Vertiv™ Avocent® HMX Advanced Manager

Release Notes

VERSION 6.2, OCTOBER 2026

Release Notes Section Outline

1. Features and Enhancements
2. Upgrade Instructions
3. Firmware Version and Compatibility Information
4. Resolved Issues
5. Known Issues
6. Minimum Supported Firmware Versions
7. Important Virtual Machine Information

1. Features and Enhancements

This version of the Vertiv™ Avocent® HMX Advanced Manager introduces the following features and maintenance improvements:

- Updated the On-Screen Display (OSD) interface for supported DVI receiver platforms.
- Improved API response consistency.
- Added support for the latest supported endpoint firmware releases.
- Improved search functionality within the management interface.
- Added pagination enhancements within the management interface.
- Improved management interface performance and reliability.
- Updated various maintenance and stability components throughout the platform.
- Support for v10 firmware for Vertiv™ Avocent® HMX800 and HMX6250 series endpoints

2. Upgrade Instructions

NOTES:

- **This firmware update is ONLY applicable for the Vertiv™ Avocent® HMX G2 manager, and is not supported for the the first-generation Vertiv™ Avocent® HMX G1 manager.**
- **For additional product information, please see the Vertiv™ Avocent® HMX Advanced Manager Installer/User Guide.**

Important Prerequisites

Prior to upgrading your firmware, please ensure you have verified the following information:

- Ensure you make a backup of the Vertiv™ Avocent® HMX Advanced Manager before upgrading.
- Ensure you are using Chrome, Firefox or Safari for upgrading; Vertiv does not recommend using Microsoft IE or non-Chromium based Edge browsers.
- Check your Vertiv™ Avocent® HMX Advanced Manager factory firmware version. If it is below 4.1.36651, you MUST upgrade to version 4.15 before upgrading to firmware version 5.5 or higher.

© 2026 Vertiv Group Corp. All Rights Reserved.

- Ensure your Vertiv™ Avocent® HMX 5100, 5200, 6200 and 6210 extender firmware is version 5.5 or higher. (Version 5.5 is the minimum endpoint firmware requirement for those extenders to be listed in the Vertiv™ Avocent® HMX Advanced Manager software Transmitter and Receiver tabs.) After upgrading the Vertiv™ Avocent® HMX Advanced Manager, a warning message with a link to the list of endpoints not meeting the minimum firmware requirement will appear in the Transmitter and Receiver tabs.
- Check your Vertiv™ Avocent® HMX 6500 receiver firmware version. If it is a version lower than 1.1.0.16, it MUST be upgraded before upgrading the Vertiv™ Avocent® HMX Advanced Manager to version 4.15. or 5.5.

  NOTE: When upgrading the Vertiv™ Avocent® HMX 6500 receiver, do not select the *Reboot before Upgrade* option.
- If upgrading multiple Vertiv™ Avocent® HMX Advanced Manager servers, ensure you upgrade the primary first and then the backup.

  NOTE: Do not upgrade the primary and backup concurrently.

Upgrading the Firmware

To upgrade the firmware on the Vertiv™ Avocent® HMX Advanced Manager server:

1. In the user interface (OBWI) of the Vertiv™ Avocent® HMX Advanced Manager server, or the primary server, select *Dashboard – Settings - Managers* and ensure that the Require Authentication radio button is set to No. If it is not set to No, change it and click *Save*.
2. Select *Dashboard - Backups* and ensure the backup option to Download to your computer is selected. Click *Backup Now*.
3. Using the Vertiv™ Avocent® HMX Advanced Manager software server, verify that all transmitters and receivers are connected and online.
4. Navigate to *Dashboard - Updates* and browse to the location of the software update file.
5. Select the file and click *Open*.
6. Click *Upload*. Do not restart or turn the Vertiv™ Avocent® HMX Advanced Manager software server off until the upgrade is complete.
7. After the upgrade is complete, click *Restart Now*.

   NOTE: While the update is applied, the primary server temporarily loses communication. During this time, the backup server acts as the primary server. You are redirected to the backup server's web User Interface (UI) and automatically logged in. When the primary server becomes available, you are redirected back to that web UI.
8. If you have a Vertiv™ Avocent® HMX Advanced Manager backup server, repeat the steps above to upgrade the backup server. Then, proceed to the next step.
9. The upgrade should now be complete. To verify, select *Dashboard – Settings - Managers* on the primary Vertiv™ Avocent® HMX Advanced Manager software server and confirm both servers are upgraded and synchronized.

3. Firmware Version and Compatibility Information

APPLIANCE/PRODUCT	IMAGE/CODE VERSION
Vertiv™ Avocent® HMX Advanced Manager	v6.2

This release has been tested with the following browsers:

- Microsoft Edge: ver. 150.0.4078.83 (Windows 10/11)
- Microsoft Internet Explorer: ver. 8.0.7601.17514 (Windows 7)

© 2026 Vertiv Group Corp. All Rights Reserved.

- Mozilla Firefox: ver. 100.0 to 152.0.6 (Windows 10/11) and ver. 115.9.1 (Windows 7)
- Google Chrome: ver. 97.0.4692 to 150.0.7871.129 (Windows 10/11) and ver. 97.0.4692.71 (Windows 7)

4. Resolved Issues

This version of the Vertiv™ Avocent® HMX Advanced Manager resolves the following issues.

- Fixed inconsistent OSD presentation when switching between channels, presets, and C-USB LAN on supported DVI receivers.
- Fixed an issue that limited the number of items assigned to a preset.
- Fixed an issue where the OSD displayed channels but did not display presets when launched on supported DVI receivers.
- Fixed an issue that could prevent a backup file from being restored.
- Fixed an issue that could delay login access to a backup or newly configured manager.
- Fixed an issue that prevented a static IP address from being assigned to an additional network port on supported receivers.
- Fixed an issue where password and two-factor authentication settings were not retained when both settings were changed during the same user reconfiguration.
- Fixed an issue where the IGMP Force v3 option was not highlighted when selected by default with Global Multicast enabled.
- Fixed an issue where a successful device replacement could also display an incorrect failure message.
- Fixed an issue where the backup manager Eth2 IP address was not displayed in the server list after a description and location were added.
- Fixed an issue where transmitter and receiver list filters applied only to the currently displayed page.
- Fixed an issue where the Disconnect All button appeared on the Receivers page when the feature was disabled in the global settings.
- Fixed an issue where the selected locale was not applied correctly to receiver OSD pages.

5. Known Issues

The following issues apply to the Vertiv™ Avocent® HMX Advanced Manager.

- **Active Directory Issues**
  - Users are unable to filter Active Directory server-fetched users when the Directory Server name contains a plus (+) symbol.
  - Selecting Preview also performs a synchronization with the Active Directory server.
  - After removing the filter from the Directory Server configuration, the save and synchronization functions do not work from the scanned server tab. To resolve the issue, navigate to another Vertiv™ Avocent® HMX Advanced Manager tab and attempt to save the users again.
  - When Active Directory is configured with Kerberos authentication, data can initially be retrieved successfully. However, after changing the manager time, the manager may be unable to retrieve Active Directory data. The syslog displays a "Directory Server bind failed!" message. To resolve the issue, edit and re-save the Directory Server settings.
- **Application Programming Interface Issues**
  - API access remains active when web access is blocked on the KVM network.
  - When creating a preset through the API, the system allows the preset to be created when an invalid channel-receiver identifier is provided.

© 2026 Vertiv Group Corp. All Rights Reserved.

- The get_presets API may not update the preset count and details for an exclusive mode preset. As a workaround, enable all connection modes on the preset.

- **Authentication Issues**
  - The Auto-Logout feature is not supported for an anonymous user. The anonymous user is logged out when the Auto-Logout timer expires.
  - Kerberos settings may not update correctly after they have been saved. To change the settings, disable Kerberos, re-enable it, and re-enter the settings.
  - Kerberos settings are not retained when the feature is disabled and then re-enabled. Re-enter the Kerberos settings after re-enabling the feature.
  - Enabling two-factor authentication does not prevent use of the Auto Login feature. Users can continue to use hotkeys to switch channels without logging in to the OSD.
  - Two-factor authentication is suspended when the backup manager is acting as the primary manager.
  - Assigning a password to the anonymous user prevents No Login Required from operating.
  - Bulk Enable/Disable Two-Factor Authentication is not supported for Directory Server users. Use the individual 2FA toggle on the Users page.
- **Channel and Preset Issues**
  - There is no option in the OSD to disconnect a preset from a receiver. Presets can be disconnected through the manager web interface or API.
  - Receiver groups and global USB settings are linked. Changing USB settings for a receiver group also modifies the global USB settings. Revert the global USB settings after making receiver group USB changes.
  - Restricted character support applies to device, channel, and preset names. Only the following special characters are supported: _ ( ) : -. When upgrading from version 5 to version 6, existing names are imported correctly. However, editing and saving a page may require unsupported characters to be removed.
  - When using the Connect Channel interface, a receiver connected by another user cannot be disconnected. Use the disconnect button from the Receivers list instead.
- **Network Issues**
  - Vertiv™ Avocent® HMX 8000 series devices may appear offline in the Advanced Manager if the Eth2 IP address is blank while the network cable is connected in DHCP Reservation mode. To resolve the issue, disconnect the Eth2 network cable, enter a DHCP Reservation IP address, or restore the applicable DHCP setting.
  - The web server may become inactive on the primary manager after system downtime of one to three days. To resolve the issue, start the Apache server or reboot the manager.
  - The DHCP server does not verify that an IP address is available before assigning it. Ensure the endpoint address pool is separate from the IP addresses assigned to the managers.
  - An error may occur when attempting to disable the second Ethernet port on a satellite manager through the primary manager. To resolve the issue, manually disable the applicable interface on the satellite manager and then change the Eth2 setting.
  - Communication between satellite and primary managers is interrupted when the primary manager Eth1 port is set to DHCP. To resolve the issue, use a static route.
  - Bonded Mode does not operate when Disable Vertiv™ Avocent® HMX Advanced Manager UI over KVM Network is enabled. Do not use Bonded Mode when this option is enabled.
  - Devices previously replaced using a static IP address or DHCP Reservation may revert to DHCP. Reconfigure the applicable IP address.

© 2026 Vertiv Group Corp. All Rights Reserved.

- Network Time Protocol synchronization supports an IP address only. Domain names are not supported. After initiating synchronization, allow time for the primary manager clock to synchronize. The backup and satellite manager clocks then synchronize with the primary manager.
- A static IP address assigned to the Eth2 port of a backup or satellite manager does not operate if Eth2 on the primary manager is set to DHCP. Configure a static IP address on the primary manager.
- The secondary port of Vertiv™ Avocent® HMX5160 and HMX6150 series devices allows unsupported IP configuration settings. Any IP configuration applied to Port 2 has no effect.
- HMX IP address validation allows loopback and broadcast addresses to be configured.

- **On-Screen Display Issues**
  - Channel names can be truncated in the OSD. The OSD supports 25 characters, while the Vertiv™ Avocent® HMX Advanced Manager supports 45 characters. Some Japanese, Korean, and Chinese characters are treated as two or more characters.
  - Channel, Description, and Location fields may be truncated to maintain proper display alignment. Hover over the field to view the complete value.
  - Duplicate OSD hotkey combinations can be configured. When a duplicate combination conflicts with the Enable OSD hotkey, behavior may vary depending on the receiver model. Avoid using duplicate hotkey assignments.
  - The C-USB LAN list may appear blank after a user logs out and back into the OSD. Switch between the Home and Help tabs to refresh the display.
  - On DVI receivers, the cursor focus does not automatically move to the username field on the login page. Click inside the field before entering credentials.
  - Vertiv™ Avocent® HMX6500R-400 receivers do not support Windows key combinations as OSD hotkeys. Use supported key combinations only.
  - Vertiv™ Avocent® HMX6500R-400 receivers may not open the OSD when unsupported hotkey patterns are configured. Use Ctrl+Shift, Ctrl+Alt, or Shift+Alt combinations.
  - If an Auto Login user is deleted while Auto Login is enabled, OSD access may not be recoverable. Assign Auto Login to another user or disable Auto Login to restore normal operation.
- **Primary and Backup Manager Issues**
  - A backup server cannot be added to the primary manager if the backup server is powered on but is not connected to the same network as the primary manager during configuration. Connect the backup server to the same network and power-cycle it.
  - The "Backup/Satellite Manager has taken over" message does not appear on the active backup or satellite manager when Auto Login is enabled.
  - When a backup manager is deleted and later rejoins the primary manager, historical configuration data may be displayed incorrectly for its disabled second network port. Re-enable DHCP, save the configuration, then reconfigure and save the required network settings.
  - HTTPS access may continue in the same browser session after SSL is disabled because the browser still trusts the certificate. Opening the system from a different browser or IP address avoids this behavior.
  - Backup and satellite managers may not join or recover correctly if SSL is enabled during firmware uploads. Temporarily disable SSL before upgrading.
- **Receiver and Device Issues**
  - Untrusted devices manufactured before 2015 that do not contain a unique SSL certificate cannot be added to the system.
  - Fixed EDID Generic modes have no effect on Vertiv™ Avocent® HMX6200, HMX6210, and HMX8000 series devices. If selected through General Settings, the devices use the EDID information provided by the connected monitor.

© 2026 Vertiv Group Corp. All Rights Reserved.

- Replacing a Vertiv™ Avocent® HMX6200 series device with a Vertiv™ Avocent® HMX6200 or HMX6210 series device may require a manual channel reconnection when the replacement is not an identical model.

- **Remote Desktop Protocol Issues**
  - An RDP channel may continue to connect in single-head mode after the channel is changed to add a second display. Log out of the receiver and log in again for the change to take effect.
  - The syslog may display an SQL syntax error if an RDP name contains a quotation mark.
- **Satellite Manager Issues**
  - When adding a satellite manager to the primary manager, the satellite manager may remain on its link-local IP address. Reset the satellite manager.
  - A satellite manager may become unstable after a factory reset in Bonded Mode. Disable bonding before performing a factory reset.
  - A satellite manager may occasionally report a failed state after recovery and reconfiguration. Reboot the satellite manager.
  - After recovery and rejoining the primary manager, a satellite manager may incorrectly report a failed status.
- **Security Issues**
  - Secure HTTPS access requires the use of port 4433.
  - When SSL is enabled, some Kerberos help links may not be accessible unless port 4433 is manually included in the URL.
  - Enabling SSL from the Network Tools page may display an erroneous error message even though the operation completes successfully.
- **SNMP Issues**
  - The SNMP client may not display updated server status when retrieving information from a backup or satellite manager.
  - The SNMP Server Details table may not update the backup manager status when a satellite manager is active.
  - HTML VDI URLs may be displayed incorrectly in IP address fields in the web user interface, SNMP, and API responses.
- **Syslog Issues**
  - The syslog may display an SQL syntax error when an RDP name contains a quotation mark.
  - When Debug Level Timeout is configured, the syslog may display an unnecessary "Failed to check if job exists or not" message. This message does not affect system operation or performance.
- **Upgrade and Downgrade Issues**
  - A "Something went wrong" notification may be displayed during a successful upgrade or downgrade. The operation completes successfully and the message can be ignored.
  - Firmware uploads to primary, backup, or satellite managers may fail when SSL is enabled. Temporarily disable SSL before upgrading.
  - Do not select Reboot Before Upgrade when upgrading Vertiv™ Avocent® HMX6500R-400 receivers. If selected during multiple upgrades, only the first receiver may be upgraded.
- **USB Issues**
  - Receiver group USB settings and global USB settings are not fully independent. Changes made to receiver group USB settings may also modify the global USB configuration.
- **Virtual Desktop Infrastructure Issues**

© 2026 Vertiv Group Corp. All Rights Reserved.

- HTML VDI URLs may be displayed incorrectly in IP address fields in the web user interface, SNMP, and API responses.

- **Web User Interface Issues**
  - Previous IP address information may continue to be displayed temporarily during DHCP-to-static or static-to-DHCP transitions. Refresh the page.
  - Licensed Features information may not be displayed when the page is opened for the first time. Reopen the page or perform another interaction to refresh the data.
  - SMTP settings cannot be saved unless an Alert Email address is specified.
  - The video calibration page link for Vertiv™ Avocent® HMX5150T-VGA transmitters is not available from the interface and must be accessed directly.
  - HTTPS access requires specifying port 4433 in the URL.
  - The Save & Sync function does not work correctly from the scanned server tab after filters are removed from Directory Services.
  - Some error notifications may be displayed even when operations complete successfully. These messages are benign and can be ignored.

6. Minimum Supported Firmware Versions

MODEL	MINIMUM VERSION	LATEST VERSION
HMX6200R (DVI)	v5.2.52850	v5.3.53065
HMX6200T (DVI)	v5.2.52850	v5.3.53065
HMX6210T	v5.2.52850	v5.3.53065
HMX5100R	v5.2.52850	v5.3.53065
HMX5100T	v5.2.52850	v5.3.53065
HMX5200R	v5.2.52850	v5.3.53065
HMX5200T	v5.2.52850	v5.3.53065
HMX5150T-VGA	v4.11.1	v4.11.1
HMX8000R	v5.05	v8.07
HMX8000T	v5.05	v8.07
HMX6500R	1.1.0	v1.5
HMX5160T-DVID	4.10.1	v4.10.1
HMX6150T-HDMI	4.10.1	v4.10.1
HMX6150T-DP	4.10.1	v4.10.1
HMX6200R (DP)	v5.06	v8.06
HMX6200T (DP)	v5.06	v8.06
HMX6200T (HDMI)	v5.06	v8.06

© 2026 Vertiv Group Corp. All Rights Reserved.

7. Important Virtual Machine Information

In order to access a virtual machine via the Vertiv™ Avocent® HMX 6500 high performance KVM receiver, your system must be set up in a specific configuration where the receiver is connected to two separate networks. Then, through the Vertiv™ Avocent® HMX Advanced Manager software, you are able to configure the receiver, access hosts connected with Vertiv™ Avocent® HMX transmitters and access virtual machines running RDP hosts on a corporate network. For instructions on configuring access to a virtual machine, see the Vertiv™ Avocent® HMX 6500 High Performance KVM Receiver Configuring Access to a Virtual Machine Technical Note available on the product page at Vertiv.com.

© 2026 Vertiv Group Corp. All rights reserved. Vertivā and the Vertiv logo are trademarks or registered trademarks of Vertiv Group Corp. All other names and logos referred to are trade names, trademarks or registered trademarks of their respective owners. While every precaution has been taken to ensure accuracy and completeness here, Vertiv Group Corp. assumes no responsibility, and disclaims all liability, for damages resulting from use of this information or for any errors or omissions.