



Avocent[®] HMX Advanced Manager

Network Recommendations and Troubleshooting Technical Note

The information contained in this document is subject to change without notice and may not be suitable for all applications. While every precaution has been taken to ensure the accuracy and completeness of this document, Vertiv assumes no responsibility and disclaims all liability for damages resulting from use of this information or for any errors or omissions. Refer to other local practices or building codes as applicable for the correct methods, tools, and materials to be used in performing procedures not specifically described in this document.

The products covered by this instruction manual are manufactured and/or sold by Vertiv. This document is the property of Vertiv and contains confidential and proprietary information owned by Vertiv. Any copying, use or disclosure of it without the written permission of Vertiv is strictly prohibited.

Names of companies and products are trademarks or registered trademarks of the respective companies. Any questions regarding usage of trademark names should be directed to the original manufacturer.

TABLE OF CONTENTS

1 General Overview	1
1.1 Prerequisites	1
2 Configuration	2
2.1 Initial Setup	2
2.2 Subnet Operations	2
2.3 Protocols and Ports	6
2.3.1 TCP	6
2.3.2 UDP	7
2.3.3 Device communication	7
2.4 Video Settings	7
2.4.1 Helpful terms to know	7
2.4.2 Customizations	7
2.5 Manager Configuration Reset	8
2.6 Manager Configuration Upgrade	8
2.7 Backup Manager Server	10
Appendices	11
Appendix A: Network Switch Recommendations	11
Appendix B: Troubleshooting	19
Vertiv™ Avocent® HMX Advanced Manager G2 Server Quick Installation Guide	27
Vertiv™ Avocent® HMX Advanced Manager Installer/User Guide	29

This page intentionally left blank

1 General Overview

The Vertiv™ Avocent® HMX Advanced Manager is a secure, web browser-based, centralized enterprise management solution that provides competitive flexibility in the distribution of high-performance computing power. Requiring only a single run of cable, the HMX Advanced Manager reliably transfers high-resolution DVI video, audio, RS232 serial and four USB streams. Additionally, this product offers a streamlined web User Interface (UI) to manage all administration, access control, monitoring and firmware upgrades across the Vertiv™ Avocent® HMX IP KVM extender system.

For optimal performance, the manager servers must be structured and configured properly. This guide highlights key product elements and provides suggestions for successful implementation and troubleshooting solutions. It is a supplemental guide to the Vertiv™ Avocent® HMX Advanced Manager G2 Server Quick Installation Guide and the Vertiv™ Avocent® HMX Advanced Manager Installer/User Guide, where additional information about product installation or features can be found.

1.1 Prerequisites

At this point, you should have already completed the installation instructions outlined in the Vertiv™ Avocent® HMX Advanced Manager G2 Server Quick Installation Guide and the Vertiv™ Avocent® HMX Advanced Manager Installer/User Guide. For your convenience, we have provided direct links to these documents within each applicable section of this guide. Please ensure that you meet the following requirements for each server type before continuing.

NOTE: All servers in your system must use the same firmware version and endpoint licenses.

Table 1.1 Prerequisites

Server Role	Description	Prerequisite(s)
Primary	The main server	<ul style="list-style-type: none"> Select <i>No</i> for the Require Authentication option. The primary server automatically assigns the backup server with the next available IP address, so ensure your primary server does not use the last IP address in a range. Ensure the HMX Advanced Manager server has a 1GB network connection. <p>NOTE: To directly connect to a HMX Advanced Manager G2 server, a 1GB network interface is required.</p>
Backup	The secondary server that shares the same subnet as the primary manager for redundancy	<ul style="list-style-type: none"> Perform a factory reset on the backup server before adding it to the network. <p>NOTE: To add another license, connect the primary and backup servers, reboot the system, then complete a second factory reset to the backup. The second reset is critical to properly adding the backup manager.</p>
Satellite	A backup server on a different subnet than the primary	<ul style="list-style-type: none"> Ensure the satellite server is using firmware version 4.2.37829 or later. To add a satellite server, enable multiple subnet operations on the primary server. Perform a factory reset on the satellite server before adding it to the network. When adding a satellite server, ensure the IP address assigned to the server is included in the DHCP option 125.

2 Configuration

The following sections highlight the available configuration options, key communication protocols and specific system customizations that can be completed after configuring your manager server.

2.1 Initial Setup

The HMX Advanced Manager server uses zero-config networking. When it is in an “out of the box” state, the manager server reflects a blank LCD screen and is ready to be configured.

Figure 2.1 HMX Advanced Manager “Out Of The Box” State



After configuration, the LCD screen displays a default IP address. This address must be changed to perform any other actions or navigate to any other screens. To configure your manager server and change your IP address, see [Installation and Configuration](#) in the installer/user guide.

2.2 Subnet Operations

Once your primary manager server is configured, you must decide if you will need multiple subnets. Each subnet is responsible for managing a group of IP addresses. When networks become too large and complex, the abundance of IP addresses causes latency and reduces system performance. The HMX Advanced Manager provides the option to operate across multiple subnets, which improves routing efficiency by allowing for the central management of IP addresses within a scalable network.

NOTE: The multiple subnet option is available on HMX Advanced Manager firmware version 4.1 and later.

Each device in a network automatically acquires an IP address from a DHCP server. This server streamlines the process of connecting devices to the internet. If you are operating in a single subnet, the manager can act as the internal DHCP server. However, if you are operating across multiple subnets, you must use an external DHCP server.

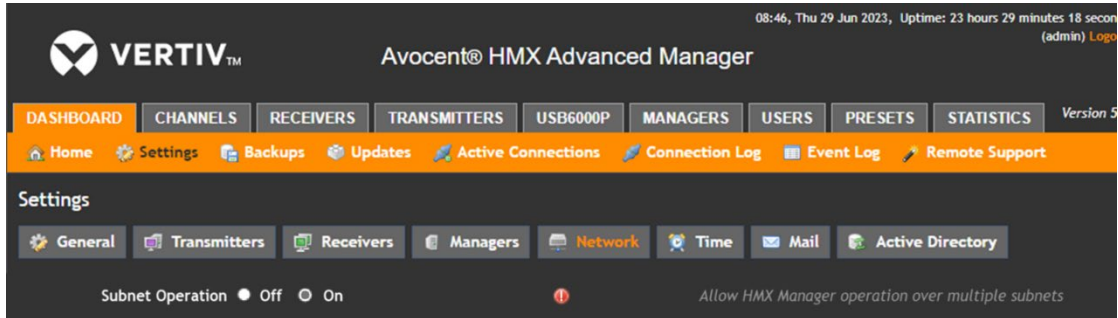


CAUTION: If you are not configuring option 125, do not enable subnet operations. This will disable DHCP and require you to manually set up IP addresses for every device in the network.

To configure subnet operations:

1. Click *Dashboard – Settings – Network*.

Figure 2.2 Subnet Operations



2. To operate on a single subnet and enable the internal DHCP server, click the Off radio button.

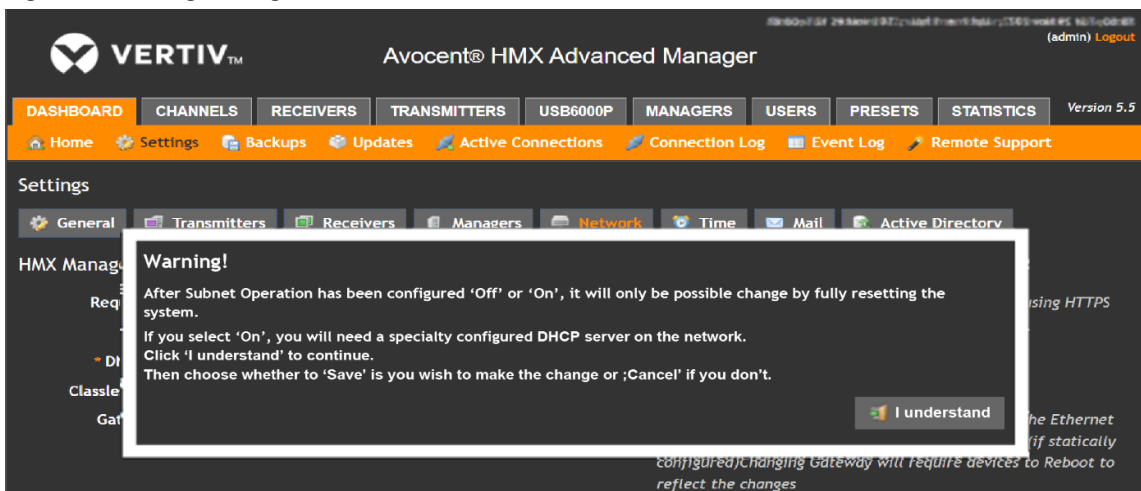
-or-

To operate across multiple subnets, click the On radio button.

NOTE: If you click the On radio button, you are responsible for setting up your corporate DHCP infrastructure to support the Vertiv™ Avocent® HMX High Performance KVM extender system. Contact Vertiv Technical Support for more information on using a Vertiv™ Avocent® HMX High Performance extender system in a multi-network environment.

3. After your selection, review the warning message and click *I understand*.

Figure 2.3 Warning Message



4. Click Save.

5. Under the Ethernet Port 1 heading, enter the HMX Advanced Manager IP address, netmask and the DNS server IP addresses.

Figure 2.4 Ethernet Port Headings



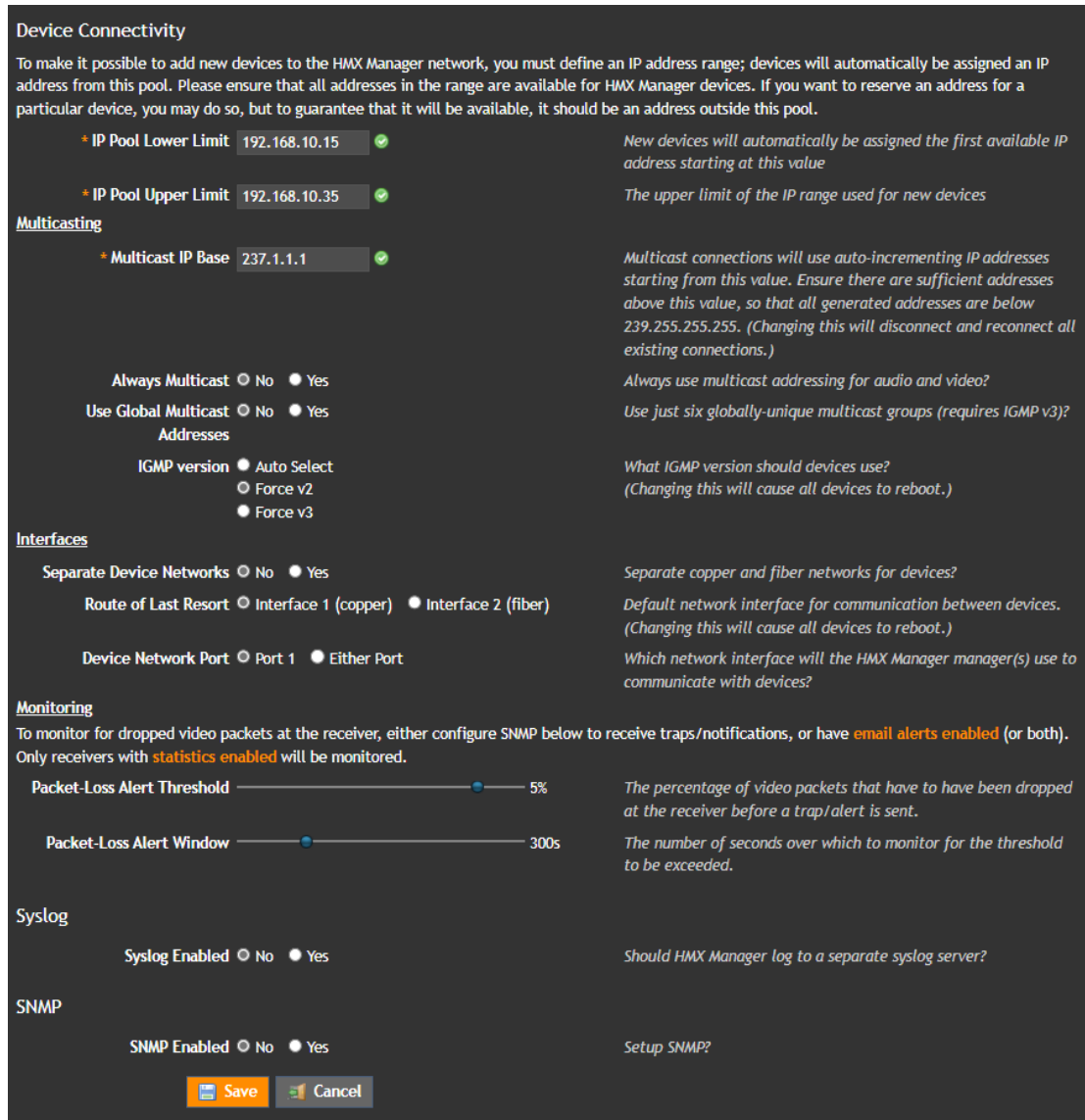
6. Under the Ethernet Port 2 heading, leave Ethernet Port 2 on the default No setting if you are operating on a single subnet.

-or-

If you are operating across multiple subnets and wish to assign corporate access, select the DHCP radio button. After you save your settings, the corporate access IP address is automatically assigned.

- Under the Device Connectivity heading, enter the IP Pool Lower Limit and IP Pool Upper Limit. It is recommended that you leave all other options on the default setting.

Figure 2.5 Device Connectivity Heading



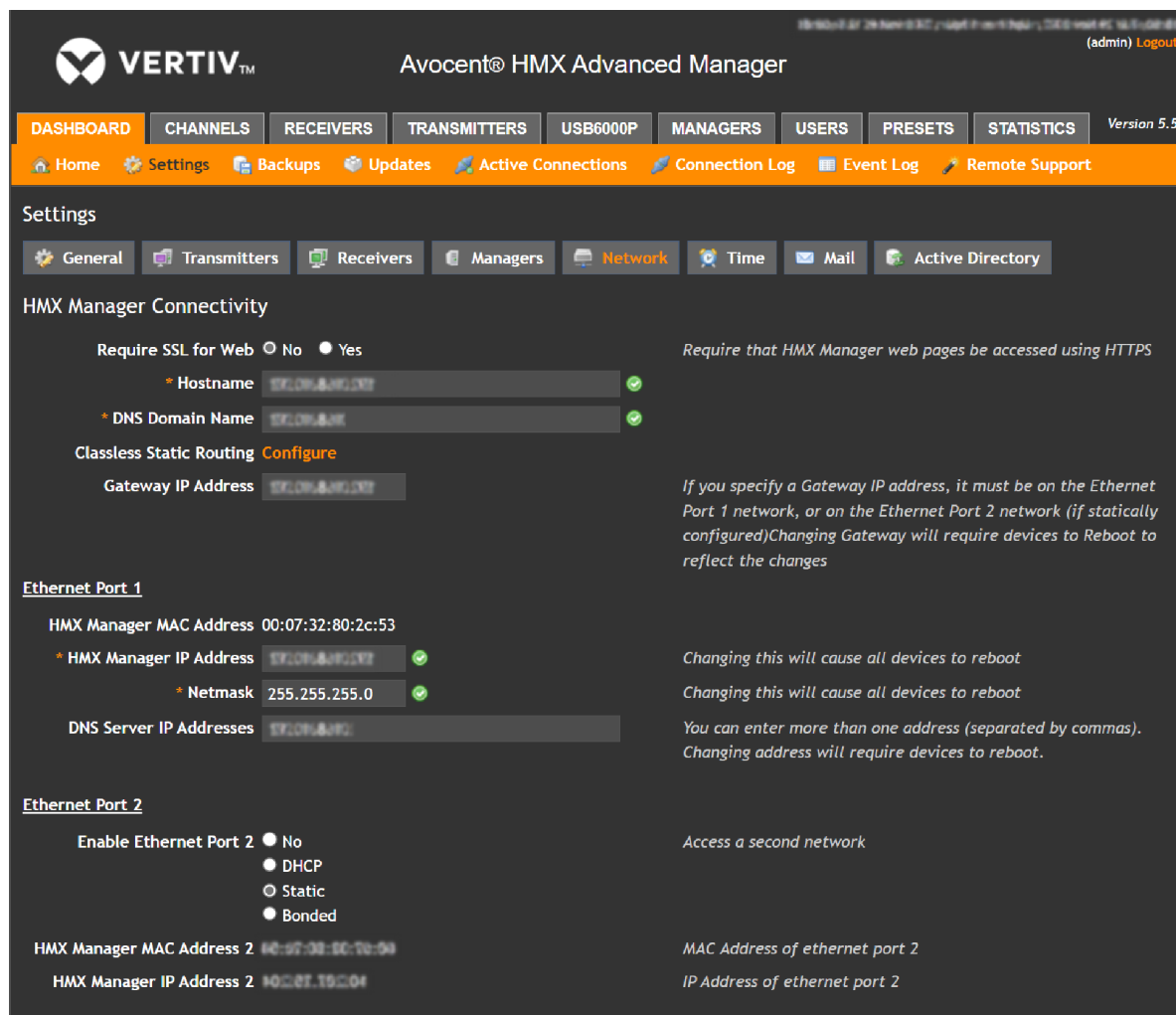
- Click Save. After saving your changes, it takes approximately 40 seconds for the new IP settings to take effect.

Figure 2.6 Saving Network Settings



After configuring and saving your subnet operations, your screen should look similar to the following figure.

Figure 2.7 Configured Network Settings



2.3 Protocols and Ports

With your HMX Advanced Manager now configured, you must ensure that your ports are open to receive data transmissions. This section describes the critical protocols each port type must follow for the successful transmission of data.

Sending high-resolution data across a GB Ethernet network requires the communication protocols outlined in the Internet Protocol Suite. This model consists of four layers: the Application Layer, Transport Layer, Internet Layer, and Link Layer. Each layer maintains its own set of protocols to achieve different tasks. Data transportation happens at the Transport Layer, and two protocols exist within this layer: Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).

2.3.1 TCP

TCP is an internetworking standard that provides a reliable data delivery route between hosts or devices. To accomplish this, TCP employs flow control to regulate data flow for the receiver, error detection to locate and replace corrupted data packets, and congestion control to avoid flooding a busy network. This process is time-consuming, resulting in connection latency issues. Therefore, HMX Advanced Manager servers use TCP to manage less time-sensitive data links, such as RS232 serial and USB connections.

2.3.2 UDP

UDP operates similarly to TCP except it does not check for any errors within the stream of transmitted data. While this expedites the transmission process, data packets are more likely to be lost. Because UDP prioritizes speed rather than error detection, it is ideal for video and audio data streams.

NOTE: UDP is not recommended for data streams with important control signals.

2.3.3 Device communication

The HMX Advanced Manager server has various ports responsible for the successful transmission of data. To communicate across a firewall and receive data streams, HMX Advanced Manager servers must have the following ports open and operating under the appropriate communication protocol.

Table 2.1 Ports and Protocols

Port	Data Type	Protocol
3030	RS232 serial	TCP
3040 to 3050	USB	TCP
3000	Control	TCP
1237	Video	UDP
3020	Audio	UDP

2.4 Video Settings

After ensuring your manager server can successfully communicate with other devices within the network, you may consider altering your video data transmission settings on the Vertiv™ Avocent® HMX transmitter to better fit your needs. When correctly configured, these customizations can increase data efficiency.

2.4.1 Helpful terms to know

For your reference, a list of helpful terms has been provided.

Anti-Dither: Anti-dither solves increased bandwidth issues caused by dithering techniques used on some computers. For transmitters, the anti-dither feature should be enabled.

Color Depth: This is the number of bits used to indicate the color of each pixel. By default, the maximum value is 24 bits. At the cost of video color reproduction, you can minimize the value and significantly reduce bandwidth consumption.

Peak Bandwidth Limiter: Reducing this setting prevents the transmitter from overusing network capacity by placing a tighter limit on the permissible amount of data.

Frame Skipping: Skipping frames reduces overall bandwidth consumption, specifically for video sources with infrequent updates or those with frequent updates that do not require high fidelity.

Background Refresh: The transmitter only sends portions of a video image that have been changed. To ensure the best user experience, the transmitter sends the whole video image in the background at a lower frame rate. The Background Refresh feature configures or disables the number of frames of video data. By default, a full frame is sent in the background every 32 frames.

2.4.2 Customizations

If you wish to customize your video settings, see the following procedure.

To access Video Settings:

1. Navigate to the *Transmitters* tab within the manager software.
2. Locate the manager server you wish to configure and select the Configure icon (the pencil).
3. On the Transmitters – Configure Transmitter screen, scroll down until the Video Settings heading appears. Under this heading, you can customize the individual settings as desired.

NOTE: It is recommended that you change settings one at a time to attribute positive and negative results to the appropriate control.

The following table provides general recommendations for improving the transmission of video data.

Table 2.2 Video Settings Customizations

Action	Result
For the Anti-Dither option, select USE GLOBAL SETTING.	Improves color quality.
Ensure Frame Skipping is on a low percentage, then reduce the Peak Bandwidth Limiter and Color Depth.	Maintains image quality for frequently transmitted video images.
Increase Background Refresh and/or increase Frame Skipping.	Resolves static display patterns.
Reduce Background Refresh to every 64 frames.	Improves overall system performance for high-traffic networks.

For more information about Transmitters settings, see [Transmitters tab](#) in the installer/user guide.

2.5 Manager Configuration Reset

Resetting the manager configuration reverts the software back to its initial configuration, original factory setting or to the latest firmware version. This process removes all devices, channels, presets, users, groups, backups, logs and uploaded firmware files. For instructions on resetting the manager configuration, see [Updates](#) in the installer/user guide.

2.6 Manager Software Upgrade

The upgrade software function is used to upgrade the manager server to the latest version.



CAUTION: It can take up to seven minutes to upgrade to firmware version 5.3 or later on a Generation 1 HMX Advanced Manager. Do not reboot or power cycle the server during the upgrade as that could cause damage to the OS (same as a BIOS upgrade interruption).

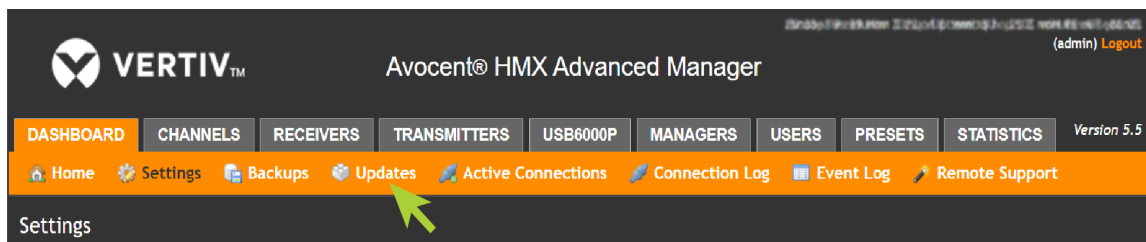
To upgrade the manager software:

1. Download the appropriate firmware file from Vertiv.com: [Avocent HMX Advanced Manager Software Downloads \(vertiv.com\)](#)

NOTE: If the firmware version you need is unavailable at Vertiv.com, contact Vertiv Technical Support. Prior to uploading the firmware file, ensure you have unzipped (extracted) the file.

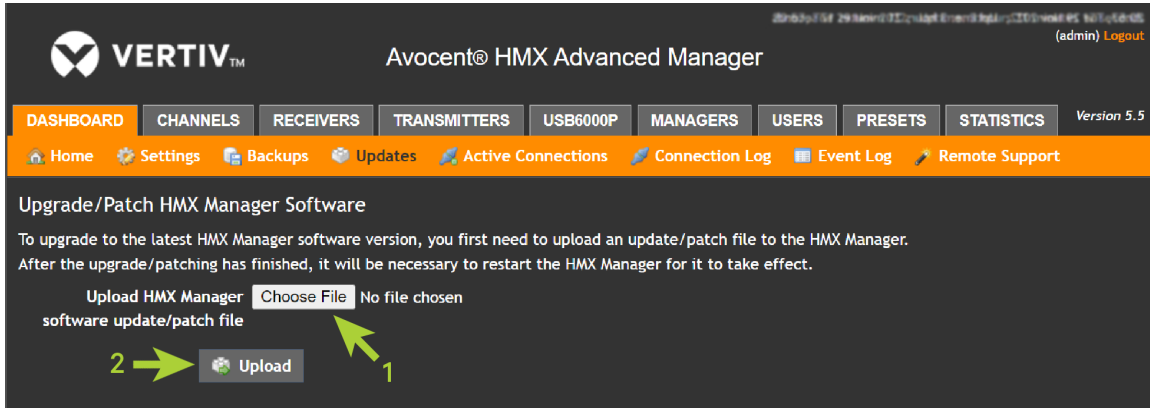
2. Click *Dashboard - Updates*.

Figure 2.8 Updates Tab



- Under the Upgrade/Patch HMX Manager Software heading, click *Choose File* to locate the firmware file you downloaded.
- Select the appropriate file on the server and click *Open*.

Figure 2.9 Firmware Upload

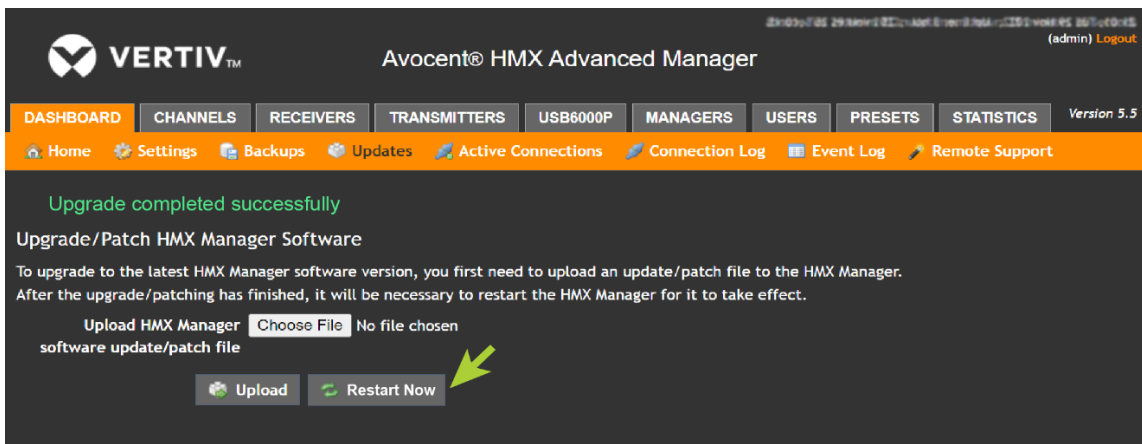


- Click *Upload*. A note appears on the screen to indicate the file is uploading.

NOTE: If there is not enough space available on your manager to complete the upgrade, then delete unnecessary logs, firmware files, and other file types.

- Once the file has uploaded, click *Restart Now*. The restart takes up to two minutes to complete.

Figure 2.10 Restart Now Button



2.7 Backup Manager Server

After configuring your primary server, you can add a backup HMX Advanced Manager server to synchronize the manager databases and provide server redundancy.

NOTE: If you have multiple managers, they may be referred to as a cluster.

NOTE: All servers in your system must use the same firmware version and endpoint licenses.

If you wish to add a backup manager server, see [Server Redundancy](#) in the installer/user guide for instructions. Once the primary and backup servers are synchronized, you can log in to the backup server's web UI to see updates from the primary. However, despite the manager databases being synchronized, only the primary server can change configuration options, including adding and/or removing endpoints, channels and presets.

Appendices

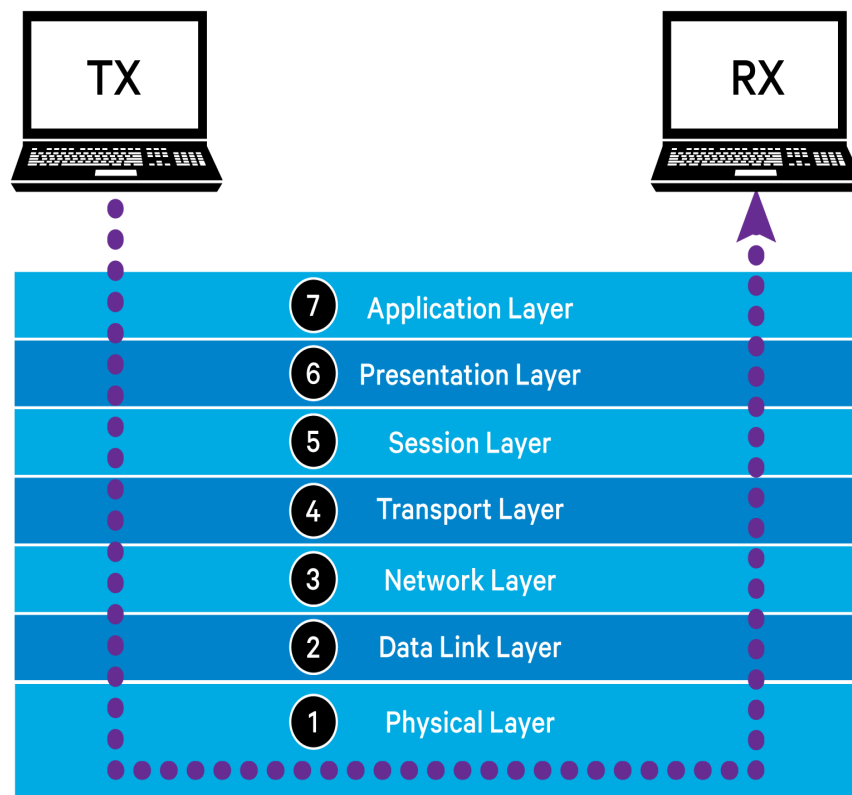
Appendix A: Network Switch Recommendations

This section provides general network information that may assist you in choosing the most appropriate network switch for your HMX Advanced Manager server, along with configuration instructions for certain switches.

A.1 The Open System Interconnection (OSI) model

The OSI model represents the multiple layers of functionality required for data to travel across a network(s) to the end-user. Data travels downstream when transmitted, then upstream to the receiver. The following figure displays the seven layers of the OSI model.

Figure A.1 OSI Model



NOTE: The upper layers (Layers 5-7) occur within the software, whereas the lower layers (Layers 1-3) occur within the hardware.

The Vertiv™ Avocent® HMX transmitter sends data down from the Application Layer to the Physical Layer, and the data becomes encapsulated in a “wrapper” at each layer. These “wrappers” contain instructions for travelling to the next layer. At the Physical Layer, it travels through a physical link, such as a cable, optical fiber, radio wave or other equipment. Then, it travels up the layers again towards the receiver. Once it has reached its intended destination, the “wrappers” are stripped away to reveal the raw data for the receiver.

A.1.1 Layer 2 and Layer 3 of the OSI model

Layer 3 packages and transfers data packets between different networks. Then, Layer 2 breaks data packets into frames to be packaged and transferred within the same network.

Traditionally, network switches operate at Layer 2 and routers operate at Layer 3 for networks with low to medium traffic. However, in larger networks, Layer 2 switches and Layer 3 routers experience latency, so Layer 3 switches are needed to provide additional flexibility to the network.

While Layer 2 switches only connect devices on the same network through their MAC addresses, Layer 3 switches handle both MAC addresses and IP addresses, which allows the switches to route data transmissions to different networks.

NOTE: Due to their complex circuitry, Layer 3 switches are more expensive than Layer 2 switches and are used sparingly in installations.

Additional information regarding switch functions is provided in the following sections.

A.2 Spanning Tree Protocol (STP)

Multiple and redundant links between switches are important for both transfer speeds and network resilience. However, if the links are not carefully managed, the neighboring switches will cause bridge loops and use the duplicated links to repeatedly send data packets.

STP operates at Layer 2 and encourages communication between all switches to prevent bridge loops. However, it can also cause problematic timeouts by temporarily blocking newly found network links for up to 50 seconds to ascertain their function. This would then affect device discovery because the HMX Advanced Manager server cannot be configured correctly.

To resolve the problematic timeouts:

Immediately place any new connection into forwarding mode by enabling PortFast for all host links on a switch. The following section provides information regarding the various forwarding modes for you to determine which one is most suitable.



CAUTION: Do not enable PortFast on switch-to-switch connections as this results in bridge loops.

A.3 Forwarding mode

Forwarding mode quickly and efficiently deciphers, checks and transfers data packets. To determine the best forwarding method for your needs, refer to the following table.

NOTE: Adaptive switches automatically choose one of the following methods listed in Table A.1.

Table A.1 Forwarding Methods

Name	Description
Store-and-forward	This is the original method. To buffer memory, each data packet is saved and put through an error check. Then, it is either forwarded or discarded, depending on if an error is found. NOTE: If the network produces numerous data errors, this method is recommended.
Cut-through	This method addresses latency issues found in some store-and-forward switches. To begin, the switch interprets each data packet upon arrival. Then, the switch forwards the data packet while the remainder is underway. When the entire packet has arrived, the switch runs an error check to tag faulty data packets. However, this method prevents the switch from discarding faulty packets. A host discards any tagged packets instead. NOTE: For HMX Advanced Manager servers, the cut-through method produces the fastest results.
Fragment-free	This method combines the two previous methods. When the first 64 bits have been received, the switch begins forwarding the data packets, which enables the switch to locate and discard faulty packets caused by collisions with other data packets more easily.

A.4 Jumbo frames

NOTE: For jumbo frames to work, all devices within that network must support them.

The HMX Advanced Manager server supports an optional payload size of 9000 bytes, which is beneficial for transmitting certain high-resolution video signals across a network. Since jumbo packets contain more data, less packets need to be managed and transferred, which reduces latency rates. To efficiently handle these enlarged frames, each switch within the subnet must have jumbo frames enabled. Specifically, if any of the computers attached to your Vertiv™ Avocent® HMX transmitters are using or will use any resolution with 2048 horizontal pixels, such as 2048 x 1152, ensure that jumbo frames are enabled on all switches within the subnet.

A.5 Multicasting

Multicasting allows for the simultaneous delivery of identical data to multiple receivers without needing to maintain individual links. It is used when a Vertiv™ Avocent® HMX transmitter must stream video to two or more Vertiv™ Avocent® HMX receivers. Because Layer 2 switches bind all hosts together within the subnet, the multicast transmissions spread to all ports rather than just the port for which the data was intended. This action is referred to as multicast flooding because hosts are forced to process a flood of unrequested data. Internet Group Management Protocol (IGMP) provides an efficient solution for managing multicast transmissions and reducing network congestion.

A.6 IGMP

IGMP is a communications protocol that allows multiple devices to operate under one IP address by joining a multicast group. Each multicast group has its own IP address, and all hosts within a group receive the same network traffic. Hosts and routers can join or leave multicast groups by sending Join or Leave Group messages to the IGMP querier. The querier is a Layer 3 switch that determines which multicast groups the hosts are members of by sending them IGMP Group-Specific Query messages. By identifying the members of each multicast group, the querier prevents hosts from receiving unrequested multicast transmissions. Therefore, hosts only receive transmissions from the multicast groups they have requested to join.

Three different versions of IGMP with varying functionality are available. To learn more about the different versions, refer to the following descriptions:

- IGMPv1: This version allows hosts to opt into a multicast group using a Join Group message. Then, the router must determine when hosts no longer wish to receive transmissions from that group by polling them until they no longer respond.
- IGMPv2: Building off the capabilities of the first version, hosts can also opt out of multicast groups by using a Leave Group message.
- IGMPv3: Maintaining the features of both versions 1 and 2, IGMPv3 enables hosts to specify sources of multicast data.

A.6.1 IGMP fast-leave

When a host wants to leave a multicast group, it sends an IGMP Leave Group message. Then, on the same port the message was received on, the switch sends an IGMP Group-Specific Query message. This Query message results in a delay in switch processor activities because the querier must communicate with each host to determine if any hosts wish to remain a part of the multicast group.

The IGMP fast-leave feature streamlines the process of implementing Leave Group messages. Once the Leave Group message is received, IGMP fast-leave allows for the immediate removal of the host from that multicast group, ultimately preserving network bandwidth.

NOTE: It is recommended to enable IGMP fast-leave on all switches with a direct connection to the HMX Advanced Manager(s).



CAUTION: Ensure all HMX Advanced Manager servers are fully updated to the latest firmware version. HMX Advanced Manager firmware versions prior to 2.1 are not compatible with the timing of IGMP join and leave commands, resulting in multicast flooding in certain configurations.

A.6.2 IGMP snooping

Typically, network switches cannot see which multicast groups the devices have joined. IGMP snooping allows the switches to identify multicast group members by “snooping” on the IGMP Join and Leave Group messages. As a result, the switches can determine which host has requested a multicast and distribute the data to the appropriate host. This feature prevents multicast flooding and improves network efficiency.

When enabling IGMP snooping, ensure that you also enable IGMP Fast-leave on all switches directly connected to HMX Advanced Manager servers. This allows the switches to respond quicker to changes in multicast arrangements.

NOTE: While IGMP messages are effective, they only operate at Layer 3 and are intended for routers to determine whether multicast data should enter a subnet.

A.6.3 Cisco Group Management Protocol (CGMP)

Some Cisco switches support a proprietary standard called Cisco Group Management Protocol (CGMP), which achieves a similar outcome to IGMP. CGMP sends multicast group messages at Layer 2, so switches can natively read these without needing to perform IGMP snooping. The use of CGMP is only possible if all the switches within your network are Cisco units that support this standard.

A.7 Key switch features

NOTE: It is recommended that you use the same switch make and model throughout a single subnet to simplify configuration. Additionally, you should compare the switch specifications with the manager requirements to ensure the switch meets those standards.

A.7.1 Layer 2 switches

When data is transmitted at high rates and/or there are multiple IGMP groups to monitor, implementing IGMP snooping on a low-end switch with a slow processor can cause severe performance problems. If a switch cannot keep pace, then backlogs will occur, causing large numbers of data packets to be arbitrarily discarded and/or multicast flooding to ensue. Ultimately, this results in slow video updates and a poor user experience.

For optimal performance, the following Layer 2 switch features are recommended:

- GB (1024 Mbps) or faster Ethernet ports.
- Supports IGMPv2 or v3.
- Supports jumbo frames up to 9216 bytes.
- High-bandwidth trunk connections between switches, preferably Fibre Channel.
- Ability to perform complex tasks using multiple dedicated processors, such as IGMP snooping.
- The maximum number of concurrent “snoopable” groups meets or exceeds the number of transmitters that will be used to create multicast groups.
- Uses full-duplex operation with 1000 Mbps up- and down- stream speeds per port.
- The switching capacity should match the following equation.

$$\text{Switching capacity} \geq \text{number of ports} \times 1448 \text{ Mpps}$$

If available, enter your switch specifications into a suitability calculator to see if they meet this requirement.

A.7.2 Layer 3 switches

Ensure your Layer 3 switch can operate as an IGMP querier and has sufficient capacity for your subnet size. This is crucial because Layer 3 switches fulfill the role of the multicast router, particularly for private networks that do not require links to wider external networks. The multicast router is a key component for multicast distribution and ensures network traffic reaches the correct Layer 2 switches and their connected hosts.

A.7.3 Commonly used Layer 2 and Layer 3 switches

NOTE: The asterisks (*) signify the switches with examples provided in the following section.

- Cisco 2960 *
- Cisco 3750 *
- Cisco 4500
- Cisco 6500 *
- Extreme Networks X480
- Extreme Networks X460-24t*
- HP Procurve 2810
- HP Procurve 2910
- H3C 5120

A.8 Switch setup examples

The configuration of each switch can significantly impact overall performance. This section provides detailed instructions for properly configuring several common switches.

A.8.1 Cisco Catalyst 2690S and 3750

To configure the Cisco Catalyst 2960S and 3750 switches:

1. Begin in privileged EXEC mode and follow the Command Line Interface (CLI) sample below to manually assign the IP address and default gateway to multiple Switched Virtual Interfaces (SVIs).

```
configure terminal
interface vlan 1
ip address
exit
ip default-gateway
end
show interfaces vlan 1
show ip redirects
copy running-config startup config
```

2. Follow the CLI sample below to assign VLAN1 with an IP address.

```
configure terminal
vlan 1
end
copy running-config startup config
```

3. Follow the CLI sample below to enable IGMP snooping globally.

```
configure terminal
ip igmp snooping
end
copy running-config startup-config
```

4. Follow the CLI sample below to enable IGMP snooping on VLAN1.

```
configure terminal
ip igmp snooping vlan 1
end
copy running-config startup-config
```

5. Follow the CLI sample below to enable IGMP querier.

```
#configure terminal
#ip igmp snooping querier
#end
#show ip igmp snooping vlan 1
#copy running-config startup-config
```

6. Follow the CLI sample below to enable jumbo frames and maximize the size (9000 bytes).

```
configure terminal
system mtu jumbo 9000
end
copy running-config startup-config
reload
```

7. Follow the CLI sample below to enable STP PortFast.

```
configure terminal
interface
spanning-tree portfast
end
show spanning-tree interface portfast
copy running-config startup-config
```

A.8.2 Cisco 6500

NOTE: By default, IGMP version 2 is disabled and IGMP version 3 is enabled.

To configure the Cisco 6500 switch:

1. Follow the CLI sample below to enable STP PortFast for the initial device discovery process.

```
Switch#
Switch#spanning-tree portfast
```

2. Follow the CLI sample below to enable ig IGMP snooping fast-leave.

```
ip igmp snooping fast-leave
```

-or-

Follow the CLI sample below to disable ig IGMP snooping fast-leave.

```
no ip igmp snooping fast-leave
```

Syntax Description

This command has no arguments or keywords.

Command Modes

Interface configuration

Command History

Release Modification

- 12.2(17d)SXB – Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
- 12.2(33)SRA – This command was integrated into Cisco IOS Release 12.2(33)SRA.

A.8.3 Extreme X460-24t

To configure the Extreme X460-24t switch:

1. Assign VLAN1 with an IP address by completing the following steps:
 - a. Connect a terminal or workstation running terminal emulation software to the console port.
 - b. At your terminal, press **Return** or **Enter** until you see the login prompt.
 - c. To login as a returning user, enter a username and password with administrator privileges. Administrator privileges enables you to access all switch functions.

NOTE: Only the password is case-sensitive.

-or-

To login as a first-time user, enter the default username **admin**. No password is required for the default username.

- d. Press **Return**. When you have successfully logged into the switch, the command line prompt displays the name of the switch.
- e. Assign an IP address and subnet-mask for the default VLAN using the following command:

```
configure {vlan} <vlan_name> ipaddress ipv6-linklocal
configure vlan default ipaddress 123.45.67.8 255.255.255.0
```

For example:

The changes take effect immediately.

NOTE: Dotted decimal notation and Classless Inter-Domain Routing (CIDR) notation are used to express subnet-mask when configuring IP addresses for the switch. CIDR is formatted with a forward slash and the number of bits in the subnet-mask. If using CIDR notation, refer to the following example:

```
configure vlan default ipaddress 123.45.67.8/24
```

- f. Configure the default route for the switch using the following command:

```
configure iproute add default <gateway> {<metric>} {multicast
| multicast-only | unicast | unicast-only} {vr<vrname>}
```

For example:

```
configure iproute add default 123.45.67.17
```

- g. Save configuration changes to the currently booted configuration by entering the **save** command.

-or-

Save configuration changes to an existing or new configuration file by entering the **save configuration <new-config>** command.

NOTE: ExtremeXOS allows you to choose where to save the configuration or create a configuration file name of your choice.

- h. Log out by entering **logout** or **quit**.

2. Follow the CLI sample below to enable IGMP snooping.

```
enable igmp snooping {forwardmcrouter-only | {vlan} | withproxyvr }
```

-or-

Follow the CLI sample below to disable IGMP snooping.

```
disable igmp snooping {forwardmcrouter-only | with-proxy | vlan }
```

3. Follow the CLI sample below to enable IGMP fast-leave.

```
enable igmp snooping {vlan} fastleave
```

-or-

Follow the CLI sample below to disable IGMP fast-leave.

```
disable igmp snooping {vlan} fast-leave
```

4. Enable jumbo frames on desired ports and follow the CLI sample below to maximize the size.

```
configure jumbo-frame-size <framesize></fr
```

NOTE: The jumbo frame size range is 1523-9216. This value describes the maximum size of the frame in transit, including four bytes of Cyclic Redundancy Check (CRC) and four bytes of 802.1Q tagging.

5. To set the MTU size for the VLAN, use the following command:

```
configure ip-mtu vlan
```

Appendix B: Troubleshooting

Table B.1 Troubleshooting

Issue and Explanation	Possible Causes	Possible Solutions
<p>Horizontal lines appear across the screen of the Vertiv™ Avocent® HMX receiver.</p> <p>This issue is referred to as blinding. When video data is transmitted, the various lines of each screen are divided up and transmitted as separate data packets. Blinding occurs when the reception of those packets is disturbed. The horizontal lines are the lost data packets. To resolve this issue, refer to the causes and solutions provided in this table.</p>	<p>Multicast flooding has caused unnecessary network traffic.</p>	<ul style="list-style-type: none"> • Enable IGMP snooping on all switches within the subnet. • Enable IGMP fast-leave where each HMX Advanced Manager is connected to a switch as the sole device on a port connection to reduce unnecessary processing. • Ensure that one device within the subnet, usually a multicast router, is correctly configured as an IGMP querier.
	<p>The speed/memory bandwidth of the switch cannot manage the high volume of data being transmitted, causing the switch to lose data packets.</p>	<ul style="list-style-type: none"> • Check the size of the video resolution(s) being fed into the Vertiv™ Avocent® HMX transmitters. If video resolutions with 2048 horizontal pixels are unavoidable, then ensure that jumbo frames are enabled on all switches. • If you are using a less efficient switch, use the cut-through forwarding method to reduce latency.
	<p>The HMX Advanced Manager server is outputting jumbo frames when the network switches have not been configured to use jumbo frames. Therefore, the switches attempt to break down the large packets into standard packets, causing data packets to be lost.</p>	<ul style="list-style-type: none"> • Enable jumbo frames on switches transmitting video resolutions of 2048 or more horizontal pixels. • Adjust the transmitter settings on each manager to streamline the output data. For more information, see Video Settings on page 7.
	<p>The HMX Advanced Manager server is using an old firmware version. Firmware versions prior to v2.1 exhibited an issue with the timing of IGMP join and leave commands that caused multicast flooding in certain configurations.</p>	<ul style="list-style-type: none"> • Ensure every manager uses firmware version 2.1 or later.

Table B.1 Troubleshooting (Continued)

Issue and Explanation	Possible Causes	Possible Solutions
<p>The HMX Advanced Manager server cannot locate other working manager servers.</p> <p>This issue is caused by incorrectly configuring a manager server.</p>	<p>The servers are not reset to their zero config IP addresses for discovery. If you add a server to a network with other working servers, those servers must be factory reset for device discovery.</p>	<ul style="list-style-type: none"> • Ensure the Vertiv™ Avocent® HMX High Performance extender system and the manager server are located within the same subnet. The manager cannot cross subnet boundaries. • To manually reset the system and server to their zero config IP addresses, see Updates in the installer/user guide.
	<p>Layer 2 Cisco switches have STP enabled but do not have PortFast enabled on the ports to which the servers are connected. PortFast must be enabled for the primary manager to locate the other managers.</p>	<ul style="list-style-type: none"> • To determine if PortFast is enabled on a switch running STP, check how long it takes for the port indicator to change from orange to green when you plug the link cable from a working HMX Advanced Manager server into the switch port. If it takes roughly one second, PortFast is enabled. If it takes roughly 30 seconds, PortFast is disabled. • If PortFast is disabled, enable it on all switch ports connected to the servers. <p>-or-</p> <ul style="list-style-type: none"> • Temporarily disable STP on the switches while the manager attempts to locate the servers.
<p>The mouse pointer of the Vertiv™ Avocent® HMX receiver is delayed when moved across the screen.</p> <p>This issue often relates to using dithering on the video output of one or more transmitting computers or using VGA-to-DVI video converters.</p>	<p>HMX Advanced Manager servers attempt to reduce network traffic by only transmitting the pixels that change between video frames. Using dithering and/or VGA-to-DVI converters can change nearly every pixel between each frame, resulting in increased network traffic and a delayed response from the receiver.</p>	<p>Based on your computer, refer to the following solutions:</p> <ul style="list-style-type: none"> • Linux: Ensure the Dither video option is disabled in the video settings of the computer. • Apple Mac with ATI graphics: Use the Vertiv™ Avocent® HMX 8000 High Performance KVM extender system with the Magic Eye dither removal feature. • Windows: Contact Vertiv Technical Support for assistance.

Connect with Vertiv on Social Media



<https://www.facebook.com/vertiv/>



<https://www.instagram.com/vertiv/>



<https://www.linkedin.com/company/vertiv/>



<https://www.twitter.com/Vertiv/>



Vertiv.com | Vertiv Headquarters, 505 N Cleveland Ave, Westerville, OH 43082, USA

© 2023 Vertiv Group Corp. All rights reserved. Vertiv™ 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.

ITSYS_PUBS_REVA_08-23

Avocent® HMX Advanced Manager G2 Server



Quick Installation Guide

NOTE: The Avocent HMX Advanced Manager G2 server is supplied fully pre-loaded. All configuration takes place after the network is connected and running.

1. Connecting to your network

Insert the supplied SFP module into socket 1 on the back of the HMX Advanced Manager G2 server. Connect one end of a CAT 5e or 6 network cable to the SFP module in socket 1 and the other end to a network port to which all HMX transmitters and receivers are connected.

A second SFP module may be inserted into socket 2 to provide a redundant connection to the HMX network or to an external network for administrative access.

Ethernet port 3 is not supported.

NOTE: The HMX Advanced Manager G2 server may be connected to two different networks using SFP socket 1 (right) and SFP socket 2 (left) on the back panel. Port 1 must be used to connect to the network where the transmitters and receivers are connected. Port 2 may be used to connect to another network. The administrator may gain web browser access to the HMX Advanced Manager G2 server from a computer connected to either network.

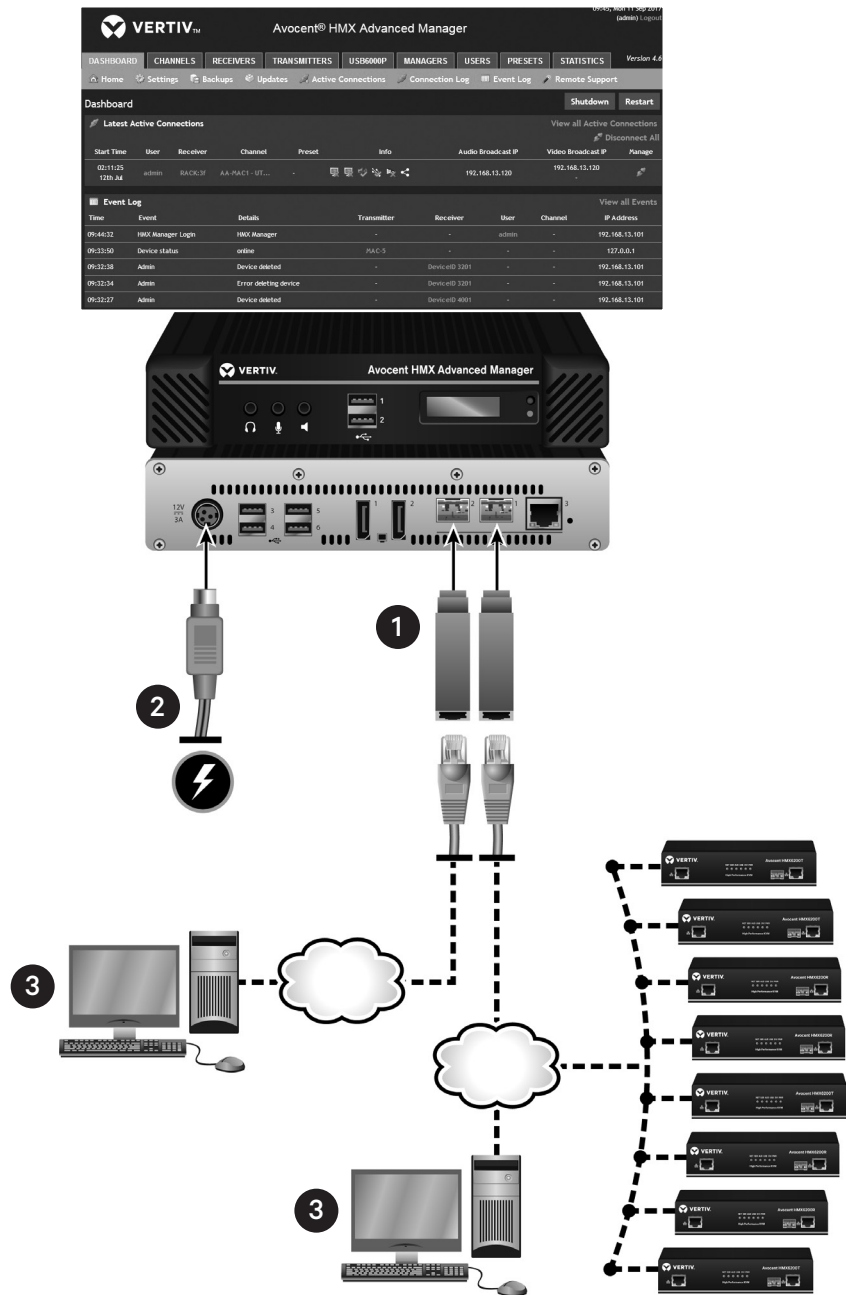
2. Connecting the power supply

Attach one end of the supplied power cord into the back panel of the HMX Advanced Manager G2 server and attach the other end to an appropriately earthed power outlet. Allow approximately three minutes for the booting process to complete.

3. Configuring the IP address

After the HMX Advanced Manager G2 server is fully running, open a web browser on any computer within your

Avocent® HMX Advanced Manager G2 Server Configuration



local network. Enter **169.254.1.3** as the default IP address to access the HMX Advanced Manager software. See the Avocent® HMX Advanced Manager Software Installer/User Guide for information on passwords,

network configurations, permissions and management of the Avocent® HMX High Performance KVM extender system.



To contact Vertiv Technical Support: visit www.Vertiv.com

© 2021 Vertiv Group Corp. All rights reserved. Vertiv™ 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. Specifications, rebates and other promotional offers are subject to change at Vertiv's sole discretion upon notice.





Avocent[®] HMX Advanced Manager

Installer/User Guide

The information contained in this document is subject to change without notice and may not be suitable for all applications. While every precaution has been taken to ensure the accuracy and completeness of this document, Vertiv assumes no responsibility and disclaims all liability for damages resulting from use of this information or for any errors or omissions. Refer to other local practices or building codes as applicable for the correct methods, tools, and materials to be used in performing procedures not specifically described in this document.

The products covered by this instruction manual are manufactured and/or sold by Vertiv. This document is the property of Vertiv and contains confidential and proprietary information owned by Vertiv. Any copying, use or disclosure of it without the written permission of Vertiv is strictly prohibited.

Names of companies and products are trademarks or registered trademarks of the respective companies. Any questions regarding usage of trademark names should be directed to the original manufacturer.

Technical Support Site

If you encounter any installation or operational issues with your product, check the pertinent section of this manual to see if the issue can be resolved by following outlined procedures.

Visit <https://www.vertiv.com/en-us/support/> for additional assistance.

TABLE OF CONTENTS

1 Product Overview	1
1.1 Features and Benefits	1
1.1.1 On-Board Web Interface (OBWI)	1
1.1.2 Groups	1
1.1.3 Channel management	1
1.1.4 Security	1
1.1.5 Third-party authentication	1
1.1.6 External Application Program Interface (API)	2
1.1.7 Supported Browsers	2
2 Installation and Configuration	3
2.1 System Requirements	3
2.2 Zero-config Networking	3
2.3 Installation	3
2.3.1 Initial configuration	4
2.4 Server Redundancy	4
2.5 Licenses	6
2.6 Server Setup	6
2.6.1 Basic setup	6
2.6.2 Replacing a manager server	6
3 Administration	9
3.1 Dashboard tab	13
3.1.1 Dashboard Home screen	13
3.1.2 Settings	14
3.1.3 USB6000P LAN extender	17
3.1.4 Backups	20
3.1.5 Updates	22
3.1.6 Active Connections	23
3.1.7 Connection Log	23
3.1.8 Event Log	23
3.1.9 Remote Support	23
3.2 Adding Extenders	23
3.2.1 Channels tab	24
3.2.2 Receivers tab	25
3.2.3 Transmitters tab	25
3.2.4 Managers tab	25
3.2.5 Users tab	26
3.2.6 Presets tab	28
3.2.7 Statistics tab	29
4 External API	31

Appendices	53
Appendix A: Technical Specifications	53
Appendix B: Advanced USB Features	54

1 Product Overview

The Vertiv Avocent HMX Advanced Manager software is a secure, web browser-based, centralized enterprise management solution that provides remote management and monitoring of multiple Vertiv™ Avocent® HMX High Performance KVM extender systems. In a typical scenario, the HMX extender system connects numerous transmitters and receivers to communicate through a central switch or a network of switches.

As you expand your extender system, the HMX Advanced Manager software provides a streamlined user interface to handle all administration, access control, monitoring and firmware upgrades across the HMX extender system. With the software, you can manage, authenticate and authorize sessions and operate remote video, USB peripherals and audio.

NOTE: For more information on the HMX high performance KVM extender system, see the [Vertiv™ Avocent® HMX High Performance KVM Extender System Installer/User Guide](#).

1.1 Features and Benefits

The HMX Advanced Manager software streamlines processes using group designations, channel management, security and third party authentication.

1.1.1 On-Board Web Interface (OBWI)

A user interface is provided with the HMX Advanced Manager software as a central location for the administrator to view and create user accounts and groups, configure transmitters and receivers, perform database backups and upgrade the firmware of any linked unit.

1.1.2 Groups

Administrators can designate permissions, assign access/control rights and schedule tasks via groups. This involves assigning users to user, receiver or channel groups, which designate their access to the system. The groups also allow inheritance of settings and permissions made in other groups.

1.1.3 Channel management

The On-Screen Display (OSD) for each receiver displays a list of remote computers, called channels, that you have permission to access. Using the HMX Advanced Manager software, administrators can assign channels to users or groups, configure channel access rights and determine the USB, data and video streams for each channel.

1.1.4 Security

With the HMX Advanced Manager, you can ensure users only have access to the systems for which they have permission. This is managed in a three-part relationship between the users, the HMX receivers and the channels.

1.1.5 Third-party authentication

An internal authentication service is provided with the software, which verifies the login username and password against user account information stored in the internal database of the server. In addition, the software supports authentication of users using one or more external Active Directory (AD) systems.

1.1.6 External Application Program Interface (API)

The HMX Advanced Manager software includes an external API that provides queries to retrieve information about channels, presets, users and devices. See [External API on page 31](#) for more information.

1.1.7 Supported Browsers

The HMX Advanced Manager software requires a browser with Javascript enabled. The following are supported browsers:

- Google Chrome
- Mozilla Firefox
- Microsoft® Internet Explorer
- Apple Safari

NOTE: Always use the most recent versions of supported browsers.

2 Installation and Configuration

At this point you should have already completed the installation instructions outlined in the Avocent® HMX Manager Software Quick Installation Guide. Additional information on your configuration options is highlighted in the following sections, as well as basic steps that need to be completed prior to any advanced configuration.

2.1 System Requirements

For optimal performance, ensure your HMX extender system has the following:

- All HMX transmitters and receivers linked with the HMX Advanced Manager server have firmware version 4.1 or higher
- The same firmware version must be used across all units in your system.
- IGMP v2 or v3 support
- Jumbo frame support up to 9216 bytes
- Portfast option is enabled on each port of the switches that have an HMX Advanced Manager server connected

2.2 Zero-config Networking

The HMX Advanced Manager server uses zero-config networking. The default IP addresses are listed in the following table.

Table 2.1 HMX Advanced Manager Server Default IP Addresses

Name	IP Address	Description
Primary HMX Advanced Manager server	169.254.12	Fixed server address.
HMX Advanced Manager ETH1	169.254.13	Address used for initial log in and must be changed to a permanent network address.
Backup HMX Advanced Manager server	169.254.14	If two HMX Advanced Manager servers are on the same network, one server is the backup server; this IP address is automatically assigned.

NOTE: If you are using a static zero-config address, set the IP address to 169.254.11 to avoid potential IP address conflicts.

2.3 Installation

The first time you log in, the default IP address of the HMX Advanced Manager server must be changed in order to perform any other actions or navigate to any other screens.

To change the IP address:

1. From a web browser on your local computer, enter the default IP address <http://169.254.13> for the HMX Advanced Manager server.
2. Enter the default username **admin** and password **password**.
3. Click the *Dashboard* tab, then click *Settings - Network*.
4. For Ethernet Port 1, change the IP address and netmask address, then click *Save*.
5. After the web browser automatically redirects to the new IP address, enter your username and password to log in to the server.
6. After you change the server IP address, change the admin password.

NOTE: If the HMX Advanced Manager server is offline, verify your computer can access the new IP address.

2.3.1 Initial configuration

To configure the initial setup:

1. Set the management IP address to 169.254.1.99 with a subnet mask of 255.255.0.0.
2. From a browser, enter the IP address 169.254.1.3.
3. Enter admin for the username and password for the password.
4. On the Managers tab, click *Configured*.
5. On the Configure Manager screen, if you only have one manager, click the Solo radio button and click Save.
6. On the Network Settings page, enter the IP Pool Lower Limit and IP Pool Upper Limit and click Save. It is recommended that you leave all other options on the default setting. After the settings are saved, it takes approximately forty seconds for the new IP settings to take effect.

To change the admin password:

1. From a web browser, enter the IP address of the HMX Advanced Manager server.
2. Enter **admin** and **password**, then click *Login*.
3. Click the *Users* tab and click the *Configure User* icon for the admin user.
4. On the Configure User screen, enable the Change Password radio button.
5. In the appropriate fields, enter your new password twice and click Save.

NOTE: If you use password as your password, no password is required to log in.

2.4 Server Redundancy

When a manager server boots the first time, it checks for other manager servers on the network. First, it scans to find a primary manager on the same subnet. If discovered, the manager requests an IP address from the primary manager server. Typically, the IP address assigned is the next available IP address. Once the backup server is given the IP address, a Transport Layer Security (TLS) trust relationship is established using private and public keys. This is used to encrypt the communications between the manager and the endpoints. If a primary server is not discovered on the same subnet, the server attempts to acquire an IP address from a DHCP server. The server temporarily accepts the IP address including the subnet mask, gateway and DNS settings and reads the custom option 125 value, if present. The manager server cycles through the IP addresses in option 125 to see if any are being used by another manager server. If the IP address is free, the manager automatically configures itself by statically setting the IP address and using the subnet mask, gateway and DNS provided by DHCP.

The database is synchronized between the primary and backup managers. Depending on the size of the database, this can take up to ten minutes to complete. During this time, the status in the primary manager interface is "Initializing". When the synchronization is complete, the status changes to "Standby". In the server redundancy setup, both the primary and the backup server databases are synchronized to ensure they are identical. If for any reason the backup server is turned off, any changes to the system configuration are not maintained by the backup server.

In the event of a failure, the backup server acts as the primary server and the extenders begin communicating with the second IP address stored in their configuration. During this time, new devices cannot be added and the configuration cannot be changed. If new extenders must be added, the backup server must be promoted as the primary server. When the primary server comes back online, it resumes its role as the primary server. However, if the backup server has been promoted to primary, when the primary server comes back online, the backup server must be factory reset.

NOTE: It is not possible to have two primary servers on the same network.

For server redundancy, a primary and backup manager must be configured. The following steps are required to configure a primary and a backup server.

Prerequisites:

- Both units must have the same version of firmware and the same end point license.
- The Require Authentication setting on the primary unit must be set to No.
- The Primary unit cannot use the last IP address in a range, for example, x.x.x.254. The primary unit automatically assigns the backup unit with the next available IP address, which is not available.
- The backup unit must be factory reset before adding it to the network.

To configure server redundancy:

1. From the web interface, log in to the primary HMX Advanced Manager server.
2. Click the *Dashboard* tab and click *Settings - Managers*.
3. Verify the Require Authentication radio button setting. If set to No, new servers can join the network as soon as they are plugged in. If set to Yes, enter a cluster password for each HMX Advanced Manager server.
4. On the *Managers - Configure Server* screen, select the primary radio button, configure the Ethernet port 1 address and click *Save*.
5. Add the new backup HMX Advanced Manager server with factory default settings to the network. The new server is labeled Unconfigured on the main Servers tab screen. After five minutes, the backup server is added to the list as the backup and its status is Standby.

NOTE: It is not possible to have two servers with different licenses in a cluster.

NOTE: If the transfer of the backup database is interrupted, and only a partial database is transferred, the problem is reported on the management server page. If this occurs, it will not be possible to log in to the backup database and the firmware version of the backup will be reported as V. After five minutes, click *Factory Reset* in order to clear this issue.

6. Click the Configure icon to configure the backup server.

-or-

Click the Restricted Page Configure icon to open a restricted screen and configure the server directly from its own IP address. Using this method, the configuration options are limited to: View the logs, Update/Reset HMX Advanced Manager server and Configure this server.

To set up a backup server:

NOTE: The default IP address of the backup server is 169.254.1.3. It is recommended that you directly connect to the backup server during setup in order to prevent the primary server from taking control.

1. Choose an IP address out of the DHCP pool scope on the subnet. The IP address must be added to DHCP option 125 on all the DHCP servers that service the network.
2. On the backup server, click *Dashboard - Updates*, update the firmware and reboot the server.
3. On the primary server, click *Dashboard - Settings - General* and verify the number of supported devices matches the licenses on the backup server.
4. On the primary server, click *Dashboard - Settings - Servers*, click *No* on the Require Authentication setting and click *Save*.
5. Perform a factory reset on the backup server and reboot the server. See [Reset the manager configuration on page 22](#).

After the reboot, the backup server establishes its IP address and makes contact with the primary manager server. The primary server synchronizes its database with the backup.

2.5 Licenses

The HMX Advanced Manager servers are licensed according to the number of devices that can be managed. For additional information on upgrading your licenses, contact Technical Support or your Sales representative.

NOTE: For server redundancy, the primary and backup servers must have the same type and number of licenses.

To upgrade your license:

1. From the manager server, click the *Dashboard* tab and click *Settings - General*.
2. Click *upgrade license* to display the unique product code.
3. Provide the following to retrieve the unique license key from Technical Support:
 - Unique product code
 - Serial number on the base of the manager server
 - Current number of supported devices
 - Number of devices available for upgrade
4. On the Upgrade License screen, enter the provided license key and click *Save*.

NOTE: Only enter the license key for the applicable HMX Advanced Manager server.

5. Click the *Dashboard* tab, click *Settings - General* and verify the license is upgraded.

2.6 Server Setup

The HMX Advanced Manager server is configured using either basic setup or server redundancy. Basic setup consists of one HMX Advanced Manager server. Server redundancy consists of two HMX Advanced Manager servers, where one server is the primary server and the other is the backup server. If the primary server fails for any reason, the backup server will failover.

NOTE: For server redundancy, the primary and backup servers must have the same type and number of licenses.

2.6.1 Basic setup

In the basic setup, each extender must be reset to the factory default and discovered by the HMX Advanced Manager software. The software completes re-configuring the IP addresses of the extenders.

To configure your server:

1. After the server is installed on the network, perform a factory reset on all extenders to force the extenders back to their default states.
2. Using a computer connected to the same network, log in to the server.
3. After the extenders are discovered you can begin configuring access to them.

2.6.2 Replacing a manager server

If an existing manager server needs to be replaced, proceed to the following applicable procedure.

NOTE: When replacing a manager server, the extender devices are undetectable and may require a factory reset.

To replace a solo HMX Advanced Manager server:

1. Before connecting the new manager server to the main network, connect it to an isolated network switch.

2. Using a computer connected to the same switch, log in to the new server.
3. Verify the new server is running the same firmware version as the one being replaced.
4. Set the IP address of the new manager server to match the original server.
5. Restore a backup file of the original manager server database to the new server.
6. Remove the original manager server from the network.
7. Connect and turn on the new manager server.
8. Perform a factory reset on all extenders so the extenders inherit the security certificate of the new manager server.

To replace the primary server in a redundant configuration:

1. Promote the backup server to the primary server.
2. Replace the primary server. The replacement server begins communicating with the primary server and downloads the database as the backup server.

To replace the backup server in a redundant configuration:

Replace the backup server with a new server. The replacement server begins communicating with the primary server and downloads the database as the backup server.

This page intentionally left blank

3 Administration

You can expand and customize the system components using the HMX Advanced Manager OBWI. Operations include authenticating and authorizing sessions between receivers and transmitters in the system, as well as all administration, access control, monitoring and firmware upgrade activities across the HMX extender system.

The HMX Advanced Manager software is designed with on screen tips and hover instructions to guide you through the operations. The following section describes the on screen elements and provides procedures, where applicable.

Figure 3.1 HMX Advanced Manager Home Screen

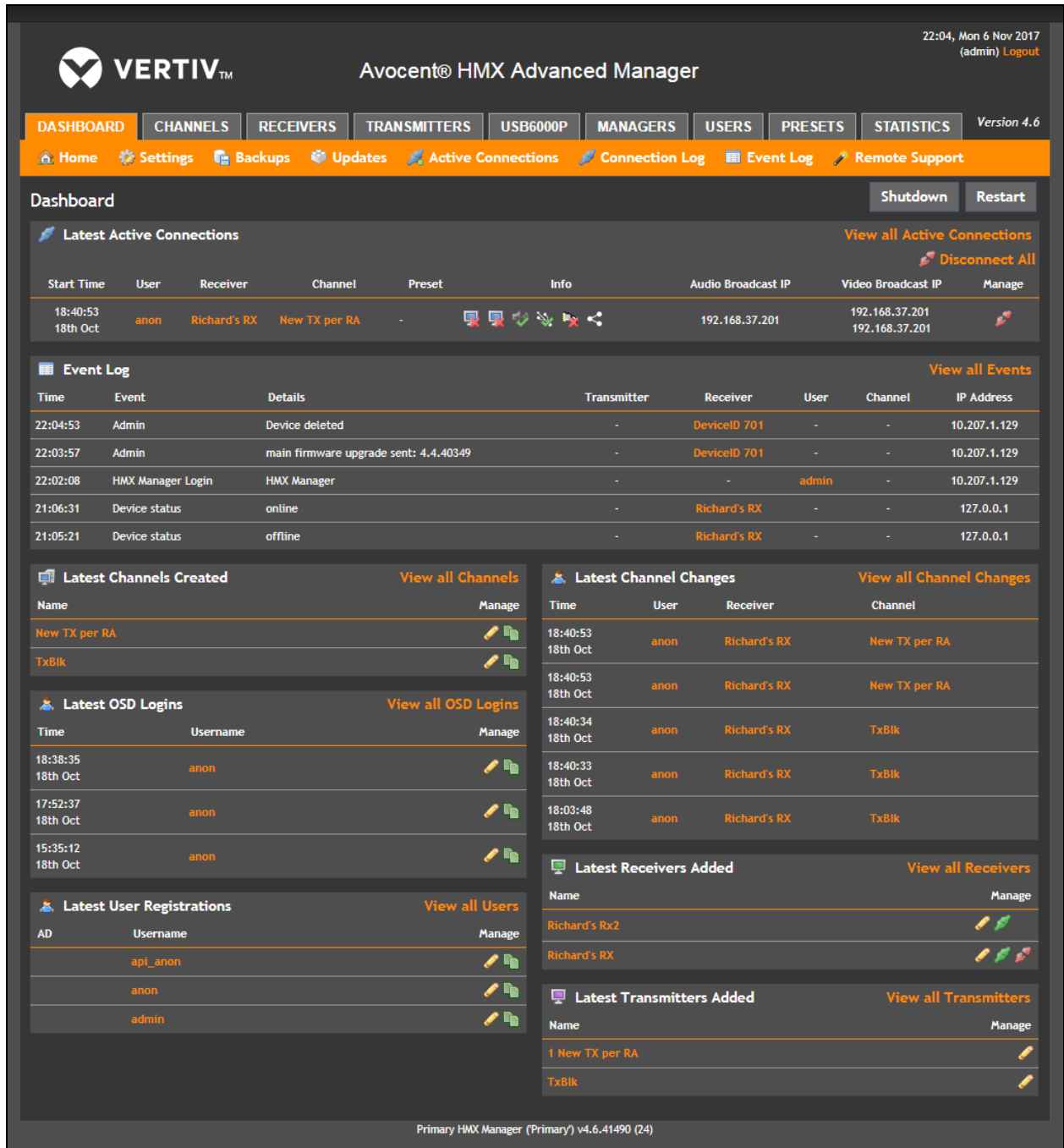


Table 3.1 Home Screen Descriptions

Number	Description
1	Top Navigation Tabs
2	Tab Menu
3	Menu Buttons
4	Icons (see the Icons Description table for more information)

The top navigation tabs, which are used to manage the components in your system, are defined in the following table.

Table 3.2 Top Navigation Tabs

Tab	Function
DASHBOARD	Status of all HMX Advanced Manager operations
CHANNELS	Transmitter video, audio and USB stream configuration
RECEIVERS	Individual receiver configuration
TRANSMITTERS	Individual transmitter configuration
MANAGERS	All servers in the HMX Advanced Manager network
USERS	All users in the HMX Advanced Manager network
PRESETS	New and existing preset configuration
STATISTICS	Real-time data measurements

Table 3.3 Icon Descriptions







Icon	Description	Icon	Description
	Accept		Group
	Add		Find
	Application form		View mode
	Application view detail		Warning
	Refresh		Email
	Switch		Error
	Audio disabled		Home
	Audio enabled		Information
	Empty bin		Inherit
	Chart		Lightbulb
	Computer key		Lock
	Connect		Lock off
	Active connection		Lock on
	Lock open		Lock open
	Copy page		Configure

Table 3.3 Icon Descriptions (continued)

Icon	Description	Icon	Description
	User		Configure restricted
	Sound		Add server
	Sound off		Delete server
	Stop		Servers
	Table		Serial off
	Check		Serial on
	Dual video on		USB off
	Video off		USB on
	Video on		Wand
	Video wide off		Multicast
	Video wide on		Zoom
	Cross		Delete

3.1 Dashboard tab

The Dashboard tab is the Home screen for checking and changing the general status of all HMX Advanced Manager operations. You can also access specific status information from the following buttons on the Dashboard Home screen: Settings, Backups, Updates, Active Connections, Connection Log, Event Log and Remote Support screens. The Home screen is auto-refreshed every 10 seconds to ensure that the most current information is displayed.

3.1.1 Dashboard Home screen

From the Dashboard Home screen, you can view the following general status information.

Table 3.4 Dashboard Home Screen Options

Option	Description
Shutdown	The admin user can shut down the HMX Advanced Manager server. The OSD is disabled on the receivers. The HMX Advanced Manager server must be manually started again.
Restart	The admin user can reboot the HMX Advanced Manager server. The OSD and admin section is unavailable while the server is rebooting.
Latest Active Connections	Displays the five most recent active sessions and includes the following information for each: when the session started, which user/receiver/channel is used, connection type (icons show audio, video, serial, USB and exclusive) and the IP addresses in use. The red unplug icon on the far right allows the admin user to disconnect a connection.
Event Log	Displays all actions performed by the admin or users in the HMX Advanced Manager system.
Latest Channels	Displays the last five channels created in the HMX Advanced Manager system. A channel is created by default when a new transmitter is added and configured. The edit icon next to a channel allows the admin user to configure the channel.
Latest User Logins	Displays the last five users who logged in (either to the HMX Advanced Manager admin or a receiver).
Latest User Registrations	Displays the last five users added to the HMX Advanced Manager system, with a link to edit the user details/permissions.
Latest Channel Changes	Displays the last five users who changed a channel, either while using the on-screen display (OSD) at a receiver, or via the HMX Advanced Manager admin control panel.
Latest Receivers Added	Displays the last five receivers to be added and configured in the HMX Advanced Manager network. Click to configure a receiver, connect to channel or disconnect an existing connection.
Latest Transmitters Added	Displays the last five transmitters to be added and configured in the HMX Advanced Manager network. Click to configure a transmitter.

3.1.2 Settings

From the Dashboard tab, the Settings button displays global options for the HMX Advanced Manager system. This button gives you access to the General, Transmitters, Receivers, Managers, Network, Time, Mail and Active Directory screens.

Settings - General button

The options in General screen are described in the following table.

Table 3.5 General Screen Options

Option	Description
Receiver OSD Timeout	Displays the period of inactivity in the OSD after which a standard user is automatically logged out.
HMX Advanced Manager Admin Timeout	Displays the period of inactivity in the HMX Advanced Manager config screens after which an admin user is automatically logged out.
Anonymous User	Displays the user shown in the log when a receiver is set to No login required.
Hide Dormant Devices	Displays the devices that have been offline for more than 24 hours are hidden, if this option is enabled.
Allow All Users Exclusive Access	Designates if a user can connect to a channel exclusively and prevents any other users from connecting to that channel. If not set, users can connect in view-only mode or shared mode. Settings that are applied specifically to a user override settings applied to user groups. For a detailed explanation, see Allow All Users Exclusive Access below.
Allow All Users Remote OSD Access	If this option is enabled, receivers may be switched remotely from another receiver OSD menu.
Allowed Connection Modes	Displays the global connection mode setting applied to all new channels. Settings are only applied as a default and can be overridden at the channel level. For a detailed explanation, see Allowed Connection Modes below.
Rows per Page	Displays the number of rows displayed in the administration section tables.
API - Login Required	Disables anonymous use of the API.
API - Anonymous User	Determines the user permissions used when accessing the API without logging in.
License - Supported Devices	Displays the number of devices that can be connected to the manager server. Click the <i>upgrade license</i> link to display the Upgrade License screen and upgrade the current license.
License - Licensed Features	Displays the current license features installed. Click the <i>view/change</i> link to display the Licensing screen and add additional feature licenses.

Allow All Users Exclusive Access

Exclusive mode at user level overrides all other settings. If a user is set to inherit the allow exclusive mode from their user groups and one of the groups has allow exclusive mode granted, or if one of the groups is configured to inherit the allow exclusive mode from a global setting, the user is granted allow exclusive mode.

Allowed Connection Modes

By default, all new channels are set to inherit this global value. If a channel has its own setting, the global setting has no effect on that channel. The following table describes the available connection modes.

Table 3.6 Connection Modes

Mode	Description
View only	Allows users only to view/hear the video and audio output, the USB channel is denied.
View/Shared only*	Prevents users from gaining exclusive access to a channel.
Shared only	Ensures that all connections are shared.
Exclusive only	Ensures that all connections to a channel are made singularly.
View/Shared & Exclusive*	Permits either type of connection to be made.

* If USB is disabled, Shared mode is not available as an option.

Settings - Transmitters button

Transmitters screen options apply a global configuration settings for all transmitters. Settings made on individual transmitters override the global settings. Individual settings can be modified on the Transmitters tab.

Table 3.7 Transmitter Options

Option	Description
Anti-Dither	Anti-dither solves increased bandwidth issues caused by dithering techniques used on some computers. For transmitters, the anti-dither feature should be enabled.
Display Data Channel (DDC)	DDC determines if the video configuration details are retained from connected display screens or if a static fixed EDID is used. Only the dual extenders support dual-link video resolutions.
EDID optimization	EDID optimization compares the transmitter native resolution settings of the monitors when switching. If the monitor has the same native resolution as the previous one, the new EDID is not sent to the graphics card. If the new receiver has a monitor with a different native resolution, the EDID is updated to allow for a change in video mode.
Hot Plug Detect Control	Determines if hot plug detection is enabled for monitors .By default this is enabled.
Hot Plug Detect Signal Period	The 100 ms (default) setting is sufficient for most graphics cards.
Background Refresh	Configures or disables the number of frames of video data. Selecting longer periods or disabling this function reduces the required bandwidth.
Compression Level	Provides greater compression for increased speed where pixel perfect results are not the primary focus. For a detailed explanation, see Compression Level below .
Enable Dummy Boot Keyboard	Configures a virtual keyboard to report to the USB host during startup. It may be necessary to disable this for use with some KVM switches.
USB Speed	Selects USB 2 Hi-Speed or USB 1 Full Speed.
USB Hub Size	Selects the number of USB devices that can be connected to a single transmitter.
Reserved USB ports	Determines how many USB ports can be reserved for transmitters. This setting can only be applied globally. It is not available for individual transmitter configurations because all receivers need to know how many USB ports are available for the advanced USB features.
Serial port options	The Serial Parity, Serial Data Bits, Serial Stop Bits and Serial Speed settings allow you to define the key parameters for the AUX port of the transmitter to match the operation of the device attached to it.

Compression Level

From the Transmitter Video Configuration screen, you can choose one of the following compression modes:

- Pixel Perfect - only uses pixel perfect AVCT
- Adaptive - guarantees frame rate, builds to pixel perfect
- Smoothest Video - forces the maximum compression
- Advanced - allows you to choose the minimum and maximum compression.

3.1.3 USB6000P LAN extender

The USB6000P LAN extender allows you to connect up to four USB peripherals using a standard LAN or direct cable connection up to 328 feet (100 m) in length. The extender modules support USB version 1.1 and 2.0 devices. USB 3.0 devices can also be used, but they will operate in USB 2.0 compatibility mode.

Pairing and unpairing

If purchased together, the transmitter and receiver are already paired with each other. If the modules are purchased separately, or if you need to change the pairing, follow these steps.

To pair modules:

1. Ensure the transmitter and receiver modules are either directly connected to each other or are connected to the same subnet on your network.
2. Press and hold the Mode button on the rear panel of the transmitter module. Release the button within ten seconds. The green Link indicator will flash.
3. Within ten minutes of activating the pairing mode on the transmitter, press and hold the Mode button on the rear panel of the receiver module. Release the button within ten seconds. The green Link indicator will flash.

NOTE: Both modules must be connected to the same subnet.

The link indicators on both units may flash slowly. When the link is established between both units, the Link indicators will be on. If more than ten minutes pass before the units are paired, the modules will exit pairing mode and reestablish their previous links.

To cancel pairing mode, press and hold the Mode button a second time and release it within ten seconds.

To unpair modules:

With both units on, press and hold the Mode button on the rear panel of either module. The green Link indicators on the front of both modules will no longer illuminate.

Table 3.8 Indicator Description

Item	Description
Power (Blue)	On when power is supplied by the computer for the transmitter module and by the power adaptor for the receiver module.
Link (Green)	On when a paired data link is established, fast flash when in pairing mode and slow flash when attempting to establish a pairing link.
Host (Green)	On when modules are correctly enumerated on the computer. Flashes when in a suspended state.
Activity (Amber)	Flashes when data transmission is occurring, off when in a suspended state.

Settings - Receivers button

Receivers screen options apply a global configuration settings for all receivers. All settings made on individual receivers or receiver groups override the global settings, except hot key settings.

Table 3.9 Receiver Options

Option	Description
Hotkey Settings	Designates the hotkeys that can be used to invoke certain functions. It is not possible to use both mouse buttons and key combinations or mix left and right shift, ctrl or alt keys.
Login Required	Designates if you must log in to the receiver.
Enable Receiver OSD Alerts	Enables or disables receiver OSD alerts.
Video Compatibility Check	Reads the EDID from the attached monitor and determines whether the monitor is capable of displaying the selected video mode before connecting a channel. This setting prevents the receiver from displaying a black screen and prevents the user from being locked out if a dual link resolution is selected to display on a single link monitor.
Force 60Hz	Enables or disables the frame rate. If enabled, the receiver frame rate is set at 60 Hz, regardless of the video input frame rate. Video Switching options cannot be altered when this option is enabled.
Video switching	Fast switching (default) retains the same frame rate at either 50 Hz or 60 Hz, depending on which video resolution is displayed first. Match Frame Rate follows the source frame rate and changes the frame rate every time this changes, even if the video resolution does not change. If you have one receiver switching between 1920 x 1080 @ 60 Hz and 1920 x 1080 @ 50 Hz, this setting changes the frame rate from 60 Hz to 50 Hz every time you switch.
Receiver Keyboard Country Code	Allows you to select the language for the keyboard connected to the receiver.
USB Settings	Global USB settings that can be overridden by the receiver and receiver groups. For more information, see the Global USB settings table.
Audio Input Type	Selects the required audio input type.

Table 3.10 Global USB Settings

Setting	Description
HID only	If enabled, only HID devices (mice and keyboards) may be connected to the receiver.
Disable Isochronous Endpoint OSD Alerts	When an isochronous USB device is connected to the receiver, warning messages are not displayed. Extenders do not support isochronous devices.
Enable Isochronous Endpoint Attach	Some USB devices combine many USB devices behind a USB hub. By enabling this option, devices cannot connect to receivers and the isochronous part of the devices do not work.
Advanced Port Features	The advanced port allows you to determine USB port behavior for use with certain USB devices. The defaults are no reserved ports, merging enabled and no feature code set. Do not change the default settings without direction from Technical Support.

Settings - Managers button

The Manager screen is used to configure redundant operation for the HMX Advanced Manager servers. With two servers on the same subnet, one server becomes the primary and the other becomes the backup. If the primary server fails, the backup server takes over until the primary server is repaired. This functionality is only possible if the licenses of both HMX Advanced Manager servers match and both servers control the same number of endpoints.

Table 3.11 Server Redundancy Options

Option	Description
Primary Timeout	Number of seconds for the primary server to be unavailable before the backup server takes over.
Conflict Timeout	Number of seconds after which an inactive server is considered offline.
Backup Check Interval	Interval between the primary server polling the backup to determine if it is online.
Backup Timeout	Period of time that a backup server can be offline or unreachable before it is considered a failed server.
Require Authentication	Designates if managers in the cluster are allowed to communicate without authentication. If <i>No</i> , a manager is permitted to join the cluster by being plugged in. If <i>Yes</i> , a password is required to validate.
Cluster Password	Allow new managers to join the cluster without disabling the authentication requirement. If this method is used, it is necessary to set the same password on any new machine separately before it can join the cluster.

Settings - Network button

The Network screen allows you to set the network configuration for the HMX Advanced Manager network.

Table 3.12 Network Options

Option	Description
Syslog Enabled	Determines whether Syslog should be used to record log data to an external Syslog server.
Syslog IP Address	IP address of the external syslog server.
Require SSL for Web	Determines if a certificate must be downloaded and all connections use <code>https://</code> rather than the default <code>http://</code> .
Multicast IP Address	Multicast connections use auto-incrementing IP addresses starting from this value. Ensure there are sufficient addresses above this value, so that all generated addresses are below 239.255.255.255
IP Address Pool	Specifies an IP address pool. Devices are automatically assigned the first available IP address within this pool.
Ethernet Port 1	IP settings for the primary Ethernet port, which must be configured using a static IP address.
Ethernet Port 2	IP settings for Ethernet port 2 can be disabled, configured using a static IP address or DHCP.
SNMP	Allows the HMX Advanced Manager to connect to an external SNMP server. If SNMP is enabled, there are three connection modes: <ul style="list-style-type: none"> • Authentication + privacy (two authentication types, SHA or MD5, and two Privacy types, AES or DES, are available) • Authentication only (two authentication types, SHA or MD5, are available) • No authentication

Settings - Time button

Up to three external Network Time Protocol (NTP) servers can be defined.

Table 3.13 Time Options

Option	Description
NTP Enabled	Determines whether one or more external Network Time Protocol servers is used to provide time for the server.
Server address	IP address of the NTP server.
NTP Key Number and NTP Key	For symmetric key authentication of the server, enter an appropriate NTP key number and key.
Time Zone Area and Time Zone Location	Drop-down list with selectable time zone options.

Settings - Mail button

The mail function allows you to configure a mail server to receive email alerts and backups. A mail server must be on the network to use the mail function.

Table 3.14 Mail Options

Option	Description
Mail Enabled	Determines whether the mail features of HMX Advanced Manager should be invoked.
SMTP Domain name/IP	Name or IP address of the external SMTP server that will be used to process all outgoing mail.
SMTP Port	Port on the SMTP server.
Username, Password	Username and password for access to the SMTP server.
Email Address for Alerts	Email address to be used to send alert messages.

Settings - Active Directory button

The Active Directory screen is used to configure third-party authentication.

Table 3.15 Active Directory options

Option	Description
AD Enabled	Assigns Active Directory features.
Account Suffix	Assigns the account suffix for your domain.
Base DN	Assigns the base distinguished name for the top level of the directory service database.
Domain Controller	Assigns the IP address or name of the server that holds the required directory service.
Username, Password	Assigns the username and password for the domain account.
Sync Schedule	Designates the synchronization schedule.

3.1.4 Backups

Backup copies of the HMX Advanced Manager database, containing all devices, users, channels and logs, can be scheduled to run on a recurring basis or can be performed manually.

NOTE: It is a best practice to schedule regular backups of your HMX Advanced Manager database.

Backup Options

Backups can be scheduled to download to the manager server or your local computer, or they can be emailed to a user.

To download to the manager server:

1. Verify the Download to your computer option is not checked.
2. Click *Backup Now* to save the backup file to the server.

To download to your computer:

1. Enable the Download to your computer checkbox.
2. Click a schedule option and click *Save Setting*.

-or-

Click *Backup Now*.

To email a backup:

NOTE: The Email backup option requires you to store a valid email address on the *Dashboard - Settings* screen.

1. Enable the Email backup checkbox.
2. In the Email Backup To field, enter a valid email address.
3. Click a schedule option and click *Save Setting*.

-or-

Click *Backup Now*.

NOTE: Emailed backups are encrypted; these backup files are automatically decrypted by the HMX Advanced Manager server when they are used.

Restore from Server

All backups are saved on the server with a time-stamp of when the backup was run. A previous backup can be restored to the server or to a different location.

NOTE: Before restoring a previous backup, back up the current manager server. Restoring the contents of a backup file overwrites all data in the HMX Advanced Manager system with the data in the backup file including configured devices, channels, users, connection logs and action logs.

Restore from File

Restore from file is used to upload a backup file that you have previously downloaded or received by email. Restoring the file overwrites the contents of the current HMX Advanced Manager system.

Archive Log to CSV File

Connection or log data can be archived to a CSV file. Old log data is removed from the database, simultaneously. Clicking *Archive* saves a CSV file to the server.

Download CSV Archive

You can download any archived CSV file created using the archive log by selecting it from the archives saved on the server. The CSV file can be opened in Microsoft Excel to review actions and connections.

3.1.5 Updates

In the updates screen you can upgrade the manager software, install firmware on the extenders and reset the manager server configuration. In a managed matrix configuration, use the HMX Advanced Manager software to quickly upgrade the firmware across multiple transmitters and receivers. The HMX 5100 and 5200 extenders are not downgradable, so the HMX Advanced Manager server must be upgraded to the same version as the extenders to be compatible.

Upgrade the manager software

The upgrade software function is used to upgrade the manager server to the latest version.

To upgrade the manager software:

1. From the Vertiv web site or via Technical Support, download the appropriate firmware file.
2. Click *Dashboard - Updates*, then under the Reset HMX Manager Configuration, click *Choose File* to locate the firmware file that you downloaded.
3. Select the appropriate file on the server and click *Open*.
4. Click *Upload*. The file is uploaded, checked and applied.
5. Restart the manager server for the update to take effect.

NOTE: All firmware files are encrypted and digitally-signed for HMX Advanced Manager-server integrity.

Reset the manager configuration

The HMX Advanced Manager can be reset to its initial configuration, original factory setting or to the latest firmware. All devices, channels, presets, users, groups, backups, logs and uploaded firmware files are removed.



CAUTION: It is recommended that you download a backup before continuing.

To reset the manager configuration:

1. From the Dashboard tab, click *Updates*.
2. Select the checkbox to enable the Also reset the manager IP address option.
3. Select the checkbox to enable the Also delete security certificates option.
4. Click *Reset HMX Manager Configuration*.
5. Click *Reset* on the pop-up.

NOTE: The reset pop-up is displayed until all of the data is reset.

6. After the reset completes, click *Restart Now*. The restart takes up to two minutes to complete.

Firmware Upgrade

Before you can upgrade firmware for the extenders, you first need to download the firmware file.

To upload new transmitter/receiver firmware:

1. From the Vertiv web site, download the appropriate firmware file.
2. Click *Dashboard - Updates*, then under the Upload New TX/RX Firmware, click *Choose File* to locate the firmware file that you downloaded.
3. Select the appropriate file on the server and click *Open*.
4. Click *Upload*. The file is uploaded, checked and applied.

To upgrade firmware globally:

1. Under Install Firmware onto Devices, select the device type and firmware type.
2. Click the Available firmware drop-down menu and select the new firmware version.
3. Click *Install* to apply the firmware to the devices.
4. Click to enable the Upgrade boxes next to each device to apply the firmware upgrade.

-or-

Select *Upgrade All* to apply the firmware globally to all devices.

NOTE: Select *Reboot First* or *Reboot All First* when using the Upgrade All option.

5. Click *Upgrade Selected* to create a queue of devices to be upgraded. The status of devices is displayed on the receiver/transmitter and device screens, including if the device is in the queue to be upgraded or if it is in the process of rebooting with the new firmware.

3.1.6 Active Connections

Shows only connections that are currently active in the HMX Advanced Manager network.

3.1.7 Connection Log

The Connection log displays all connections in the HMX Advanced Manager system. Direct links display the IP address of the receiver only and multicast broadcasts are indicated by the multicast icon and the common multicast IP address.

3.1.8 Event Log

The Event log displays events in the Manager system. The event list can be filtered using a drop-down list from the top of the screen and event log data can be archived to a .CSV file via the Archive log data link.

3.1.9 Remote Support

The remote support provides Technical Support remote access to the HMX Advanced Manager server.

NOTE: Contact Technical Support before enabling remote support.

3.2 Adding Extenders

Unless extenders have been locally configured using the System Configuration utility, new extenders that are added to the network automatically appear in the HMX Advanced Manager software. When the HMX Advanced Manager server sees the connection, each extender is displayed in the administrator view of the dashboard, and is ready for configuration.

To prevent overwriting configurations, if you have initially configured your extender with the System Configuration utility, you must perform a factory reset on the extender before adding it into the HMX Advanced Manager software. For more information to factory reset the transmitters and receivers, see the Avocent® HMX High Performance KVM Extender System Installer/User Guide.

When adding an extender, if the extender is not located by the HMX Advanced Manager software, proceed as follows.

To add a new extender:

1. Connect the extender unit to the network and ensure it is turned on.
2. On a local computer connected to the same subnet as the extender, log in to the HMX Advanced Manager server as **admin**.

3. Verify the extender is displayed at the top of the Dashboard screen. If not, verify the following:
 - The extender is using the factory default settings.
 - The extender is located in the same Ethernet segment as the HMX Advanced Manager server.
 - The extender and the extender cables are connected properly.
4. For a single extender, click *Configure*.
-or-
For multiple extenders, click *Configure All New Devices*.
5. Click the configuration icon and on the Configure New devices screen, enter a new IP address for each extender.
6. Enter a unique description and location for each extender.

NOTE: If necessary, click the extender icon to flash the front panel indicator and confirm the location.

7. Click Save to restart the new extender to save the new IP address.

NOTE: The extenders can be updated from the relevant transmitter and receiver screens.

3.2.1 Channels tab

The Channels tab provides access to all settings and options related directly to the video, audio and USB streams, collectively known as channels, emanating from any number of transmitters. From this tab, you can view and add channels and channel groups.

View Channels

The View Channels screen lists all channels that currently exist in the HMX Advanced Manager system. A channel is automatically created for every transmitter when it is added and configured in the HMX Advanced Manager network. The new default channel for each added transmitter inherits the name of the transmitter. These default names can be altered at any time. New channels can be created manually.

In the list of channels, the Allowed Connections column indicates how each channel can be accessed by users. By default, these settings are inherited from the global setting, however, each channel can be modified as required.

To add a channel:

1. Click the *Channels* tab and click *Add Channel*.
2. Enter the Channel Name, Description and Location.
3. Using the drop-down menus, select the available video, audio, USB and serial stream from the transmitter. You can select all four streams from the same transmitter or select the streams from different transmitters.

NOTE: Where necessary, channels can be created without video, audio, USB and/or serial. Only one receiver can use the serial port of a transmitter at any time.

4. Select the type of Allowed Connections.

NOTE: This setting for each channel designates if exclusive access is permitted. If you deny exclusive access rights, exclusive access for any user cannot take place for this channel, regardless of other settings.

5. Select the Group Membership and Permissions for the channel and click Save. The channel automatically inherits the key settings of that group.

To add a channel group:

1. Click the *Channels* tab and click *Add Channel Group*.

2. Enter the Channel Group Name and Description.
3. Select the Group Membership and Permissions for the channel group and click Save. The Group Membership and Permissions sections use the same method to determine inclusion and exclusion.

To add a channel to a group membership or permission:

Select the channel from the left column and add it to the right column.

3.2.2 Receivers tab

The Receivers tab displays a table of all receiver devices in the HMX Advanced Manager network. From this tab you can view or search for receivers, create or delete receivers, view receiver groups or update the receiver firmware.

To add a Receiver Group:

1. From the Receiver tab, click *Add Receiver Group*.
2. Enter a unique Group name and Description.
3. Select the appropriate radio button for Login Required. If *No*, anyone can use the receiver and connect to a channel.
4. Select the appropriate radio button for Enable OSD Alerts.
5. Select the appropriate radio button for Enable Video Compatibility Check. This option reads the EDID from the attached monitor and determines if the monitor is capable of displaying the selected video mode before connecting to the channel.
6. Select Force 60Hz option, as desired. If enabled, the receiver frame rate is held at 60Hz regardless of the video input frame rate.

NOTE: The Video Switching options cannot be altered when this option is enabled.

7. Select the appropriate video switching option.
 - Fast Switching (default state) - Retains the same frame rate (at either 50Hz or 60Hz) depending upon which video resolution was displayed first.
 - Match Frame Rate - Follows the source frame rate and will change the frame rate every time this changes even if the video resolution doesn't change.
8. Select the Group Memberships and Permissions for the group and click Save.

3.2.3 Transmitters tab

The Transmitters tab displays all transmitter devices in the HMX Advanced Manager network. Individual transmitters can be edited by selecting the pencil icon in the manage column. Changes made on this screen override global settings. For more information on the options available, see [Settings - Transmitters button on page 16](#).

3.2.4 Managers tab

The Managers tab displays all servers in the HMX Advanced Manager network. Basic settings are editable. For installations that require greater redundancy, it is possible to have two HMX Advanced Manager servers running on the same subnet.

Table 3.16 Manager Roles

Role	Description
Unconfigured	The server is a factory fresh device or a factory reset has been performed.
Solo	The solo server is a standalone HMX Advanced Manager server. If there is only one HMX Advanced Manager on the subnet, this is the role that is used. All HMX Advanced Manager servers with firmware less than 4.1 are set to the solo role.
Primary	The primary server is configured as a fully functional HMX Advanced Manager server.
Backup	The backup server is configured to serve as a backup to the primary server.

The server status on the Managers tab cannot be edited, but the following are the available status options.

Table 3.17**Server Status**

Status	Description
Active	The server is functioning as an HMX Advanced Manager server and is administering extenders. Primary or solo servers with this status are fully functional HMX Advanced Manager servers that accept network configuration changes. A backup server with this status functions as an Active primary server. It executes channel changes, but does not accept network configuration changes.
Standby	The standby server maintains its database as a copy of the primary server in readiness to take over, if necessary.
Offline	The offline server is not able to obtain a copy of the database.
Initializing	The initial status after the server starts up.
Quiescent	An active server on the network, but cannot function. Typically you will see this status if there are two primary servers on the same subnet.
Failed	The server has failed.

3.2.5 Users tab

The Users tab displays all users in the HMX Advanced Manager network. From this tab, you can view or search for users, create or delete users and view user groups. The two types of users in the HMX Advanced Manager system are:

- Admin users - can access the HMX Advanced Manager software and change the operation of the software.
- Regular users - can access one or more computers that are linked to the HMX transmitters. The HMX receiver provides an On Screen Display (OSD) that lists all the accessible computers and allows permitted access.

The View Users screen displays information about each user. The users can be edited by selecting the pencil icon in the manage column. In the list, the admin user is always present and cannot be deleted. The username and details of the admin account can be edited as required.

Table 3.18 User Information

Field	Description
AD	Indicates if the user is imported from Active Directory.
Username	Account username.
User Groups	Number of groups to which the user belongs.
Channels	Number of channels the user can access.
Receivers	Number of receivers the user can access.
Allow Exclusive	Indicates if the user is permitted to access channels in exclusive mode. Options are: Yes, No or Inherited.
Suspended	Indicates if the user account is suspended.
HMX Advanced Manager Admin	Indicates if the user has admin privileges.

Permissions

Permissions between a user and a receiver can be applied in any of the following ways:

- User to Receiver
- User to User Group to Receiver
- User to User Group to Receiver Group to Receiver
- User to Receiver Group to Receiver

To add a user:

1. From the Users tab, click *Add User*.
2. Enter a unique Username, First Name, Last Name and Email.
3. Select the appropriate Required Password option.
4. If a password is required, enter the password twice.
5. Select the HMX Admin option to deny or grant admin rights.
6. Select the appropriate Account Suspended option.
7. Select the Allow Private Mode option to designate if the user is able to connect to channels exclusively. When this option is set to Inherit from user groups/Global Setting, if any user or group that this user is a member of is granted exclusive permission, this user also has exclusive access.
8. Select the Enable Remote OSD option to deny or grant permission to the selected user to use the remote OSD functionality that allows access to remote receivers. Access allows the user to change channels or presets even though the user has not logged into those receivers.
9. Select the Group Membership and Permissions for the user and click *Save*

NOTE: By default, all users are initially granted permission to all receivers.

To add a user group:

1. From the Users tab, click *Add User Group*.
2. Enter a unique User Group Name.
3. Select the Allow Private Mode option to designate if the user group is to connect to channels exclusively.
4. Select the Enable Remote OSD option to deny or grant permission to the selected user group to use the remote OSD functionality that allows access to remote receivers.
5. Select the Group Membership and Permissions for the user group and click *Save*

Active Directory

To simplify integration with existing systems in your organization, the HMX Advanced Manager software can be synchronized with an LDAP or Active Directory server. This allows a list of users and user groups, along with their usernames and group memberships to be imported.

NOTE: If a user is synced with Active Directory, it is not possible to change the Username, First/Last Name, Password, or User Group membership. These items must be edited on the Active Directory server and the changes will filter through to HMX Advanced Manager software the next time a sync takes place with Active Directory.

To configure Active Directory:

NOTE: Active Directory must be enabled on the *Dashboard - Settings - Active Directory* screen before integration. For more information on Active Directory setup, see [Settings](#) on page 14.

1. From the *Dashboard - Settings* screen, configure the Active Directory server.
2. Scan the AD server for a list of folders and users/groups within those folders.
3. Once scanned, the Import Users from Active Directory screen shows all folders that are available on the AD server.
4. Use the *Include Users* and *Include Groups* checkbox columns on the right to select which items to import.
 - a. If an AD user was not in the HMX Advanced Manager user database, they are imported.
 - b. If an AD user is already in the HMX Advanced Manager user database, they are kept.
 - c. If an AD user is not marked for Import/Sync from the AD import screen, and they already exist in the HMX Advanced Manager user database, they are removed from the HMX Advanced Manager user database during the sync operation.

NOTE: To prevent the removal of users from the HMX Advanced Manager system, always select all users for Import/Sync.

5. Select the required *Re-Synchronize* interval.
6. Select to synchronize immediately.

-or-

Click *Preview* to view the list of users to be added/updated/ removed for this synchronization.

7. If changes are necessary, return to the filter screen and edit your settings.
8. When configuration is complete, click *Save and Sync* to synchronize the selected items in the HMX Advanced Manager user database.

NOTE: The HMX Advanced Manager server only imports folders/groups/users up to the limit set by the AD server. Any users/groups beyond the limit are not imported.

3.2.6 Presets tab

A preset allows multiple receivers to switch between transmitters using a single action. Administrators can create new presets or configure existing presets. The presets table displays the preset name, description, allowed connection modes and the number of receiver-channel pairs in the preset. If any preset-pairs are configured incorrectly, a warning triangle appears and the preset is not usable.

NOTE: Permissions are not configured for a preset. Instead, a preset is available to users who have permission to use all receivers and channels in the preset.

To add presets:

1. From the Presets tab, click *Add Preset*.

2. Enter a Preset Name and Description.
3. From the drop-down menu, select a receiver and a channel for Pair 1.
4. Click *Add another pair* to define another pair and repeat the previous step.

NOTE: While channels can be assigned to multiple receivers, each receiver can only appear once in a single preset.

5. Select an Allowed Connections option and click Save.

NOTE: If multicasting is present, it is not possible to choose the Exclusive only connection mode.

3.2.7 Statistics tab

The Statistics tab displays a range of real-time data measurements related to links in the HMX Advanced Manager network. The statistics are useful for troubleshooting or optimization purposes.

To view statistics:

1. From the *Statistics* tab, click the graph icon for the extender.
2. Click the name of an extender to display its available statistics in a dynamic graph.

This page intentionally left blank

4 External API

The HMX Advanced Manager API version 4 allows external applications to access key routines in the HMX Advanced Manager software.

Table 4.1 Methods

Action	Command
login	(http://<HMX Manager.ip.address>/api/#login)
info	(http://<HMX Manager.ip.address>/api/#info)
logout	(http://<HMX Manager.ip.address>/api/#logout)
get_devices	(http://<HMX Manager.ip.address>/api/#get_devices)
get_channels	(http://<HMX Manager.ip.address>/api/#get_channels)
get_presets	(http://<HMX Manager.ip.address>/api/#get_presets)
connect_channel	(http://<HMX Manager.ip.address>/api/#connect_channel)
connect_preset	(http://<HMX Manager.ip.address>/api/#connect_preset)
disconnect_channel	(http://<HMX Manager.ip.address>/api/#disconnect_channel)
disconnect_preset	(http://<HMX Manager.ip.address>/api/#disconnect_preset)
create_preset	(http://<HMX Manager.ip.address>/api/#create_preset)
delete_preset	(http://<HMX Manager.ip.address>/api/#delete_preset)
create_channel	(http://<HMX Manager.ip.address>/api/#create_channel)
delete_channel	(http://<HMX Manager.ip.address>/api/#delete_channel)

Login

The API requires a valid user login to be presented in the first request. The API returns an authentication code, which must be passed in all future requests. This authentication code can be reused until a log out request is made, at which point the authentication code is longer valid.

The concept of an anonymous user can apply to the API. If no login username and password are provided, the API returns an authentication token for the anonymous user (either the same one as for the OSD or a created anonymous API user account).

Table 4.2 Input Parameters

Parameter	Description
username	Current user
password	Current user password
v	HMX Manager API version for this request

Table 4.3 Output Values

Value	Description
version	Current API version number
timestamp	Current server time
success	0 = fail, 1 = success
token	Authentication code for future API requests

Examples

Input

```
/api/?v=1&method=login&username=xxxxx&password=xxxxx
```

Output

```
<api_response>
<version>1</version>
<timestamp>2012-12-14 12:12:12</timestamp>
<success>1</success>
<token>5cf494a71c29e9465a57a81e0a2d602c</token>
</api_response>
or
<api_response>
<version>1</version>
<timestamp>2012-12-14 12:12:12</timestamp>
<success>0</success>
<errors>
<error>
<code>2</code>
<msg>Invalid username or password</msg>
</error>
</errors>
</api_response>
```

Logout

The authentication token provided by the Login function can be used until the logout function is called.

Table 4.4 Input Parameters

Parameter	Description
token	Authentication code for future API requests
v	HMX Manager API for this request

Table 4.5 Output Values

Value	Description
timestamp	Current server time
success	0 = fail, 1 = success

Examples

Input

```
/api/?method=logout&token=xxxxx&v=1
```

Output

```
<api_response>
<version>1</version>
<timestamp>2011-02-04 15:24:15</time>
<success>1</success>
</api_response>
or
<api_response>
<version>1</version>
<timestamp>2012-12-12 12:12:12</timestamp>
<success>0</success>
<errors>
<error>
<code>3</code>
<msg>Error logging out (you may already have logged out)</msg>
</error>
</errors>
</api_response>
```

get_devices

The get_devices function returns a list of devices.

Table 4.6 Input Parameters

Parameter	Description
token	Authentication code for future API requests
v	HMX Manager API version for this request
device_type	Receivers = rx, transmitters = tx; default = rx
filter_d_name	Device name search string, optional
filter_d_description	Device name search string, optional
filter_d_location	Device name search string, optional
sort	Sorts results by name/description/location; default = name, optional
sort_dir	Optional; sort direction for results asc/desc; default = asc
status	Optional; ";outdated_HMX Manager_ip';rebooting';offline';outdated_firmware';invalid_backup_firmware';rebooting';upgrading_firmware';backup_mode'
show_all	Optional; if configured and not blank, shows all receivers, not just those the logged-in user is permitted to use
page	Page number to start showing results; default = 1
results_per_page	Number of results per page. Default = 1000

Table 4.7 Output Values

Value	Description
version	Current API version number
timestamp	Current server time
success	0 = fail, 1 = success
page	Page number
results_per_page	Number of results per page; default is unlimited
total_devices	Total number of devices.
count_devices	<p>Number of devices on this page.</p> <p>For each device:</p> <p>attribute: item</p> <p>d_id (device id)</p> <p>d_mac_address (MAC address for interface 1)</p> <p>d_mac_address2 (MAC address for interface 2)</p> <p>d_name (device name)</p> <p>d_online (0 = interface 1 offline, 1 = interface 1 online)</p> <p>d_online2 (0 = interface 2 offline, 1 = interface 2 online)</p> <p>d_type (rx, tx)</p> <p>d_version (1 = ALIF1000R/ALIF1000T, 2 = all other devices)</p> <p>d_variant ('b' = ALIF2002T, 'v' = ALIF2112T, 's' = ALIF1002R/ALIF1002T, 't' = ALIF2020R/ALIF2020T)</p> <p>d_ip_address (IP address for interface 1)</p> <p>d_ip_address2 (IP address for interface 2)</p> <p>d_description (device description)</p> <p>d_location (device location)</p> <p>d_configured (0 = no, 1 = yes)</p> <p>d_valid_firmware (0 = no, 1 = yes)</p> <p>d_valid_backup_firmware (0 = no, 1 = yes)</p> <p>d_firmware (Firmware version. For example, 2.5.17879)</p> <p>d_backup_firmware (backup firmware version)</p> <p>d_date_added (Date device added to HMX Manager network. For example, 2012-07-13 22:17:22)</p> <p>d_status (0 = device offline, 1 = device online, 2 = rebooting, 4 = firmware_upgrading, 6 = running backup firmware)</p>

The following property is only returned for transmitters:

count_transmitter_channels (the number of channels containing this transmitter)

The following properties are only returned for receivers:

- con_exclusive (0/1 - if the last connection is/was in exclusive mode)
- con_control (0/1 - if the last connection has/had USB enabled)
- con_start_time (start time of last connection e.g. 2012-09-07 13:33:17)
- con_end_time (empty if connection still active, else date/time the connection was ended. For example, 2012-09-07 13:33:17)
- u_username (username of the user who initiated the last connection)

- u_id (user ID of the user who initiated the last connection)
- c_name (name of the channel last connected)
- count_receiver_groups (the number of receiver groups this receiver is a part of)
- count_receiver_presets (the number of presets this receiver is a part of)
- count_users (the number of users who have access to this receiver)

Examples

Input

```
/api/?v=2&method=get_devices&token=xxxxx  
/api/?v=2&method=get_devices&device_type=tx&page=2&results_per_page=3&token=xxxxx
```

Output

```

<api_response>
<version>2</version>
<timestamp>2012-09-12 14:56:11</timestamp>
<success>1</success>
<page>2</page>
<results_per_page>3</results_per_page>
<total_devices>12</total_devices>
<count_devices>3</count_devices>
<devices>
<device item="4">
<d_id>170</d_id>
<d_mac_address>00:0F:58:01:6E:3D</d_mac_address>
<d_mac_address2>00:0F:58:5B:6E:3D</d_mac_address2>
<d_name>RX 123</d_name>
<d_online>1</d_online>
<d_online2>0</d_online2>
<d_type>rx</d_type>
<d_version>2</d_version>
<d_variant></d_variant>
<d_ip_address>10.10.10.66</d_ip_address>
<d_ip_address2>10.10.10.67</d_ip_address2>
<d_description></d_description>
<d_location>Server Rack 3</d_location>
<d_configured>1</d_configured>
<d_valid_firmware>1</d_valid_firmware>
<d_valid_backup_firmware>1</d_valid_backup_firmware>
<d_firmware>2.3.16682</d_firmware>
<d_backup_firmware>2.3.16682</d_backup_firmware>
<d_date_added>2012-07-14 01:37:07</d_date_added>
<d_status>1</d_status>
<con_exclusive>0</con_exclusive>
<con_control>1</con_control>
<con_start_time>2012-09-07 13:33:19</con_start_time>
<con_end_time/>
<u_username>admin</u_username>
<u_id>1</u_id>
<c_name>Channel 1</c_name>
<count_receiver_groups>1</count_receiver_groups>
<count_receiver_presets>2</count_receiver_presets>
<count_users>1</count_users>
</device>
</devices>

```

```

</api_response>
<api_response>
<version>2</version>
<timestamp>2012-09-12 14:56:11</timestamp>
<success>1</success>
<page>1</page>
<results_per_page>1</results_per_page>
<total_devices>1</total_devices>
<count_devices>1</count_devices>
<devices>
<device item="1">
<d_id>64</d_id>
<d_mac_address>00:0F:58:01:56:85</d_mac_address>
<d_mac_address2>00:0F:58:5B:56:85</d_mac_address2>
<d_name>TX 456</d_name>
<d_online>0</d_online>
<d_online2>0</d_online2>
<d_type>tx</d_type>
<d_version>1</d_version>
<d_variant></d_variant>
<d_ip_address>1.1.201.31</d_ip_address>
<d_ip_address2>1.1.201.32</d_ip_address2>
<d_description></d_description>
<d_location></d_location>
<d_configured>1</d_configured>
<d_valid_firmware>1</d_valid_firmware>
<d_valid_backup_firmware>1</d_valid_backup_firmware>
<d_firmware>2.1.15747</d_firmware>
<d_backup_firmware>2.1.15747</d_backup_firmware>
<d_date_added>2012-07-13 17:50:04</d_date_added>
<d_status>0</d_status>
<count_transmitter_channels>3</count_transmitter_channels>
</device>
</devices>
</api_response>

```

get_channels

The get_channels function returns a list of channels available to the authenticated user for a specific receiver.

Table 4.8 Input Parameters

Parameter	Description
token	Authentication code for future API requests
v	HMX Manager API version for this request
device_id	ID of the receiver connected to this channel; recommended to ensure full checks for connection mode availability
filter_c_name	Channel name search string
filter_c_description	Channel name search string
filter_c_location	Channel name search string
filter_favourites	Set this non-empty to only show the favorites of the user
page	Page number to start showing results; default = 1
results_per_page	Number of results per page; default = 1000

Table 4.9 Output Values

Value	Description
version	Current API version number
timestamp	Current server time
success	0 = fail, 1 = success
page	Page number
results_per_page	Number of results per page; default = unlimited
count_channels	Number of channels on this page available to the authenticated user For each channel: attribute: item (for example, 17th channel) c_id (channel id) c_name (channel name) c_description (channel description) c_location (channel location) c_favourite (True if this channel is in user favorites, 0-9 if it is a numbered shortcut)
view_button	disabled/enabled/hidden - if the user can connect to the preset in view-only mode disabled - not allowed because it is in use by someone else, hidden = never, enabled = yes Not necessarily an accurate indication that other connections may interfere if the device_id of the proposed receiver in the connection is not provided
shared_button	Disabled/enabled/hidden, but in shared mode
exclusive_button	Disabled/enabled/hidden, but in exclusive mode
c_video1	Device ID
c_video1_head	1 2
c_video2	Device ID
c_video2_head	1 2
c_audio	Device ID
c_usb	Device ID
c_serial	Device ID

Examples

Input

```
/api/?v=2&method=get_channels&token=xxxxx
```


Output

```

<api_response>
<version>2</version>
<timestamp>2012-12-14 12:12:12</timestamp>
<success>1</success>
<page>1</page>
<results_per_page>10</results_per_page>
<count_channels>2</count_channels>
<channel item="1">
<c_id>3</c_id>
<c_name>Channel 1</c_name>
<c_description>Description for Channel 1</c_description>
<c_location>Location of Channel 1</c_location>
<c_favourite>>false</c_favourite>
<view_button>disabled</view_button>
<shared_button>disabled</shared_button>
<exclusive_button>disabled</exclusive_button>
</channel>
<channel item="2">
<c_id>5</c_id>
<c_name>Channel 2</c_name>
<c_description>Description for Channel 2</c_description>
<c_location>Location of Channel 2</c_location>
<c_favourite>2</c_favourite>
<view_button>disabled</view_button>
<shared_button>enabled</shared_button>
<exclusive_button>hidden</exclusive_button>
</channel>
</api_response>

```

get_presets

The `get_presets` function returns a list of presets available to the authenticated user.

Table 4.10 Input Parameters

Parameter	Description
token	Authentication code for future API requests
v	HMX Manager API version for this request
results_per_page	Number of results per page; default is 1000
page	Page number to start showing results for; default is 1

Table 4.11 Output Values

Value	Description
version	Current API version number
timestamp	Current server time
success	0 = fail, 1 = success
page	Page number
results_per_page	Number of results per page; default = unlimited
total_presets	Total number of presets available to the authenticated user
count_presets	Number of presets on this page available to the authenticated user For each connection_preset: <ul style="list-style-type: none"> • attribute: item (for example, 17th preset) • cp_id (preset id) • cp_name (preset name) • cp_description (preset description) • cp_pairs (number of channel-receiver pairs in this preset)
problem_cp_pairs	Number of channel-receiver pairs that are mis-configured (for example, receiver offline or receiver not defined)
cp_active	If all, any or none of the channel-receiver pairs in this preset are currently connected; values are full, partial and none
connected_rx_count	Number of receivers in this preset that are already connected
view_button	Disabled/enabled/hidden - if the user can connect to the preset in view-only mode Disabled = no; it is in use by someone else, enabled = yes, hidden = never
shared_button	Disabled/enabled/hidden, but in shared mode
exclusive_button	Disabled/enabled/hidden, but in exclusive mode

Examples

Input

```
/api/?v=1&method=get_presets&token=xxxxx
```

Output

```

<api_response>
<version>1</version>
<timestamp>2012-12-14 12:12:12</timestamp>
<success>1</success>
<page>1</page>
<results_per_page>10</results_per_page>
<total_presets>2</total_presets>
<count_presets>2</count_presets>
<connection_preset item="1">
<cp_id>3</cp_id>
<cp_name>Preset 1</cp_name>
<cp_description>Description for Preset 1</cp_description>
<cp_pairs>1</cp_pairs>
<problem_cp_pairs/>
<cp_active>full</cp_active>
<connected_rx_count>1</connected_rx_count>
<view_button>disabled</view_button>
<shared_button>disabled</shared_button>
<exclusive_button>disabled</exclusive_button>
</connection_preset>
<connection_preset item="2">
<cp_id>4</cp_id>
<cp_name>Preset 2</cp_name>
<cp_description>Description for Preset 2</cp_description>
<cp_pairs>2</cp_pairs>
<problem_cp_pairs/>
<cp_active>none</cp_active>
<connected_rx_count/>
<view_button>enabled</view_button>
<shared_button>hidden</shared_button>
<exclusive_button>hidden</exclusive_button>
</connection_preset>
</api_response>

```

connect_channel

The connect_channel function connects a receiver to a channel.

Table 4.12 Input Parameters

Parameter	Description
token	Authentication code for future API requests
v	HMX Manager API version for this request
c_id	ID of the channel acquired from get_channels
rx_id	ID of the receiver acquired from get_receivers
view_only	Options are 0/1; default = 0; optional
exclusive	Options are 0/1; default = 0; optional

Table 4.13 Output Values

Value	Description
version	Current API version number
timestamp	Current server time
success	0 = fail, 1 = success
errors	Details about returned errors

Examples

Input

```
/api/?v=2&method=connect_channel&token=xxxxx&c_id=1&rx_id=2&exclusive=1
```

Output

```
<api_response>
<version>2</version>
<timestamp>2012-12-12 12:12:12</timestamp>
<success>1</success>
</api_response>
or
<api_response>
<version>2</version>
<timestamp>2012-12-12 12:12:12</timestamp>
<success>0</success>
<errors>
<error>
<code>231</code>
<msg>ERROR - exclusive connection not available</msg>
</error>
</errors>|
</api_response>
```

connect_preset

The connect_preset function connects all channel-receiver pairs in a preset.

Table 4.14 Input Parameters

Parameter	Description
token	Authentication code for future API requests
v	HMX Manager API version for this request.
id	ID of the preset acquired from get_presets.
force	Determines whether to ignore errors with the preset pairs. optional, 0/1; default = 0
view_only	Optional, 0/1; default = 0
exclusive	Optional, 0/1; default = 0

Table 4.15 Output Values

Value	Description
version	Current API version number
timestamp	Current server time
success	0 = fail, 1 = success
errors	Details on errors are returned

Examples

Input

```
/api/?v=1&method=connect_preset&token=xxxxx&id=1&force=1
```

Output

```
<api_response>
<version>1</version>
<timestamp>2012-12-12 12:12:12</timestamp>
<success>1</success>
</api_response>
or
<api_response>
<version>1</version>
<timestamp>2012-12-12 12:12:12</timestamp>
<success>0</success>
<errors>
<error>
<code>210</code>
<msg>”.$config[‘error_codes’][210].”</msg>
</error>
</errors>
</api_response>
```

disconnect_channel

The disconnect_channel function disconnects a receiver, a number of receivers or all connected receivers.

Table 4.16 Input Parameters

Parameter	Description
token	Authentication code for future API requests
v	HMX Manager API version for this request
rx_id	ID of the receiver as an integer or comma-separated set of integers; optional, if not supplied all connections will end
force	Determine whether to disconnect existing connections by other users or for offline receivers

Table 4.17 Output Values

Value	Description
version	Current API version number
timestamp	Current server time
success	0 = fail; 1 = success
errors	Details on errors are returned

Examples

Input

```
/api/?v=2&method=disconnect_channel&token=xxxxx&rx_id=1
/api/?v=2&method=disconnect_channel&token=xxxxx&rx_id=1,2,3
/api/?v=2&method=disconnect_channel&token=xxxxx&force=1
```

Output

```
<api_response>
<version>2</version>
<timestamp>2012-12-12 12:12:12</timestamp>
<success>1</success>
</api_response>
```

disconnect_preset

The `disconnect_preset` function disconnects all channel-receiver pairs in a preset or disconnects all connections in the whole HMX Manager network.

Table 4.18 Input Parameters

Parameter	Description
token	Authentication code for future API requests
v	HMX Manager API version for this request
id	If not supplied, all connections end; optional
force	Determines whether to ignore errors with some of the preset pairs

Table 4.19 Output Values

Value	Description
version	Current API version number
timestamp	Current server time
success	0 = fail, 1 = success
errors	Details on errors are returned

Examples

Input

```
/api/?v=1&method=disconnect_preset&token=xxxxx&id=1&force=1
```

Output

```
<api_response>
<version>1</version>
<timestamp>2012-12-12 12:12:12</timestamp>
<success>1</success>
</api_response>
```

create_preset

The create_preset function creates a new preset. The API user must have admin privileges to call this method successfully.

Table 4.20 Input Parameters

Parameter	Description
token	Authentication code for future API requests
v	HMX Manager API version for this request
name	Display name for the new preset
pairs	A comma-separated list of the channel ID and receiver ID pairs for the preset; each ID in the pair is separated by a hyphen
allowed	Permitted connection modes for the preset; optional, if omitted, the global setting is inherited Permitted values: v - view only vs - view and shared only s - shared only e - exclusive only vse - any mode allowed

Table 4.21 Output Values

Value	Description
version	Current API version number
timestamp	Current server time
success	0 = fail, 1 = success
errors	Details on errors are returned
id	ID of the new preset, if it was created

Examples

Input

```
/api/?v=3&method=create_preset&token=xxxxx&name=my_preset&pairs=1-1,1-2,2-3,2-4&allowed=vs
```

Output

```
<api_response>
<version>3</version>
<timestamp>2012-12-12 12:12:12</timestamp>
<success>1</success>
<id>5</success>
</api_response>
```

delete_preset

The delete_preset function deletes a preset. The API user must have admin privileges to call this method successfully.

Table 4.22 Input Parameters

Parameter	Description
token	Authentication code for future API requests
v	HMX Manager API version for the request
id	ID of the preset to be deleted

Table 4.23 Output Values

Value	Description
version	Current API version number
timestamp	Current server time
success	0 = fail, 1 = success
errors	Details on errors are returned

Examples

Input

```
/api/?v=3&method=delete_preset&token=xxxxx&id=5
```

Output

```
<api_response>
<version>3</version>
<timestamp>2012-12-12 12:12:12</timestamp>
<success>1</success>
</api_response>
```

create_channel

The create_channel function creates a new channel. The API user must have admin privileges to call this method successfully. Although the source device ID inputs are each optional, at least one is required.

Table 4.24 Input Parameters

Parameter	Description
token	Authentication code for future API requests
v	HMX Manager API version for the request
name	Name for the new channel
desc	Description for the new channel; optional; default = empty
loc	Location for the new channel; optional; default = empty
allowed	Permitted connection modes for the channel; optional; if omitted, the global setting is inherited Permitted values: v - view only vs - view and shared only s - shared only e - exclusive only vse - any mode allowed
video1	Device ID of video source 1
video1head	Video head number for source 1
video2	Device ID of video source 2
video2head	Video head number for source 2
audio	Device ID of the audio source
usb	Device ID of the USB source
serial	Device ID of the serial source.

Table 4.25 Output Values

Value	Description
version	Current API version number
timestamp	Current server time
success	0 = fail, 1 = success
errors	Details on errors are returned
id	ID of the new channel

Examples

Input

```
/api/?v=4&method=create_channel&token=xxxxx&name=my_channel&video1=21&audio=81
```

Output

```
<api_response>
<version>3</version>
<timestamp>2012-12-12 12:12:12</timestamp>
<success>1</success>
<id>91</success>
</api_response>
```

delete_channel

The function is used to delete a channel. The user must have admin privileges to call this method successfully.

Table 4.26 Input Parameters

Parameter	Description
token	Authentication code for future API requests
v	HMX Manager API version for the request
id	ID of the preset to be deleted

Table 4.27 Output Values

Value	Description
version	Current API version number
timestamp	Current server time
success	0 = fail, 1 = success
errors	Details on errors are returned

Examples

Input

```
/api/?v=4&method=delete_channel&token=xxxxx&id=5
```

Output

```
<api_response>
<version>4</version>
<timestamp>2012-12-12 12:12:12</timestamp>
<success>1</success>
</api_response>
```

This page intentionally left blank

Appendices

Appendix A: Technical Specifications

Table A.1 Technical Specifications

Category	Value
Hardware and Software Specifications	
Hardware	Single-board computer with solid state memory
Software	Closed system with bespoke application preloaded
Mechanical	
Dimensions (W x D x H)	8.3 x 8.5 x 1.6 inches (210 x 215 x 40 mm)
Weight (without cables)	4 pounds (1.8 kg)
Power	
Connector	3-pin locking plug
DC Power	12VDC, 5A max
AC Input Range	100-240 VAC, 50/60 Hz
Power Consumption	20W (typical)
Permitted Operational Ambient Conditions	
Operating Temperature	0 to 40° C / 32 to 104° F
Relative Humidity	10-90% non-condensing
Permitted Altitude	<2000 m
Approvals	CE, FCC

Appendix B: Advanced USB Features

The Avocent HMX Advanced Manager has four advanced USB features:

- Device merging
- Port reservation
- Flow control
- USB quirks or advanced features

NOTE: For the advanced USB features to work, both endpoints must be on the same firmware version. For USB flow control to be enabled, all endpoints must be at version 3.5 or above.

B.1 Device merging

Device merging is the default setting on the receiver. It allows multiple equivalent USB human interface devices (HID) to be combined to appear as a single device. The HID devices must have the same vendor ID and product ID to bypass the 13 device limitation on devices connecting to a single USB hub. All devices attached to a port with the merge capability disabled are treated as individual devices.

NOTE: Merging does not work for all USB devices.

B.2 Port control

The transmitter reports itself as a 13-port USB hub. Up to 13 devices can be allocated to ports beginning with the lowest available port number. Though port allocation is sequential, it is random because each device is connected to the next available port.

Issues arise when a driver is looking for a device on a specific USB port. Allocated ports can change when receivers are switched away from and reconnected to the transmitter, and this can prevent the device driver from finding the device on a specified port. To overcome this issue, it is possible to reserve a number of USB ports on the transmitter and assign a reserved port to a particular device on the receiver. This feature is required for a unit receiver using dual touch screens. If the touch screen's port number changes, control of the screen also changes. Reserving the USB port for a particular screen prevents this from happening.

B.3 Flow control

USB flow control is required for a number of more complex USB peripherals including some touch screens and multifunction combined devices.

B.4 USB quirks

Some USB devices may have delay or configuration issues when used with the unit. The advanced USB settings allow quirks to be applied. Quirks are used to instruct USB devices to deviate from normal operating behaviors to facilitate compatibility with the unit.

You can control quirks from the USB Advanced Settings page by adding a kernel or user code in the appropriate field. There are two input methods depending on if the unit is being used point to point via the receivers' web interface or if the unit's receivers and transmitters are under HMX control. HMX requires the codes to be entered as a decimal value and the units require them to be entered as a Hex value.

Known device codes

The following table lists the devices that require an advanced USB code and the associated settings. Point-to-point (P-P) mode refers to when the web server on the individual units is used to set up the device.

Table B.1 Known USB Device Codes

USB Device	P-P Kernel Code	P-P User Code	HMX Kernel Code	HMX User Code	FW Version
Eizo cx240 screen with Colormunki	0x0	0x0AEA	0	2794	3.1
Eizo CG276 monitor	0x0	0x0AEA	0	2794	3.1
Thrustmaster HOTAS joystick	0x0	0x0AAC	0	2732	3.1
Mousetrappor Office	0x4	0x0	4	0	3.1
Logitech K310 keyboard	0x4	0	4	0	3.1
Logitech illuminated keyboard	0x4	0	4	0	3.1
Microsoft wired 600 keyboard	0x0	0x0ABA	0	2746	3.1
Wacom Intuos 4 tablet	0x0	0x0	0	0	3.1
Newtek Tricaster	0x0	0x1000AAA	0	16779946	3.5
ELO ET2201L Touch screen	0x0	0x1000AAA	0	16779946	3.5
PQlabs pqp4a2101 touch panel	0x4	0x1000AAA	4	16779946	3.5
Dell KB813Combined Keyboard + CAC	0x0	0x1000AAA	0	16779946	3.5
Cherry ST-2000 card reader	0x0	0x1000AAA.	0	16779946	3.5
Dell SK3205 card reader	0x0	0x1000AAA.	0	16779946	3.5
Disable Logitech Set point	0x0	0x0AAE	0	2734	4.1

Point to point set up

You need to reserve a number of USB ports for a point-to-point setup.

To set up a quirk:

1. Navigate to the transmitter USB settings page.
2. For the receiver, click *enable advanced features*, set the appropriate quirk codes and click *save*.

HMX control set up

From HMX ensure that a number of USB ports are reserved. This can be done from the global or local settings.

To set up HMX control:

1. At the receiver, select a device from the Advanced Port Features drop-down list on the Configure USB Receiver settings page.
-or-
Create a new device if you have been given a new code to try.
2. Refer to the list in this document for the features of each firmware version.

Connect with Vertiv on Social Media



<https://www.facebook.com/vertiv/>



<https://www.instagram.com/vertiv/>



<https://www.linkedin.com/company/vertiv/>



<https://www.twitter.com/Vertiv/>



Vertiv.com | Vertiv Headquarters, 1050 Dearborn Drive, Columbus, OH, 43085, USA

© 2021 Vertiv Group Corp. All rights reserved. Vertiv™ 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. Specifications, rebates and other promotional offers are subject to change at Vertiv's sole discretion upon notice.