia, Taiwan	USA FCC
AP141	China, India, Saudi Arabia, Taiwan	USA FCC
AP170	China, Saudi Arabia, Taiwan	China, Saudi Arabia, Taiwan

Platform	Regulatory Certification in:	DFS Certification in:
AP330	Canada, China, Taiwan	Canada
AP350	Canada, China	Canada
BR100	China, Taiwan	N/A
BR200-WP	China, Saudi Arabia, Taiwan	N/A

New and Enhanced HiveManager 6.1r6a Features

The following are the new features and enhancements in the HiveManager 6.1r6a release.

BR route summarization: With this release, route summarization in HiveManager software increases the scale of a VPN gateway-BR deployment. HiveManager does a local subnet route summarization and then pushes the larger subnet configuration to each branch.

CAPWAP Delay Alarm Change: With this release, you can disable the CAPWAP delay alarms at the policy or device level to avoid excessive alarms that might be triggered as a result of variable or high latency connections between HiveManager and its Aerohive devices.

Entitlement Key Information Export: With this release, you can easily identify the number of Aerohive license entitlements and determine when they need to be renewed for your Aerohive system. After you export a summary file that contains the entitlement key information, you can assess when you will need to notify Aerohive to renew your various licenses.

ID Manager Proxy: Prior to this release, when attempting to retrieve customer IDs using an on-premises HiveManager appliance deployed on a LAN, HiveManager could not contact ID Manager if use of a proxy server was required on the local network. The HiveManager proxy server support only extended to contacting the Aerohive License Server.

With this release, an on-premises HiveManager appliance deployed in a LAN can now access ID Manager by configuring a proxy server for ID Manager connections.

Manual Selection of ID Manager Authentication Proxy: With prior releases, both on-premises HiveManager and HiveManager Online automatically selected devices to act as ID Manager authentication proxies. For example, whenever an AP became a RADIUS server, the AP automatically became the ID Manager authentication proxy by default. If many APs were configured to act as RADIUS servers, it became difficult to identify which RADIUS servers were being used.

HTTPS Security Enhancement for the NetConfig UI and TeacherView: The NetConfig UI and TeacherView now use HTTPS rather than HTTP for more secure communications over the network.

Stronger Wi-Fi Security and Transition of WPA to WPA/WPA2 "Auto" Authentication: With the decision of the Wi-Fi Alliance to discontinue certifying devices that support WPA only, or "WPA alone" authentication, WPA is still allowed, but only in the "WPA/WPA2 Mixed mode" or "Auto" mode.

To comply with this decision, HiveManager 6.1r6a no longer allows WPA-PSK (WPA Personal) or WPA-802.1X (WPA Enterprise) authentication combinations to be used. For HiveManager and HiveOS 6.1r5 and earlier versions, you can still use the WPA only option without the setting being overridden by HiveManager 6.1r6a after a configuration upload. However, for AP230 devices, if HiveManager detects that the WPA only authentication option is set, it is replaced by the WPA/WPA2 "Auto" setting after a new configuration upload.

PCI DSS 3.0 Support: PCI DSS (Payment Card Industry Data Security Standard) compliance is required for all merchants and service providers that store, process, or transmit payment cardholder data. With this release, HiveManager PCI compliance reports follow the PCI DSS 3.0 standard. This release adds the following sections to the PCI compliance report:

- Authentication and session management compliance (PCI DSS 3.0 section 6.5.10)

- Passwords and phrases requirements (PCI DSS 3.0 section 8.2.3)
- Initialization, stopping, or pausing of the audit logs (PCI DSS 3.0 section 10.2.6)

Client Management Certificate Files in .pfx Format: When enrolling clients through an 802.1X SSID that makes use of an external RADIUS server, it is necessary to export the Client Management server certificate, private key, and CA certificate files from HiveManager and then import them to the RADIUS server. When the external RADIUS server is a Microsoft NPS (Network Policy Server), it is necessary to import the files in .pfx format (PKCS #12). To simplify the file transfer, HiveManager now provides a .pfx file that contains all three required certificate and key files for export (Configuration > Advanced Configuration > Keys and Certificates). After exporting the .pfx file from HiveManager, you can then import it directly to the Windows Server running NPS.

AVC signature update: For this release, an updated version of the AVC Signature files, version 3.1.6 (dated 2014/03/16), has been added to HiveManager. To download the latest AVC Signature files, go to Configuration > Show NAV > All Devices, select the check boxes next to devices that you want to update, and then click **Update > Advanced > Upload and Activate Application Signatures**. Or, you can request this file from the Aerohive site from the Support > Software Downloads > login with your Software Downloads Login > Current Software Releases > HiveOS and HiveManager Version 6.0 > Layer 7 Application Signatures page.

New and Enhanced HiveOS and HiveManager 6.1r5 Features

The following are the new features and feature enhancements in the HiveOS and HiveManager 6.1r5 releases. For more information about these new and enhanced features, see the *Aerohive New Features Guide*.

New and Enhanced HiveOS 6.1r5 Features

The following are the new features and feature enhancements in the HiveOS 6.1r5 release.

HiveOS 6.1r5 does not support the SR2124P or SR2148P devices.

Displaying HiveOS Image File Information during an Upgrade: For this release, HiveManager now displays the HiveOS version, supported platforms, and image size information when you upgrade HiveOS on a device. Also, you can now set a device to boot on the current or backup HiveOS image.

KDDR Enhancements: The KDDR (Kernel Diagnostic Data Recorder) logs capture run-time statistical data about unexpected events and difficult-to-predict or unwanted situations that might occur with the ongoing processes and services of an Aerohive device. The KDDR logs are disabled by default in both the on-premises HiveManager appliances and HiveManager Online. With this release, KDDR support is made available on the AP230.

The following KDDR functionality is enhanced with this release:

- Descriptive kernel function symbol names are added to reference symbol address values in the history buffer, making KDDR files more readable and facilitating file analysis.
- Kernel trace content is integrated into the KDDR functionality to reduce the need to manually associate which kernel trace files correspond to which KDDR log.
- A special buffer now collects historical event data recorded during the last few moments of an abnormal system reboot.

New and Enhanced HiveManager 6.1r5 Features

The following are the new features and feature enhancements in the HiveManager 6.1r5 release:

Client Management Data Displayed in HiveManager: From the Monitor section in the HiveManager GUI, you can now see information that HiveManager retrieves from Client Management about enrolled clients. HiveManager displays their enrollment status in a new column on the Active Clients page and more detailed information in a new section on Client Details pages. Additionally, both the icon that appears in the Enrolled column on the Active Clients page and the device name on the Client Details page are hyperlinks that open the corresponding Client Info page in the Client Management GUI where you can see even more information.

HiveManager API: This release adds the HiveManager database API, which you can use to access HiveManager database objects with a REST (Representational State Transfer) client or from an external service through a REST adapter.

New and Enhanced HiveOS and HiveManager 6.1r3 Features

The following are the new features and feature enhancements in the HiveOS and HiveManager 6.1r3 releases. For more information about these new and enhanced features, see the *Aerohive New Features Guide*.

The new Help system for mobile devices is available with the HiveManager 6.1r3 release.

New and Enhanced HiveOS 6.1r3 Features

The following are the new features and feature enhancements in the HiveOS 6.1r3 release:

Generic USB Modem Support: For this release, a new framework has been added to allow generic USB modem support for BR100 and BR200 routers, and AP330 and AP350 devices functioning as routers. After a new modem type is validated by Aerohive, you will be able to configure your routers to support the modem using the NetConfig UI.

Reporting Application Usage by Clients in Application Visibility and Control: In 6.1r3, HiveManager reports application usage by clients in greater detail, helping you to understand the top clients or users using applications even if you do not have authentication such as captive web portal on an open SSID or PPSK (private preshared key) on your network. Three widgets that report application usage by clients have been added to the *Applications* perspective on the dashboard, allowing more drill-down information about clients and application usage. In addition, three widgets have been modified to display application-only information. After you drill down into client or application information, a new widget tab is created automatically which allows you faster access when revisiting the same data during the same session.

Enhancements to CAPWAP Auto Discovery: Aerohive devices and HiveManager communicate through the CAPWAP (Control and Provisioning of Wireless Access Points) protocol. In 6.1r3, there is a new auto discovery process for devices that have connected to HiveManager at least once. In addition, you can prevent devices from connecting to an unauthorized HiveManager that might have been inadvertently placed in the same subnet as these devices.

Captive Web Portal Enhancements: In this release of HiveOS firmware and HiveManager software support the following enhancements to the captive web portal:

Multiple Captive Web Portal Clients on a Wired Port: Aerohive devices support the individual authentication of multiple captive web portal users when the users are connected through a switch or hub to a single Ethernet port on the Aerohive device.

Captive Web Portal Selection by Classifier Tags: You can now configure captive web portals to forward users to custom Internet or network destinations after authentication based on the classifier tag that you assign to the device. You can not only forward users to a custom destination after successfully authenticating, but you can also forward them to a custom destination after an unsuccessful authentication, depending on the type of authentication you use with your captive web portal.

AirWatch Compliance Enforcement: In this release of HiveOS firmware and HiveManager software, Aerohive supports periodic recurring AirWatch compliance checking and enforcement, allowing administrators to block noncompliant wireless devices.

Integration of OpenDNS: HiveOS firmware and HiveManager software now integrate OpenDNS and support OpenDNS-based web content filtering and security through user profiles. Mapped to different groups of users though user profiles, this new feature allows you to enforce different security policies on Aerohive devices connected behind Aerohive routers.

DFS Support: The AP330 and AP350 now support DFS (Dynamic Frequency Selection), permitting the AP to use of radio channels in the 5 GHz UNII-2 (Unlicensed National Information Infrastructure) bands, because mechanisms are in place and certified to detect and avoid interfering with radar systems.

Topology Map Name No Longer Overrides sysLocation: This release introduces the ability to override the default behavior of overriding the sysLocation name with a topology map name.

Power Cycle Devices through PoE: This release adds the ability to cycle the power on selected PoE ports.

Default PoE on Switches Uses 802.3at: The default PoE port setting for Aerohive switches is now 802.3at instead of 802.3af.

Syslog messages for Firewall Events: Aerohive devices now include the user name and host name in firewall events destined for a syslog server. The additional information provides important security and audit information for administrators. If you already have a syslog server configured, then no further configuration is necessary in HiveManager; however, if not, simply configure a syslog server in HiveManager to provide a destination for logging events, and then choose the server in the firewall policies. Aerohive devices automatically format firewall events, and then forward them to the Syslog server.

Enhancements to Alarm Log Settings: The *Alarm Log Settings* dialog box available from Monitor > Alarms > Settings has been expanded, allowing you to differentiate between non-critical (cleared and uncleared) and critical alarms and set time and size limits for purging non-critical alarms.

Rogue Client Reporting and Expiry: When configuring a WIPS policy, you can configure HiveManager to purge a client that has previously been reported as a rogue after a specified amount of time. By default, if a rogue client is not detected on the network an hour after its last detected activity, then HiveManager drops the rogue device from its list of rogue devices.

Overwrite Protection for NetConfig UI WAN Settings: In previous versions of HiveOS firmware and HiveManager software, devices that were configured using the NetConfig UI might be overwritten when HiveManager pushed updated settings to the BRs. The default behavior of this software release is that a BR originally set up using the NetConfig UI is protected from being overwritten by updates pushed to it from HiveManager at a later date. You can disable this protection so that whenever a newer configuration is pushed to the BRs, the newer configuration will take effect.

Bonjour Sleep Proxy Support: When a Bonjour-enabled device goes into power save mode, it can inform another device—referred to as a sleep proxy server—to continue advertising services on its behalf. The server then begins responding to ARP requests and multicast DNS queries for the sleeping device. When another device requests a service from the sleeping device, the sleep proxy server sends a magic packet to wake it up. The awakened device then broadcasts a gratuitous ARP, alerting all the devices in its subnet/VLAN of its MAC address. The requesting device can then communicate directly with the previously sleeping device.

Aerohive devices functioning as Bonjour Gateways can filter the _sleep-proxy._udp service, which sleep proxy servers advertise, in the list of services that they share with other Bonjour Gateways. This allows you to control whether devices connected to Bonjour Gateways in different subnets/VLANs can access services on a device in power save mode through a sleep proxy server in another subnet/VLAN.

New and Enhanced HiveManager 6.1r3 Features

The following are the new features and feature enhancements in the HiveManager 6.1r3 release:

VMware Tools for HiveManager Virtual Appliance: VMware Tools suite is a set of utilities and drivers that increases the performance of a virtual machine and aids its management. HiveManager Virtual Appliance 6.1r3 and later deployed on VMware ESXi version 4.1 and later hypervisors support the VMware Tools suite.

Preconfigure Devices: You can now preconfigure devices before you add them to your HiveManager network. In addition, the *Managed Devices* and the *Unmanaged Devices* tabs have been added to on premises HiveManager *Configuration* and *Monitor* GUI sections. The Device Inventory menu on the *Unmanaged Devices* tab now has add, remove, export, and import options in both on premises HiveManager and HiveManager Online and this same menu on the *Managed Devices* tab provides remove and export options. There is a slight difference in behavior depending on if you are using on premises HiveManager or HiveManager Online.

Enhancements to Simplified Updates: In 6.1r3, you can push the latest HiveOS image onto a device even when the version numbers on the device and the image server are the same.

New Help System for Mobile Devices

Aerohive now allows you to link directly to a mobile version of our HiveManager 6.1r3 Help system. The HiveManager 6.1r3 Mobile Help system can be viewed using phones that do not support some of the advanced mobile web technologies. It does this by detecting the mobile device on which you are attempting to view the Help system and forwards your request to one of two independent versions of mobile Help system.

New and Enhanced Client Management (January 2014)

Client Management as a Separate Product: Client Management has been removed from HiveManager and promoted from a feature to a separate product. By default, you can use Client Management to enroll and manage up to 100 Apple, Android, and Chromebook clients. To support more mobile devices, you can obtain subscriptions from your Aerohive sales representative.

Single Private PSK SSID for Enrollment: You can now use a single private PSK SSID for enrollment and access to the network. With this option, clients use a shared PSK to enroll with Client Management, which then assigns a unique private PSK to each client to access the same SSID after enrollment.

HTTP Proxy: For clients that must access the public network through an HTTP proxy server, you can configure HTTP proxy settings for inclusion in Wi-Fi configuration profiles.

New and Enhanced ID Manager (January 2014)

Support for CoA (Change of Authorization) Disconnect from ID Manager to APs: With this release, ID Manager notifies APs as soon as a guest account is revoked, expires, or when the customer's ID Manager account has expired, it disconnects these accounts immediately.

Audit Log Enhancements: This release adds a section to the ID Manager Audit Log that shows when admin accounts have been created or deleted from the MyHive page.

Email Template Customization: This release allows ID Manager administrators to customize the template for email and print notifications by changing the icon, logo, or text.

Support for Multiple AP Networks for Anonymous Access: This release adds support for ID Manager Anonymous Access on multiple AP networks.

ID Manager Wired Access: This release adds support for ID Manager on wired networks through BR200 router configuration.

Customized Registration UI: This release introduces the capability to customize the registration UI that appears on your kiosk.

New and Enhanced HiveOS and HiveManager 6.1r2 Features

The following are the new features and feature enhancements in the HiveOS and HiveManager 6.1r2 releases. For more information about these new and enhanced features, see the *Aerohive 6.1 New Features Guide*.

New and Enhanced HiveOS 6.1r2 Features

The following are the new features and feature enhancements in the HiveOS 6.1r2 release:

Support of IEEE 802.11ac: Aerohive supports the first wave of IEEE 802.11ac technologies, features, and data rates.

Enhancements to Applications Visibility and Control (AVC): A number of enhancements have been made to the Applications Visibility and Control (AVC) feature including auto discovery of applications by usage, the ability to create custom applications, the ability to disable AVC, and support for the Microsoft Lync application:

Auto Discovery of Applications: This release adds an Application Auto Discovery feature that enables HiveManager to automatically discover applications in your network. In addition, you can add up to seven applications to an applications watchlist as well as create individual watch lists for each virtual HiveManager.

Custom Applications: In addition to the more than 700 system defined applications, in6.1r2 you can define custom applications that can be detected with the auto discovery feature and that you can add to the applications watchlist or to QoS and firewall policies. These custom applications incorporate rules that are defined by IP addresses, TCP or UDP ports as well as by HTTP and HTTPS host names. In addition, these custom applications can be viewed from the Dashboard.

Disabling AVC: Administrators with super user privileges in on-premises HiveManager appliances now have a system-wide way to disable or enable the Application Visibility and Control Settings for all VHMs.

Support for Microsoft Lync: This release adds support of the Microsoft Lync suite of products as a system-defined application.

Enhancements to Captive Web Portals: In this release, the captive web portals include the collection of client information during authentication and information to determine the Aerohive device to which a captive web portal client is associated:

Collecting Client Information from Captive Web Portal: You can now collect information submitted by the user as part of the authentication and acceptance of the terms of use when a user authenticates to a captive web portal.

NAS-ID for External Captive Web Portal: Aerohive APs now include the NAS-ID in the redirected HTTP headers sent to external captive web portals so that you can use the information to determine the Aerohive device to which a captive web portal client is associated. You can configure an Aerohive device to use its host name as the NAS-ID, or to use a custom NAS-ID that you configure consisting of 1-64 characters.

Using External DNS Servers in DHCP Offers: You no longer need routers to act as DNS proxies and can specify that DNS services be supplied from external DNS proxies or servers to obtain IP addresses in DHCP offers. You can now specify DNS services directly from external DNS proxies or servers through the enabled DHCP connection of the router.

Specifying an Ethernet Port for Switch Netdump File: You can now specify an Ethernet port on an Aerohive switch for saving the netdump file to a TFTP server on the network automatically the next time the switch boots up. When bootloader boots up and detects a need to upload the netdump file, only the specified netdump port is enabled to upload the netdump file.

Enabling or Disabling DHCP Server ARP Validation by Routers: There is now an option to enable or disable Dynamic Host Configuration Protocol (DHCP) server Address Resolution Protocol (ARP) verification by Aerohive routers. When there are many clients that require IP addresses at the same time, this option prevents the DHCP server from sending gratuitous ARP requests and waiting to validate that the IP address is usable.

Switch PSE Support for Legacy Devices: This release adds the ability to configure Aerohive switches to provide PoE support for legacy powered devices that do not comply with the current 802.3at standard.

Support for RADIUS Proxy and ID Manager Proxy on the Same Device: You can now configure a RADIUS proxy server for authentication and an ID Manager RAD Sec proxy server to operate simultaneously on a single Aerohive device.

New and Enhanced HiveManager 6.1r2 Features

The following are the new features and feature enhancements in the HiveManager 6.1r2 release:

New HiveManager Graphical User Interface Appearance: The graphical user interface has a new look and feel In this release of HiveManager. It has a new, user-friendly look and feel, a brighter color theme that is more aesthetically pleasing, new icons and buttons that promote more harmonious interaction, and customized elements that are easier to use.

Enhancements to Configuration and Monitoring Pages: Changes were made to both the *Configuration* and *Monitoring* pages and commands in this release of HiveManager. They are now called *Unconfigured Devices* and *Configured Devices* (formerly, they were *New Devices* and *Managed Devices, respectively*) and the difference depends on whether the network policy configuration was pushed to the devices.

Simplified Device Updates: The Device Update drop-down menu has been updated to make it easier to push configuration changes to a device (or devices).

HiveManager Online Configuration and Monitoring Changes: Two new tabs have been added to the Configuration and Monitor pages: Managed Devices and Unmanaged Devices. With these tabs, you can add devices to and remove devices from the Aerohive cloud and a VHM.

Enhanced ID Manager (September 2013) Features

The following improvements are included in the ID Manager (September 2013) release:

ID Manager Print Customization: ID Manager administrators now have the ability to customize the print template from the ID Manager kiosk to accommodate small-factor printers to print guest credentials on badges. Administrators can choose from two default templates, or can create and save their own templates. The default templates accommodate 8.5 x 11" standard paper and 2.4 x 4" thermal print paper. Templates can be customized for fonts, graphics, and the information that is provided on the badge or printed page.

Text Message Customization: ID Manager provides branding and personalization of text messages by enabling you to edit the body of the text message that is sent to customers.

Customization of the Guest Management Portal: We now provide the ability to have a uniquely branded URL for use with ID Manager. Previously, one URL was used, http://idmanager.aerohive.com. In this release, you can prepend your company name to the previous URL, for example, http://yourcompanyname.idmanager.aerohive.com.

Guest Approval Process Enhancements: Employees of the host company can now approve a request from a guest for Internet access before the guest receives access to the network. This feature applies to guests requesting access through the kiosk and requires configuration to enable it.

ID Manager Print Customization: ID Manager administrators now have the ability to customize the print template from the ID Manager kiosk to accommodate small-factor printers to print guest credentials on badges.

New and Enhanced HiveOS and HiveManager 6.1r1 Features

The following are the new features and feature enhancements in the HiveOS and HiveManager 6.1r1 releases.

New and Enhanced HiveOS 6.1r1 Features

The following are the new features and feature enhancements in the HiveOS 6.1r1 release:

Presence Analytics (Retail Analytics): Aerohive and Euclid have formed a partnership to give physical retailers a free *Retail Analytics* function that is integrated directly into their HiveManager online or on-premises accounts. Presence Analytics allows you to monitor an unlimited number of retail stores, browse visitor traffic, collect data about shopper engagement and loyalty, compare retail activity across stores, view historical information, and share data with fellow retailers. You can also choose to upgrade to a premium Euclid account for access to more detailed metrics, greater historical data collection, and other capabilities, such as custom analysis.

Client Management (Trial Version): With this feature, you can automatically provision and manage Apple mobile devices running i OS 5 or later and Apple computers running Mac OS X v10.7 or later as they connect to the wireless network. The Aerohive AP with which the client connects checks if the client is currently enrolled and, if not, a Wi-Fi configuration and an enrollment profile (with client and CA certificates and a mobile device management profile) are installed on the client to apply device security controls such as permitted applications and behavior. These profiles can differ based on whether the device matches a list of MAC addresses of corporate-issued devices or if it is a personally owned device.

Manual Private PSK Activation Timeout: This is a performance enhancement for private PSK activation which makes activation much faster. There is no direct customer impact.

New and Enhanced HiveManager 6.1r1 Features

The following is the new features and feature enhancements in the HiveManager 6.1r1 release:

MyHive and HiveManager Initial Login Experience. This release introduces a new user experience for system administrators logging into a new version of HiveManager. The experience differs for system administrators of on-premises HiveManager, HiveManager Online, and on-premises HiveManager with the Redirection Server (also called the Redirector). Three new screens have been added to the on-premises HiveManager and HiveManager Online login experience. The *Review Inventory* page provides a list of Aerohive devices. For on-premises HiveManager, this page displays the total number of Aerohive devices connected to HiveManager at login. For HiveManager Online, this page displays a list of Aerohive devices that have been licensed to your organization, including the device type, as well as the total number of Aerohive devices. The *Activate License* page displays license and entitlement key information and allows you to activate your license. The *Management Settings* page requires you to change the default password, choose the Express or Enterprise mode, and select a time zone. (If you delete a HiveManager database, the *Review Inventory* and *Management Settings* pages are displayed. However, the *Activate License* page is not displayed in this case.) After you have completed these changes, a *Congratulations!* page is displayed. When you exit this page, the HiveManager Configuration panel is displayed.

In addition to the changes described above, existing HiveManager Online system administrators will notice a new welcome screen in MyHive and that there is no longer a separate Redirector that is visible from this page. Instead of an external Redirector, you can use the HiveManager Online interface to add and remove devices.

Enhanced ID Manager (June 2013) Features

The following improvements are included in the ID Manager (June 2013) release:

ID Manager GUI Enhancements: This release introduces a new look for the ID Manager administration interface. The new home page is divided into three clearly defined sections that provide at-a-glance visibility into critical information about your ID Manager account, and clear pointers to ID Manager configuration processes. HiveManager Online customers can now request a free 30-day trial of ID Manager.

Anonymous Access and Self-Registration with ID Manager: This release adds Anonymous Access and Self-Registration to ID Manager. Anonymous Access allows businesses to offer Internet access to visiting guests using mobile devices as a courtesy so that they do not have to pay for this service through their Internet providers. Self-Registration allows businesses to configure a captive web portal where a guest asks for and receives a user name and password, uses these credentials to log in at first use, and then has ongoing access without the need to log in as long as they are in range, or until the ID Manager admin disables their account.

Changes to Behavior and Appearance

The following change to behavior and appearance was introduced in the HiveOS 6.1r6 and HiveManager 6.1r6a firmware release:

- For HiveOS 6.1r6, the Aerohive Initial Configuration Wizard that was available in the command-line interface console in previous HiveOS releases is no longer available on Aerohive devices with the exception of the VPN Gateway Virtual Appliance.
- The default values for Retail Analytics (Presence) reporting interval is changed from 30 seconds to 120 seconds, which greatly increases the number of devices HiveManager can support.
- The number of hosts that APs can dynamically add to a walled garden in support of the Client Management enrollment process has been increased from 64 to 512.
- With this release, user names in Aerohive local RADIUS databases are no longer case sensitive. Previously, for example, you could add both *AerohivE* and *aerohive* to a RADIUS user group as separate and valid names. In HiveOS 6.1r6, when you create a user name for a RADIUS group, regardless of the letter case usage, HiveOS retains one version of the name in lowercase. Newly created names are now changed to lowercase in HiveOS, all user names are changed to lowercase (and duplicates deleted) as a result of an image upgrade, and APs now change user names to lowercase in on-boarding messages to Client Manager.
- If LLDP (Link Layer Discovery Protocol) and CDP (Cisco Discovery Protocol) are enabled in HiveManager 5.1r6 and then HiveManager is upgraded to 6.1r6a, LLDP and CDP are now enabled on non-host ports of the SR series devices.

The following change to behavior and appearance was introduced in the HiveOS 6.1r5 firmware release:

- In this release, the ACSP (Advanced Channel Selection and Power) channel selection process is improved to provide better channel separation among APs belonging to the same hive.

- In the *Optional Advanced Settings* section for configuring radio profiles, you can no longer enable DFS (Dynamic Frequency Selection) channels to detect radar without changing channels. Configuration of the DFS radar detection feature is no longer supported by HiveManager. After upgrading to HiveManager 6.1r5 software, HiveManager will disable DFS radar detection without changing channels if the previous configuration had that enabled.

The following changes to behavior and appearance have been introduced in the HiveOS 6.1r3 firmware and HIveManager 6.1r3 software releases:

- Aerohive devices support the individual authentication of multiple captive web portal users when the users are connected through a switch or hub to a single Ethernet port on the Aerohive device.
- The AP330 and AP350 are now certified for FCC DFS (Dynamic Frequency Selection) and can switch channels automatically to avoid interfering with radar operations.
- In previous versions of HiveOS firmware and HiveManager software, devices that were configured using the NetConfig UI might be overwritten whenever HiveManager pushed updated settings to the BRs. The default behavior of this software release is that a BR originally set up using the NetConfig UI is protected from being overwritten by updates pushed to it from HiveManager at a later date.
- When you upgrade devices with the latest HiveOS image, some units in your network may already have the latest version of HiveOS installed, but not the latest release of this version. In this new release, a new option appears on the *Update Devices* dialog box allowing you to push the latest HiveOS image onto a device even when the device and image server versions are the same.
- When you select a HiveOS image file to upload to your devices, HiveManager displays the HiveOS version, supported platforms, release date, and image size so that you can ensure it is the right one before uploading it to your devices.
- HiveManager 6.1r2 software running with Internet access automatically checked at one-hour intervals to ensure that the HiveOS device image files uploaded to it matched version 6.1r2 and, if they did not match the version, uploaded the same 6.1r2 versions of the HiveOS image files from the update server. After the HiveOS image files were uploaded to and available in HiveManager, you could easily upload them to all the Aerohive devices with a simplified update push to the selected devices.

  HiveManager 6.1r3 software running with Internet access now checks and uploads the latest supported version of HiveOS image files of devices to HiveManager, rather than uploading files that match the current version of HiveManager. With this enhancement, every Aerohive device can run at its full capacity as it uses the latest version of its HiveOS image. As before, after the HiveOS image files are uploaded and available in HiveManager, you can easily upload them to selected Aerohive devices. If you select devices and then click **Update > Update Devices** (simplified update), HiveManager 6.1r3 pushes the latest supported version of HiveOS to the devices. HiveManager ensures that the latest supported version of an Aerohive device type is uploaded to the device because it automatically checks for the latest version by synchronizing with the update server every hour.

The following changes to behavior and appearance have been introduced in the ID Manager January 2014 release:

- ID Manager now reports the expiration time for guests in days and hours (for example, 4 days, 4 hours) rather than just in hours (100 hours) after the first login. This expiration time appears in the Expires field on the *Welcome, Guest!* notification page.
- In some cases, when you view Wi-Fi data usage for anonymous access clients, you may see usage rates slightly above the limit that you set for these clients. In fact, the data rate limits are being enforced, but there is a time delay while ID Manager sends the data rate limit message through the ID Manager RadSec proxy, and then to the AP. This delay is approximately one minute or less. The amount of data usage you see above the limit depends on the client data transmission rate and delay in the transmission between ID Manager, the RadSec proxy, and the AP.
- If the wired or wireless privilege or SSID setting in ID Manager does not match the self-registration captive web portal configured in HiveManager, the guest self-registration process will succeed, but the actual guest authentication will fail after the guest receives credentials from ID Manager.

The following changes to behavior and appearance have been introduced in the 6.1r2 release:

- The HiveManager graphical user interface has a new, user-friendly look and feel in this release that better fosters ease of use when configuring and monitoring Aerohive devices.
- AVC (Application Visibility and Control) watchlist changes:
  - The role of the watchlist has shifted from being a list of all the applications that you want to track to just the key applications that you want to ensure are being tracked regardless of how much they appear on the network. Due to its new role, the maximum number of applications in the watchlist has been reduced from 30 to 7. After upgrading HiveManager to 6.1r2, HiveManager starts prompting you to reduce the watchlist, although devices that are still running HiveOS 6.0 or 6.1r1 will continue to operate as normal whether or not you make the reduction. However, after you upgrade devices to HiveOS 6.1r2, the entire watchlist will automatically be removed from the devices. Furthermore, if you try to push a configuration with a watchlist in excess of 7 applications to a device running HiveOS 6.1r2, the configuration upload will fail until you reduce it to 7 or fewer applications.
  - In releases before 6.1r2, applications do not begin to appear in the applications widgets in the dashboard until after midnight or until you create a watchlist and upload it to devices. From 6.1r2, applications begin appearing in these widgets within a few minutes after a client connects to an AP and starts generating traffic.
  - There are four new widgets for tracking only the applications on the watchlist: *Watchlist Applications by Clients*, *Watchlist Applications by Usage*, *Watchlist Applications by Usage - Summary*, and *Watchlist Application Usage over Time*.
- In releases before 6.1r2, you can apply a device template to multiple device models as long as they have the same number of ports and the same function. For example, you can apply a five-port device template to a BR200-WP, BR200, and BR100 functioning as a router. From 6.1r2, you can only create a device template for a single device model. For example, in 6.1r2 you must create three unique device templates for a BR200-WP, BR200, and BR100.
- In the HiveManager GUI, devices that are called "New" in releases before 6.1r2 are referred to as "Unconfigured" in 6.1r2. Similarly, devices that are called "Managed" in previous releases are referred to as "Configured" in 6.1r2. In HiveManager Online, there are two further terms to classify devices: "Unmanaged" refers to devices that have entries in the redirector but that have not yet connected to their VHM, and "Managed" refers to devices that have successfully connected.
- The maximum number of characters for a user name in the roaming cache has been increased from 31 to 127. Because Aerohive devices truncate user names that are longer than the maximum, it is now less probable for the roaming cache to contain identical user name strings.
- This release increases the timeframe for which drilldown information is available on the dashboard perspectives from 15 days to 30 days. When drilldown information is available from a perspective report, there is a clickable link. Previously, the information available through this link was only archived for a time period of 15 days. This release increases that timeframe to 30 days. When there has been no new information collected within the 30-day timeframe, the link does not appear.
- In the *Network Summary* perspective on the *Dashboard* page, the *Current Aerohive Device Status (Network Wide)* and *Active Client Status (Network Wide)* widgets have been combined to form the Current Client and Device Status (Network Wide) widget.

The following changes to behavior and appearance have been introduced in the 6.1r1 releases:

- Only an admin with super user privileges can allow HiveManager to display the following option in 11na radio profiles: Enable radar detection without changing channels. The place where the admin can enable this is in the *Update DFS (Dynamic Frequency Selection) Settings* section on the *HiveManager Settings* page.
- HiveManager Online system administrators will notice that there is no longer a separate Redirector that is visible from the *MyHive* page. Instead of an external redirector, you can use the HiveManager Online interface to add and remove devices. In conjunction with this change, a new Remove button, available from the *Monitor* and *Configuration* pages, permits you to remove a device from your HiveManager network, the serial number of the device from the HiveManager database, and the configuration from the device. The device does not automatically reconnect to the

HiveManager network. Also, a new option in the Utilities drop-down menu, Reset Device to Default, is available from the *Monitor* and *Configuration* pages. This option allows you to reset APs, branch routers, switches, and VPN gateways. The Reset Device to Default option removes the device configuration from the device and from HiveManager. (However, the bootstrap configuration remains unchanged.) Then the device reconnects to the HiveManager network automatically.

- Another new option in the Utilities drop-down menu of HiveManager Online, Aerohive Device Inventory, permits you to access the Redirector to check the inventory list of devices as well as add devices to your network. The Redirector is displayed in a separate tab of the same browser window with which you used to open HiveManager Online. You could use this option to view your inventory of Aerohive devices and understand which devices have successfully been able to connect to the Redirector.
- In this release, QuickStart network policies, SSID objects, user profile objects, and port type objects have been removed. However, QuickStart policy templates that you created in previous releases are supported in 6.1r1.
- The tracking timeout setting has been removed from the track IP feature. Instead the timeout value is always the same as that of the tracking interval value.
- APs can provide MAC authentication on their Ethernet ports in access mode.
- PCI compliance reports can be scheduled.
- An SR2024 switch in router mode can now receive its WAN interface network settings through PPPoE.
- TeacherView resource maps have been returned to HiveManager.
- In ID Manager, an SSID that is created using an on-premises HiveManager does not appear in the drop-down list for guest types in the ID Manager administration GUI.

Upgrading HiveManager Software and HiveOS Firmware

Aerohive supports upgrading to the 6.1r6a HiveManager software on physical and virtual HiveManager appliances and HiveOS 6.1r6 firmware on Aerohive devices from 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 6.1r6a.

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 15.

Upgrade HiveManager and HIveOS 5.1r2 or later to HiveOS 6.1r6 and HiveManager 6.1r6a

To upgrade a HiveManager standalone or HA pair and HiveOS firmware, complete the following procedure:

From	Action	To
HiveManager 5.1r2 or later	Upgrade to HiveManager 6.1r6a.	HiveManager 6.1r6a
HiveOS 5.1r2 or later	To upgrade managed devices to HiveOS 6.1r6, use HiveManager running HiveManager 6.1r6a.	HiveOS 6.1r6

1. Back up your database as a safety precaution (Home > Administration > HiveManager Operations > Back Up Database).
2. Save the 6.1r6a HiveManager software file to a directory on your management system or SCP server. (Log in and download the 6.1r6a HiveManager software file from the Aerohive Support page.)
3. Log in to HiveManager running 5.1r2 or later and then upload the 6.1r6a 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.

   For a successful upgrade, Aerohive suggests rebooting 100 series devices before upgrading their HiveOS images from 6.1r2 or earlier and only upgrading them during their off-peak hours.

   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

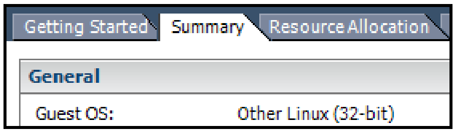
Before you can upgrade a 32-bit HiveManager Virtual Appliance to 6.0 or later, you must increase the memory for it within the ESXi hypervisor to 3 gigabytes, set the number of virtual sockets for its CPU to 2, and change VM params to 1024 megabytes.

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 6.1r1 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.

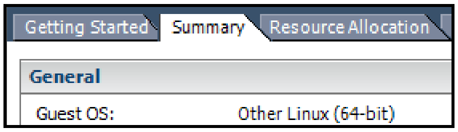
> *You can also check the system type in the HiveManager GUI. In the HiveManager 5.0 and 5.1 releases, click **Home > Dashboard**, and view the model number in the HiveManager System Information widget. The VM 1U model is 32 bits, and the VM 2U model is 64.*



General

Guest OS: Other Linux (32-bit)

32-bit HiveManager Virtual Appliance

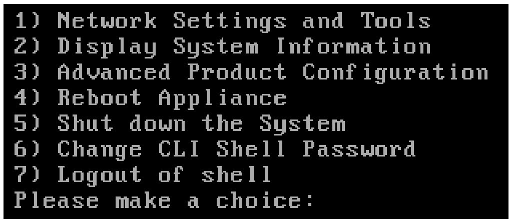


General

Guest OS: Other Linux (64-bit)

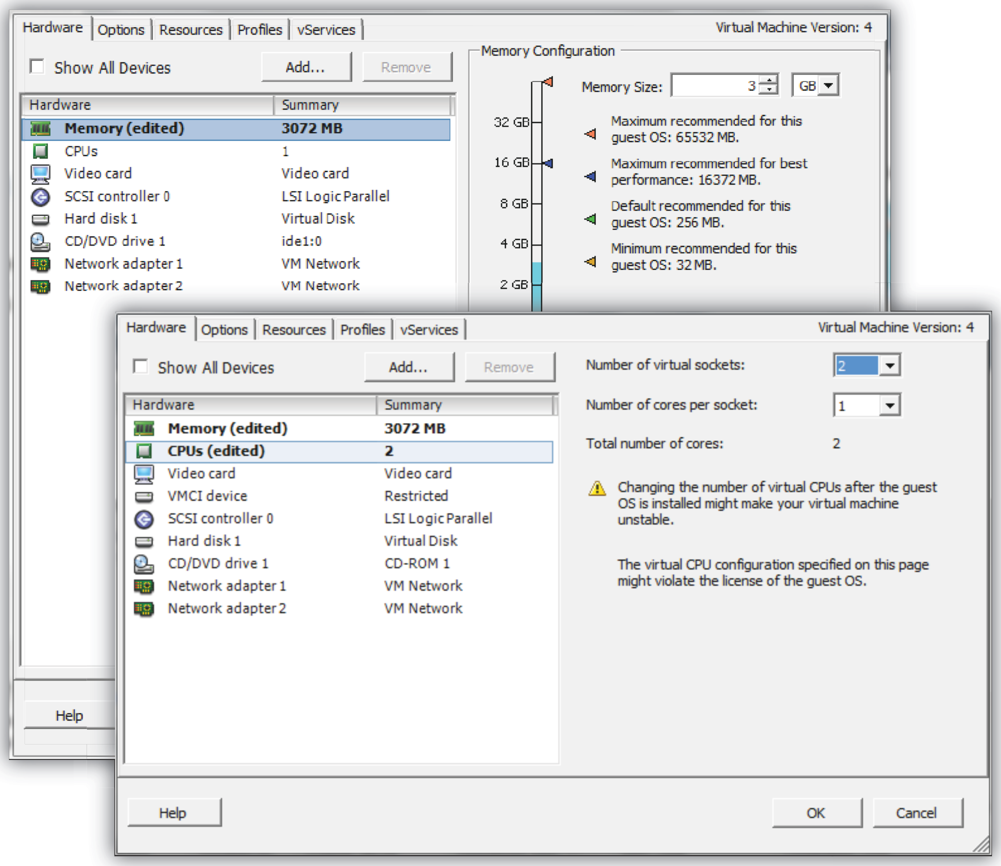
64-bit HiveManager Virtual Appliance

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**.



Virtual Machine Version: 4

☐ Show All Devices

Hardware	Summary
Memory (edited)	3072 MB
CPUs	1
Video card	Video card
SCSI controller 0	LSI Logic Parallel
Hard disk 1	Virtual Disk
CD/DVD drive 1	ide1:0
Network adapter 1	VM Network
Network adapter 2	VM Network

Memory Configuration

Memory Size: 3 GB

Maximum recommended for this guest OS: 65532 MB.

Maximum recommended for best performance: 16372 MB.

Default recommended for this guest OS: 256 MB.

Minimum recommended for this guest OS: 32 MB.

Virtual Machine Version: 4

☐ Show All Devices

Hardware	Summary
Memory (edited)	3072 MB
CPUs (edited)	2
Video card	Video card
VMCI device	Restricted
SCSI controller 0	LSI Logic Parallel
Hard disk 1	Virtual Disk
CD/DVD drive 1	CD-ROM 1
Network adapter 1	VM Network
Network adapter 2	VM Network

Number of virtual sockets: 2

Number of cores per socket: 1

Total number of cores: 2

⚠ Changing the number of virtual CPUs after the guest OS is installed might make your virtual machine unstable.

The virtual CPU configuration specified on this page might violate the license of the guest OS.

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 *Aerohive New Features Guide* as well as 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.

New Help System for Mobile Devices

Aerohive now allows you to link directly to a mobile version of our HiveManager 6.1r6a Help system. In cases where viewing the Help system in a browser is inconvenient or impossible, you can view the Help content on your smart phone. The HiveManager 6.1r6a Mobile Help system can be viewed using phones that do not support some of the advanced mobile web technologies. It does this by detecting the device on which you are attempting to view the Help system and forwards your request to one of two independent versions of mobile Help system.

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 6.1r6

CFD-361	When upgrading the BR100 to HiveOS version 6.1r6, it is possible to cause the device to become unresponsive. WA: To ensure a successful upgrade of the BR100, we recommend rebooting the device before uploading the new HiveOS image.
CFD-353	After HiveOS firmware is upgraded in networks where Cisco Model 7925G phones are deployed, APs do not connect to the Cisco phones. WA: Reboot the APs to establish connectivity with the Cisco phones.
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. WA: To increase the throughput, configure a QoS policy using the policing rate limit in Kbps. For example, set the rate limit to 2000000 Kbps.
32060	When an SR2024P device running HiveOS 6.1r3 is upgraded from 6.1r3 to 6.1r6 and you need to roll back to the previous version of HiveOS using the CLI `reboot backup` command, the 1-Gigabit fiber port connections do not return to their previous UP status. WA: If you need to roll back to the previous version of HiveOS, use the `save image` command rather than the `reboot backup` command.
31730	The Layer 2 bridge access throughput of the AP230 is less than 500 Mbps.

Known Issues in HiveManager 6.1r6a

CFD-549	After HiveManager is upgraded, the configurations for APs operating as RADIUS servers using "Strip realm name from filter" are not properly carried over during the upgrade. If the configuration is subsequently uploaded to the APs, the APs return to their default settings, causing a difference in behavior and RADIUS authentication to fail. WA: After the HiveManager upgrade, change the "Strip realm name from filter" option in HiveManager and upload the new configuration to the Aerohive devices.
CFD-480	Even though no configuration modifications are made to the device in the VHM, the *Audit* icon displayed on the *All Devices* page indicates that there is a configuration mismatch, meaning that the device configuration was modified.
CFD-413	When configuring an HTTP proxy server, the *HTTP Proxy Server IP Address/Domain Name* field only allows a 32-character or shorter length domain name instead of a 128-character domain name.
CFD-21	Multiple languages for the captive web portal use policy acceptance template running on AP121s and BR100s on HiveManger Online accounts do not display the expected language or display a series of question marks.
33275	In the *SSID Access Security* section of the *SSIDs* configuration page, the note that appears after choosing WPA-(WPA or Auto)-PSK for WPA/WPA2-PSK (Personal), WPA-(WPA or Auto)-PSK for Private PSK, or WPA-(WPA or Auto)-802.1X for WPA/WPA2 802.1X (Enterprise) is confusing. The note should state: Note: "WPA" is for platforms introduced before 6.1r5 and "Auto" (WPA or WPA2) is for platforms introduced in 6.1r5 or later.
32687	When updating the HiveManager *Customer ID Retrieval* service, the message "Disable the proxy for ID Manager service successfully" appears erroneous even though the HTTP proxy is not enabled.
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 *Self Registration* 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, 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 6.1r6

CFD-255	Although its *Success* page was returned when the captive web portal was configured to display an acceptable use policy in an iOS 7 environment, iOS 7 disconnected the iPhone from the SSID.
CFD-207	HiveOS version 6.1r6 did not support HT40 for country code 392 (Japan) on APs and returned the message, "Radio capability does not support this phymode". To resolve this issue in HiveOS 6.1r6 and later versions, you must update the country code to "(392/4014) Japan". To update the country code, navigate to the *Aerohive APs* page, select the AP120s, AP121s, and AP141s, click **Update > Advanced > Update Country Code**, select (392/4014)Japan from the *New Country Code* drop-down list, and then click **Upload**.
CFD-164	When a captive web portal applied a new user profile to registered users redirecting them to a different VLAN and DHCP server, the Aerohive device did not release their originally assigned IP addresses.
32133	When the AP230 reported the interfaces, it displayed the incorrect value of -92 dBm for the noise floor.
32101	When both radios were active processing traffic in the wireless to wired direction, the overall AP230 throughput was lower than with 5 GHz traffic only.
31414	When a report was generated, the Transmit Bit Rate Distribution values displayed in HiveManager did not match the values read directly from the AP230.
31206	When band steering was enabled, the AP230 did not steer the configured ratio of dual-band capable clients to the 5 GHz band.
30446	Even when an AP230 required a boost of airtime tokens to meet its minimum targeted throughput level, its SLA status showed it as healthy at 10-minute intervals.
30343	When WIPS and spectrum analysis were both enabled on AP121 and AP141, they conflicted with each other and resulted in an excessively long time to complete the spectrum analysis or did not complete the spectrum analysis.
30285	If you manually cleared the Phase1 SA for an IPsec tunnel on an AP230 (`clear vpn ike sa`) and a wireless client disconnected and reconnected to the AP without reauthenticating itself, the AP230 did not rebuild the GRE tunnel to the VPN server. As a result, the client could not reach any destination requiring its traffic to pass through the tunnel.
30212	Mobile devices connected to an AP230 had their batteries drain faster than expected. This was because when a wireless device was about to go to sleep, it sent a message to the AP230. Then the AP230 responded that it had buffered data to send to the device even when the AP did not have any data. This occurred on both the wifi0 and wifi1 interfaces.
25193	Occasionally, after a reboot, the AP320 or AP340 would apparently be fully booted up but would take several additional minutes before clients could connect tot he 2.4 GHz radio.

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.

Addressed Issues in HiveManager 6.1r6a

CFD-463	In HiveManager Online, when attempting to import a csv (Comma Separated Value) file by clicking **TeacherView > Classes > Import**, the import action failed.
CFD-390	After restoring a database backup for a HiveManager 6.1r5 deployment, multiple APs rebooted and reverted to their default configuration when they came back online.

Addressed Issues in HiveManager 6.1r3

30196	In the *Admin Account Manager* 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 *Unmanaged Devices* 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 *Application Usage over Time* widget did not display any data. **Note**: *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.*
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 *Device Update Results* page.
28790	After the HiveManager Online administrator logged in to a VHM (virtual HiveManager) and added or removed a device using the Device Inventory 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 Device Inventory 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 *Applications* 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 *Monitor* 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**: *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.*

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 *System Details* section of the Monitor > Devices > Routers > *router_name* 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 *TeacherView* > *Classes* > *New page,* clicking the New (+) icon launches the *New Teacher Account* dialog box. With the implementation of centralized user management through MyHive, the *New Teacher Account* 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.

Addressed Issues Manager (January 2014)

30375	ID Manager had authentication issues with captive web portal self-registration.
30362	The CA certificate server could no longer issue a certificate after running for some time.
29055	Users that had revoked Private PSKs could still continue to access the network.

28844	Viewing the Active Guests properly displayed the Expiration column. However, the Expiration column showed a range “Valid from <*date and time*> to <*date and time*>” instead of the expected time of expiration.
28503	ID Manager did not disconnect or dissociate revoked ID Manager accounts.

Addressed Issues in ID Manager (September 2013)

28503	When a guest user is revoked in ID Manager, the connection of that guest user is not disassociated from the network if the guest is still connected to an AP.
27239	Actions taken on ID Manager admin accounts were only reflected in the audit log of the system where the action occurred, not on both ID Manager and the portal.

P/N 330104-06, Rev. B