

# Vertiv™ Avocent® HMX Advanced Manager

## Release Notes

VERSION 5.11, SEPTEMBER 2024

### Release Notes Section Outline

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

### 1. Upgrade Instructions

**NOTE: 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 5.3 or higher.
- Ensure your Vertiv™ Avocent® HMX 5100, 5200, 6200 and 6210 extender firmware is version 4.9 or higher. (Version 4.9 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.

## 2. Package Version Information

APPLIANCE/PRODUCT	IMAGE/CODE VERSION
Vertiv™ Avocent® HMX Advanced Manager	V5.11

## 3. Minimum Supported Firmware Versions

MODEL	MINIMUM VERSION	LATEST VERSION
HMX6200R (DVI)	v5.0.47185	v5.2.52850
HMX6200T (DVI)	v5.0.47185	v5.2.52850
HMX6210T	v5.0.47185	v5.2.52850
HMX5100R	v5.0.47185	v5.2.52850
HMX5100T	v5.0.47185	v5.2.52850
HMX5200R	v5.0.47185	v5.2.52850
HMX5200T	v5.0.47185	v5.2.52850
HMX5150T-VGA	v4.9.05	v4.11.1
HMX8000R	v5.05	v8.03
HMX8000T	v5.05	v8.03
HMX6500R	1.1.0	v1.3.1.7
HMX5160T-DVID	4.08.40000	v4.10.1
HMX6150T-HDMI	4.08.40000	v4.10.1
HMX6150T-DP	4.08.40000	v4.10.1
HMX6200R (DP)	v5.02	v8.03
HMX6200T (DP)	v5.02	v8.03
HMX6200T (HDMI)	v5.02	v8.03

## 4. Features and Enhancements

This version of the Vertiv™ Avocent® HMX Advanced Manager introduces the following features and maintenance improvements for the new hardware platform (HMXAMGR24G2) and the HMXAMGR24-XXX, which is now EOL.

- User Authentication:
  - Added support for GSSAPI for Kerberos to work in conjunction with the LDAP/Open LDAP services.

## 5. Resolved Issues

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

- Enable filtering of connection log for the “Anon user.”
- The Vertiv™ Avocent® HMX Advanced Manager web UI and OSD to show “Permission denied” error if the user tries to log in without permission.
- Default for 2FA should be set to disable when the user enables the Password field.
- Channel name is missing on the OSD for the VMware Horizon client.
- The Vertiv™ Avocent® HMX Advanced Manager web UI should not allow private mode when video heads at the receiver are mirrored.
- On deleting a channel through the API, an event log should be generated.
- Disable a password from being added in Anon mode.
- Connected channel to be treated as last channel after OSD logout.
- Issues found in previous releases and during test.
- Security enhancement for Kerberos over Beta release. (Not in any official release.)
- API Limit set to 40 requests a second.
- LDAP: When an OU to be imported has a group with users but no users in the OU itself, the Vertiv™ Avocent® HMX Advanced Manager cannot see the users within the group.
- Multiple issues have been seen in Preset operation through the API.
- "logout\_device" API command does not work when the receiver is not connected in session.
- Sessions are connected with wrong connection mode through "connect\_channel" API.
- Transparent USB set from the transmitter channel fails to respond in the "get\_channels" API.
- The "get\_devices" API response gives the wrong device information.
- AutoLogin to be supported on all Vertiv™ Avocent® HMX devices.
- The API document has been updated for the newer models.
- Inconsistency in restoring the backup manager.
- DHCP address has not been assigned on Eth2 if the network connection is not present during configuration.
- No validation check is applied to the channel/receiver ID in API verification.
- "Schedule Auto Delete Logs" does not get applied after setting from the Backup Vertiv™ Avocent® HMX Advanced Manager.
- Unable to filter the connection log for the Video Multicast Status.
- SNMP must work on the Backup Vertiv™ Avocent® HMX Advanced Manager when it's not acting. Endpoint device status is not available on the Backup/Satellite manager.
- Pop-up notification required for any setting that requires an endpoint to reboot.
- 2FA Five failed OTP attempts on OSD suspends the Admin account, which locks the user out of the Vertiv™ Avocent® HMX Advanced Manager.
- Unable to see the multi-user information from the remote OSD.
- Vulnerability related to Vertiv™ Avocent® HMX Advanced Manager login URL has been found in testing.
- The Auto Login feature continues working even if the license has expired.

- Unexpected error appears when auto logout is triggered.
- IP address of all interfaces is seen in the Audio/Video broadcast ip list.
- Response of field favorite in get channel API response is printing incorrectly.
- Improvement to the "Disabled all" button on the statistics page of the Vertiv™ Avocent® HMX Advanced Manager dashboard.
- Improvement in behavior with a suspended user from the OSD.
- XSS Vulnerability found on the NTP server page.
- The user is unable to add a new classless route after removing all existing routes until the user saves or cancels the configuration.
- No message seen in syslogs when user "Save & Sync" DS Users from preview page.
- Session is not disconnecting even if the user deletes the user group in between the session.
- Presets are always present in the output list when the user filters through location field.
- Directory server name should reflect while hovering over the DS icon on the user group page.
- Connection modes are becoming misaligned on the OSD when the channel description or location length is long.
- The web UI shows an error when a session is disconnected while the device is rebooting from the Vertiv™ Avocent® HMX Advanced Manager.
- The session is not overridden from the Vertiv™ Avocent® HMX Advanced Manager web UI with a different admin user.
- Changing the multicast IP in the Vertiv™ Avocent® HMX Advanced Manager network settings triggers "All VDI type failed" errors in the syslog.
- An extra single quotation mark (") is visible on the Backup configuration page.
- The Vertiv™ Avocent® HMX6500R receiver experiences loss of audio and video when connecting to a channel without user permission.
- No validation check is available for the cluster password field is presented on the Vertiv™ Avocent® HMX Advanced Manager.
- The remote OSD gets closed after accessing the server credential window.
- Limit the number of API Requests in a given time to prevent a user from committing a Denial of Service attack on themselves.

## 6. Known Issues

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

AREA	ISSUE DESCRIPTION	WORKAROUND
Active Directory (AD)	Users are unable to filter the Active Directory server fetched user from the advanced manager when DS includes the plus (+) symbol in its name.	No workaround at this time.
	Downgrading from version 5.10 to 5.9 or lower will cause AD server settings to be lost.	No workaround. The server settings will need to be reapplied.
Application Programming Interface (API)	Preview button activation also performs a sync with the Active Directory server.	No workaround at this time.
	The get_presets API fails to update the preset count and details for the exclusive mode preset.	Enable all connection modes on the preset.
	The API remains active when web access is blocked on the KVM network.	No workaround at this time.
Authentication	After performing the logout device API command in the Vertiv™ Avocent® HMX6200R/6500R receiver OSD, the user is successfully	If the user issues the device_logout API command while the receiver is showing the OSD, it does not

AREA	ISSUE DESCRIPTION	WORKAROUND
Authentication (continued)	logged out of the OSD. However, if the OSD is still displayed at the time, the OSD suggests that they are still logged in.	return to the login page automatically. Refresh the page.
	The auto-logout feature should not be supported for the anonymous user.	Observation. The OSD gets logout due to the auto-logout timer expiring for the anonymous user.
	Kerberos settings are not updating correctly if edited after being saved.	To change the settings, disable the Kerberos feature, then re-enable and re-enter the Kerberos settings.
	Kerberos settings are not persistent if disabled and then enabled.	Turn the settings off/on, then re-enter the Kerberos settings.
	Does enabled 2FA affect the Auto Login feature?	No. The user can still use the hotkeys to switch channels without logging into the OSD.
	2FA is suspended when the backup manager is acting as primary.	No workaround at this time.
	Setting a password for an anonymous user stops NO login required from working.	No workaround at this time.
	The OSD 2FA verification page is only displayed in English and does not use the chosen locale.	Observation. This issue will be resolved in the next release.
Network	The DHCP server does NOT check if an IP address is available before issuing it.	To allow for the replacement of Vertiv™ Avocent® HMX Advanced Manager servers, ensure the pool of IP addresses for the endpoints are separated away from the IP addresses for the manager.
	An error occurs when attempting to disable the second Ethernet port on the satellite manager via the primary manager.	First, manually take down the eth1 interface port on the satellite manager, then revert the eth2 interface setting for the satellite manager.
	Communication between the satellite and primary managers stops when the eth1 port is set to DHCP on the primary manager.	Use a static route, which is available on the primary manager's web UI.
	Classless routes from the Graphical User Interface (GUI) get cleared if the user leaves the second row empty.	DO NOT save an empty row.
	Bonded Mode does not work when the "Disable Vertiv Avocent Advanced HMX Manager UI over KVM Network" option is enabled.	Bonded mode should not be used when the "Disable Vertiv Avocent Advanced HMX Manager UI over KVM Network" option is enabled.
Upgrades	Occasionally, the Hostname and DNS Domain do not populate when upgrading from Vertiv™ Avocent® HMX Advanced Manager firmware v4.12 to v5.5.	Prior to performing the update, make note of the settings in case they are not transferred.
	Reboots introduce an issue on the Vertiv™ Avocent® HMX 6500R receiver, where if multiple upgrades are in progress, only the first unit will be upgraded.	Do not select the option to reboot before upgrade.

AREA	ISSUE DESCRIPTION	WORKAROUND
Upgrades (continued)	Due to incompatibility in versions of underlying OS and DB between firmware versions 4 and 5, not all information is transferred between the two versions.	<p>Make note of the following settings before you upgrade to the new version:</p> <ul style="list-style-type: none"> <li>• Active Directory (all settings)</li> <li>• Email (Domain/IP, Username, Password)</li> <li>• NTP (NTP Key)</li> <li>• SNMP (Authentication &amp; Privacy Password)</li> <li>• RDP (Passwords)</li> </ul>
	The RDP passwords are lost after upgrading from firmware v4 to v5.	Unfortunately, due to the nature of the new version, there is no workaround.
	After upgrading the primary manager from V5.9 to V5.10, a backup can remain active.	Reboot the backup manager.
On-Screen Display (OSD)	Channel names have been truncated in the OSD.	<p>The OSD can only support 25 characters, whereas in the Vertiv™ Avocent® HMX Advanced Manager menu 45 characters are allowed.</p> <p><b>NOTE: Some Japanese, Korean and Chinese characters are considered as two or more characters.</b></p>
	Channel location information can sometimes be displayed under the Description column in the OSD of the Vertiv™ Avocent® HMX6200DP/8000 receivers.	No workaround at this time.
Primary/Backup Unit	The backup server will not be added to the primary manager if it's powered on and not on the same network as the primary during configuration.	Power cycle the backup manager while on the same network as the primary.
Satellite Unit	Occasionally, when adding the satellite manager to the primary, the satellite manager gets stuck on the link local IP address.	Reset the satellite manager.
Security	Secure SSL access has moved to <b>https://&lt;appliance.IP&gt;:4433</b>	
SMTP	SMTP function is inoperable after upgrading from V5.8 to V5.10. This is a rare occurrence triggered by upgrading and downgrading from various versions.	Manually update the SMTP IP address in the mail configuration page of the Vertiv™ Avocent® HMX Advanced Manager web UI. Access the SMTP config file located at "/etc/ssmtp/ssmtp.conf" and edit the IP address accordingly. After completing these steps, users should be able to send mail successfully.
SNMP	SNMP only works on the primary manager or Acting primary in firmware v5.5 and above.	This issue will be considered for change in a future release.
	SnmPB client fails to display updated server status when fetching from the backup or satellite manager.	No workaround at this time. This issue will be resolved in the next release.

AREA	ISSUE DESCRIPTION	WORKAROUND
Statistics	The device statistics cannot be re-enabled after using “Disable All” feature.	If the “Disable All” feature is used to disabled the statistics for the endpoints, reload the page to enable the statistics on an endpoint immediately after.
Syslog	The syslog shows an SQL syntax error in the RDP name. It contains a quotation mark.	Observation. This issue will be resolved in a future release.
Video	In the General setting for Fixed EDID, Generic modes have no effect on either the Vertiv™ Avocent® HMX 8000 or 6200 DP extenders.	The modes do not appear in the specific pages for each transmitter, but if selected via the General setting, the Vertiv™ Avocent® HMX 8000/6200 DP series devices will work with the connected monitors EDID.
	The RDP channel still connects as single-head after modifying the channel to add a second head.	For the change to take effect in the Vertiv™ Avocent® HMX Advanced Manager, you must log out of the Vertiv™ Avocent® HMX6500R receiver, then log back in again.
Virtual Desktop Infrastructure (VDI)	The Configure channel allows VNC, SSH and HTML channels to select two heads, despite only one head (monitor) being supported for these modes.	Ensure video 2 is set to OFF.
	The dual head RDP sessions are broken on version 10 and 11 of the Vertiv™ Avocent® HMX6500R receiver.	This issue will be resolved in the next release.
	The HDMI VDI URL/IP is missing from the Transmitters list.	Observation. This issue will be resolved in the next release.
Web User Interface (UI)	When using the Replace function for the Vertiv™ Avocent® HMX 5000/6000 extender system devices with the Vertiv™ Avocent® HMX 6200 DP extenders, the channel does not reconnect.	A manual re-connect must be initiated. This only happens when it is not directly a like-for-like model replacement.

## 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](https://www.vertiv.com).