

---

# The Avocent® HMX High Performance KVM Extender System, Next Generation, and the Avocent® HMX Advanced Manager Release Notes Version 4.4 April 12, 2017

---

This document outlines:

1. Upgrade Instructions
2. Package Version Information
3. Features, Enhancements and Resolved Issues (By Version)
4. Known Issues

---

## 1. Upgrade Instructions

---

**NOTE:** For additional product information, please refer to the Avocent® HMX High Performance KVM Extender System Next Generation Installer/User Guide and the Avocent® HMX Advanced Manager Installer/User Guide.

Transmitters and receivers are flash upgradable at any time to ensure that your system is running the most current version available. If your system is running the most current firmware version and is managed by the Avocent® HMX Advanced Manager software, then that same version must be used across all units in your system. Firmware versions can be mixed in configurations not using the Advanced Manager software, but it is always recommended to use the most current version. The Advanced Manager software On-Board Web Interface (OBWI) provides a central location for you to perform a firmware upgrade on any linked unit.

### Pre-requisites

If the Avocent® HMX Advanced Manager software is upgraded to version 4.4, then the connected transmitters and receivers (endpoints) must also be upgraded to version 4.4 in order to maintain compatibility.

If your HMX Advanced Manager software server is being used in a backup configuration, then you must upgrade all of the HMX Advanced Manager software servers before upgrading the transmitters and receivers. See the Avocent® HMX Advanced Manager Installer/User Guide for additional information.

If you are upgrading from version 4.0, be sure there are enough addresses in your IP address pool to allocate to all required ports.

**NOTE:** Teaming devices requires two IP addresses each.

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

1. In the user interface (OBWI) of the 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 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 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 interface and automatically logged in. When the primary server becomes available, you are redirected back to that web interface.

8. If you have an 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 HMX Advanced Manager software server and confirm both servers are upgraded and synchronized.

**To upgrade the firmware on the transmitters and receivers:**

1. In the user interface (OBWI) of the HMX Advanced Manager server, select *Dashboard- Updates*.
2. In the Upload new TX/RX Firmware section, click *Browse*.
3. Select the firmware file and click *Open*.
4. Click *Upload*.
5. For each transmitter and receiver to be upgraded, select the corresponding checkbox.  
 -or-  
 Select the Upgrade All checkbox.
6. Click *Upgrade Selected Transmitters*.  
 -or-  
 Click *Upgrade Selected Receivers*.

---



---

## 2. Package Version Information

---



---

Appliance/Product	Image/Code Version
Avocent® HMX High Performance KVM Extender System Transmitters and Receivers	V4.4.40349
Avocent® HMX Advanced Manager	V4.4.40323

---

---

### 3. Features, Enhancements and Resolved Issues (By Version)

---

---

This section highlights features and/or enhancements available with each version/update of the Avocent® HMX extender system and/or the Avocent® HMX Advanced Manager software.

#### Version 4.4 (This Release)

This release covers version 4.4.40349 for the Avocent® HMX 5100, 5200, and 6200 transmitters and receivers as well as the HMX 6210 transmitter. This release also covers version 4.4.40323 of the Avocent® HMX Advanced Manager software.

The 4.4 code release of the extender system and the Advanced Manager software significantly increases the longevity of the Advanced Manager software server when used in installations in excess of 2,000 transmitter/receiver endpoints and multiple fast-switching applications (<150 per minute). Regardless of the size and complexity of your installation, it is recommended that you upgrade to the latest code to take full advantage of the increased resilience provided.

#### Implemented After Version 4.4.39920 of the HMX Advanced Manager Software Code

- System logs are now rotated to prevent the disc from becoming full.
- To remedy the issue of the admin site index page taking a long time to load, the number of active connections shown has been reduced. Only five active connections are now shown.
- On the Settings/General page in the web interface, there is a new setting that allows you to disable password recovery.
- On the global receivers page in the web interface, there are two new settings that allow you to enable/disable OSD and connection hotkeys. If you disable OSD hotkeys, connection hotkeys cannot be enabled. However, if the OSD hotkeys are enabled, connection hotkeys can either be enabled or disabled.
- Previously, if the primary server had a record of its old CA certificate, it was not possible to overwrite this certificate with the new certificate from the new primary. This has been resolved so that, after being fully reset, it is now possible to add the Avocent® HMX Advanced Manager software server back into the cluster.
- In earlier releases, when the HMX Advanced Manager software server was deleted from the cluster, the HMX extender system transmitter/receiver (endpoint) certificates were no longer valid because they were issued by the Advanced Manager software server (that is now deleted). This would disconnect the HMX extender system transmitters/receivers. Now, the HMX extender system transmitters/receivers automatically rekey new certificates before the cluster table gets updated.

#### Implemented After Version 4.3.38918 of the HMX Transmitter/Receiver Code

- Support was added for the Iiyama Prolite T2236MSC-B2-Ten-point touch screen.
- An issue was resolved where, after a large number of channel changes for a USB device, a memory leak occurred, the device would not be recognized and a *Disconnect and reconnect the transmitter* error message appeared.
- Support for a 3M-Microtouch screen was previously intermittent. This has been corrected.
- Hub port allocation has been enhanced. Previously, when switching multiple devices, one would fail to enumerate if the hub size was set to seven devices. This is no longer an issue.

- In previous releases, a new device could not be added if ports were reserved but unused. For example, if one of the receiver USB ports was reserved but not used, the reserved port was being connected to the USB host. This would fill up the port list, so then new devices could not be added. Now, an unused reserved port is not included in the device list.
- An erroneous connection failure has been corrected. Previously, some devices could fail after switching when you switched with more than eight USB devices.

**Implemented After Version 4.2**

- The audio source IP address is now included in the IGMPv3 report.
- Unmerged HTML templates are no longer accessible.
- EDIDs are now read correctly when changing from dual-link to single-link video resolutions with an HPZR 30W monitor.
- Previously, after upgrading a backup server that was promoted as the primary server, the transmitter and receiver endpoints were reported as offline. This has been resolved and they are no longer reported as offline.
- A new API command has been added (Create\_Temp\_channel) to the API in order to add a temporary channel that is automatically deleted after two hours. All API users have access to this channel, and because it is created without permissions, it can be used in an On-Screen Display (OSD) or the OBWI.

**NOTE:** If you assign permissions to the temporary channel within two hours, it will not be automatically deleted and becomes a permanent channel.

- In an earlier release, Active Directory (AD) users were not being added to AD groups when using the preview function of the AD page. This has been resolved; the preview function now works the same as the save and sync functions.
- The update\_device API method has been added as a way to call and update description and location fields in the user interface.
- An HP KUS1205 card reader is now fully supported.

=====  
**4. Known issues**  
 =====

Issue	Workaround
It may not be possible to upload an upgrade file if you have large backup files stored on the Advanced Manager software server.	Delete any unnecessary backup files to clear space and allow the upgrade.
When using multi-subnet mode, you cannot add the factory reset primary server back into a cluster.	If you must add a replacement primary server into a cluster, ensure it is "factory fresh."
After upgrading a backup HMX Advanced Manager software server with Require Authentication settings enabled, the backup is in an unconfigured and inactive state.	To recover, reset the backup Manager server and add it back to the cluster. To avoid this issue, ensure the Require Authentication setting is set to No and there is no cluster password in use when upgrading the HMX Advanced Manager software server.

Issue	Workaround
The Avocent® HMX Advanced Manager software server does not save “\” in the NTP keys.	Do not use \ in the NTP keys.
It is possible to set the multicast IP bases to addresses reserved for network protocols which could potentially flood the network.	Do not set the multicast IP base to the following addresses: 224.0.0.0, 225.0.0.0, 226.0.0.0, 224.128.0.0 or 237.0.0.0
The maximum number of AD users that can be members of an AD group is 1499. If there are 1500 or more users in a group, the group is returned as empty.	None at this time.
When the OSD is called up on video resolutions of 800 x 600 or below, it is not possible to use the scroll bars to move around the menu.	None at this time.

*Avocent and the Avocent logo are trademarks or service marks of Avocent Corporation. All other marks are the intellectual property of their respective owners. This document may contain confidential and/or proprietary information of Avocent Corporation, and its receipt or possession does not convey any right to reproduce, disclose its contents, or to manufacture or sell anything that it may describe. Reproduction, disclosure, or use without specific authorization from Avocent Corporation is strictly prohibited. ©2017 Avocent Corporation. All rights reserved.*