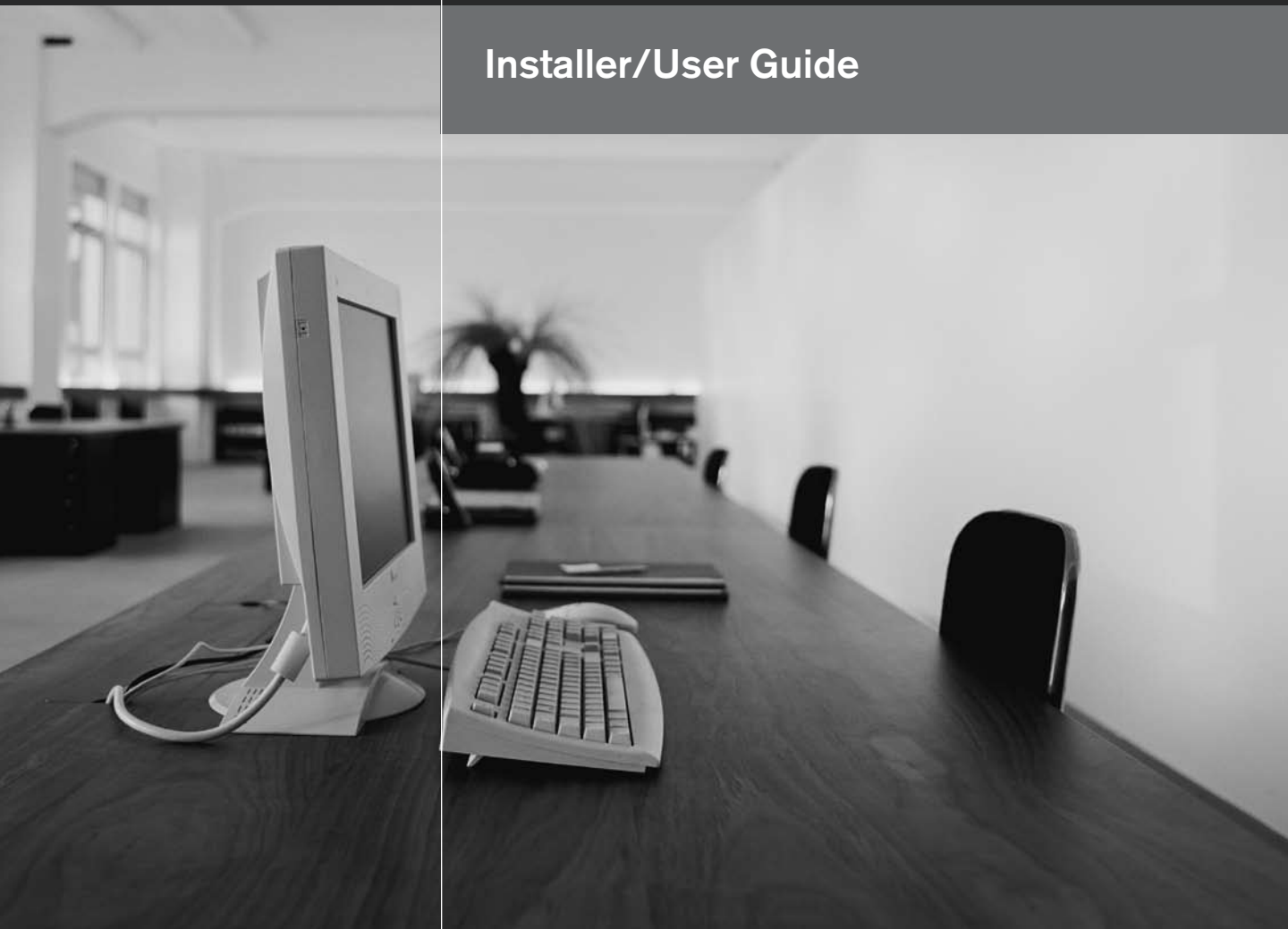
Avocent®

HMX Manager

Installer/User Guide



EMI Statements

USA

Warning: Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Canadian

This class A digital apparatus complies with Canadian ICES-003.
Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

Japan

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

Korea

기종별	사용자 안내문
A급 기기 (업무용 정보통신기기)	이기기는 업무용으로 전자파적합등록을 한 기기이오니 판매자 또는 사용자는 이 점을 주의하시기 바라며 만약 잘못 판매 구입 하였을 때에는 가정용으로 교환하시기 바랍니다.

Safety and EMC Approvals and Markings

USA (UL, FCC), Canada (cUL), Germany (TUV), European Union (CE), Japan (VCCI), Russia (GOST) and Korean (MIC)

HMX Manager
Installer/User Guide

TABLE OF CONTENTS

CHAPTER 1

Product Overview

Introduction

The HMX Manager is a secure, web browser-based, centralized enterprise management solution that allows users to remotely manage and monitor multiple HMX extender systems. The HMX extender system, which includes a transmitter and a user station, provides users with a full computer desktop experience from anywhere on the corporate TCP/IP network, while maintaining the computers securely housed in a corporate data center. The addition of the HMX Manager appliance allows the user stations and transmitters that comprise the HMX system to operate in Desktop mode. This mode allows a user to log in to any HMX user station and the system will connect automatically to the transmitter that has been assigned to that user. Through Desktop Mode, the HMX Manager appliance allows administrators to remotely manage and monitor the networks of user stations and transmitters that comprise the HMX system.

NOTE: For more information on the user stations and transmitters that comprise the HMX extender system, see the HMX System Installer/User Guide.

Features and benefits

Web-based access and control

As a web browser-based management solution, the HMX Manager appliance provides the operations, administration and maintenance interface for the HMX system. It also manages authentication, authorization, initiation and removal of media sessions between the user station and transmitter. The HMX Manager appliance provides a centralized database for storing configuration, user, unit and system information allowing administrators to add, remove, delete and change settings for managed appliances and users. In addition, the HMX Manager enables authentication, access control, logging events and monitoring of target computers.

Security

Secure Socket Layer (SSL) encryption is used to encrypt HMX Manager system data. Users are authenticated using the HMX Manager internal database. For management functions, the HMX Manager uses HTTPS (Hypertext Transfer Protocol with SSL encryption) to interact with the HMX system.

NOTE: To access the HMX Manager through a firewall, you must ensure that the firewall uses the default HTTPS port 443.

HMX extender system support

The transmitter connects externally to the video, audio and USB ports of the target computer and is attached directly to the target computer. It captures, compresses and encrypts the computer's media stream and transmits it to the user station over a standard TCP/IP network. The user station enables the desktop user's keyboard, video, mouse and audio devices to connect to the HMX system.

Safety precautions

To avoid potentially fatal shock hazard and possible damage to equipment, please observe the following precautions:

- Do not use a 2-wire power cord in any product configuration.
- Test AC outlets at the target computer and monitor for proper polarity and grounding.
- Use only with grounded outlets.

NOTE: The AC inlet is the main power disconnect.

CAUTION: Failure to observe the precautions in this section may result in personal injury or damage to equipment.

Observe the following general safety precautions when setting up and using Avocent equipment.

- Follow all cautions and instructions marked on the equipment.
- Follow all cautions and instructions in the installation documentation or on any cautionary cards shipped with the product.
- Do not push objects through the openings in the equipment. Dangerous voltages may be present. Objects with conductive properties can cause fire, electric shock or damage to the equipment.
- Do not make mechanical or electrical modifications to the equipment.
- Do not block or cover openings on the equipment.
- Choose a location that avoids excessive heat, direct sunlight, dust or chemical exposure, all of which can cause the product to fail. For example, do not place an Avocent product near a radiator or heat register, which can cause overheating.
- Ensure that the voltage and frequency of the power source match the voltage and frequency on the label on the equipment.
- AC power supplies have grounding-type three-wire power cords. Make sure the power cords are plugged into single-phase power systems that have a neutral ground.

- Do not use household extension power cords with Avocent equipment because household extension cords are not designed for use with computer systems and do not have overload protection.
- Ensure that air flow is sufficient to prevent extreme operating temperatures. Provide a minimum space of 6 inches (15 cm) in front and back for adequate airflow.
- Keep power and interface cables clear of foot traffic. Route cables inside walls, under the floor, through the ceiling or in protective channels or raceways.
- Route interface cables away from motors and other sources of magnetic or radio frequency interference.
- Stay within specified cable length limitations.
- Leave enough space in front and back of the equipment to allow access for servicing.

When installing Avocent equipment in a rack or cabinet, observe the following precautions:

- Ensure that the floor's surface is level.
- Load equipment starting at the bottom first and fill the rack or cabinet from the bottom to the top.
- Exercise caution to ensure that the rack or cabinet does not tip during installation and use an anti-tilt bar.

When using a desk or table, observe the following precautions:

- Choose a desk or table sturdy enough to hold the equipment.
- Place the equipment so that at least 50% of the equipment is inside the table or desk's leg support area to avoid tipping of the table or desk.

Cabling installation, maintenance and safety tips

The following is a list of important safety considerations that should be reviewed prior to installing or maintaining your cables:

- Maintain the twists of the pairs all the way to the point of termination, or no more that one-half inch untwisted. Do not cut off more than one inch of jacket while terminating.
- If bending the cable is necessary, make it gradual with no bend sharper than a one inch radius. Allowing the cable to be sharply bent or kinked can permanently damage the cable's interior.
- Dress the cables neatly with cable ties, using low to moderate pressure. Do not over tighten ties.
- Cross-connect cables where necessary, using rated punch blocks, patch panels and components. Do not splice or bridge cable at any point.
- Keep CAT 5 cable as far away as possible from potential sources of EMI, such as electrical cables, transformers and light fixtures. Do not tie cables to electrical conduits or lay cables on electrical fixtures.

- Always test every installed segment with a cable tester. “Toning” alone is not an acceptable test.
- Always install jacks so as to prevent dust and other contaminants from settling on the contacts. The contacts of the jack should face up on the flush mounted plates, or left/right/down on surface mount boxes.
- Always leave extra slack on the cables, neatly coiled in the ceiling or nearest concealed location. Leave at least five feet at the work outlet side and 10 feet at the patch panel side.
- Choose either 568A or 568B wiring standard before beginning. Wire all jacks and patch panels for the same wiring scheme. Do not mix 568A and 568B wiring in the same installation.
- Always obey all local and national fire and building codes. Be sure to firestop all cables that penetrate a firewall. Use plenum rated cable where it is required.

CHAPTER 2

Installation and Setup

Installation Overview

Rack mounting the HMX Manager appliance

Rack mount safety considerations

- Elevated Ambient Temperature: If installed in a closed rack assembly, the operating temperature of the rack environment may be greater than room ambient. Use care not to exceed the rated maximum ambient temperature of the switch.
- Reduced Air Flow: Installation of the equipment in a rack should be such that the amount of airflow required for safe operation of the equipment is not compromised.
- Mechanical Loading: Mounting of the equipment in the rack should be such that a hazardous condition does not exist due to uneven mechanical loading.
- Circuit Overloading: Consideration should be given to the connection of the equipment to the supply circuit and the effect that overloading of circuits might have on overcurrent protection and supply wiring. Consider equipment nameplate ratings for maximum current.
- Reliable Earthing: Reliable earthing of rack mounted equipment should be maintained. Pay particular attention to supply connections other than direct connections to the branch circuit (for example, use of power strips).

NOTE: The HMX Manager appliance may be rack mounted in a 1U configuration.

Installing the HMX Manager appliance

A typical HMX Manager configuration includes the appliance, transmitters and user stations connected to the local area network (LAN). A terminal, or a computer running a terminal emulation program, is connected to the serial port for configuring basic network settings. The HMX Manager appliance, transmitters and user stations, as well as user accounts, are then configured from the browser interface to the HMX Manager appliance.

To connect the HMX Manager appliance:

WARNING: To reduce the risk of electric shock or damage to your equipment:
- Do not disable the power cord grounding plug. The grounding plug is an important safety feature.
- Plug the power cord into a grounded (earthed) outlet that is easily accessible at all times.
- Disconnect the power from the target computer by unplugging the power cord from either the electrical outlet or the target computer.

1. Attach one end of the supplied power cord into the back panel of the HMX Manager appliance and attach the other end to an appropriate AC power source. The HMX Manager appliance has power control button on the front panel.
2. Connect the LAN Port 1 Ethernet port on the back panel of the HMX Manager appliance to the LAN to which the transmitters and user stations are connected using standard UTP cables.

NOTE: The transmitters and user stations must be connected to LAN port 1. However, you can access the HMX Manager appliance using the browser on a computer connected to either LAN port 1 or LAN port 2.

Configuring Network Settings

To assign an IP address to the HMX Manager appliance, you must establish a connection to the serial menu first, then use the options on the serial console menu to configure the network settings for each of the LAN ports on the HMX Manager appliance.

NOTE: If you are connecting to only one LAN, only LAN port 1 needs to be configured.

To configure the network settings of the HMX Manager appliance:

1. Connect a terminal or a computer that is running a terminal emulation program to the serial port on the back panel of the HMX Manager appliance.
2. Start a session with the following port settings:
   - Serial speed: 9600 bps
   - Data length: 8 data bits
   - Parity: None
   - Stop Bits: 1
   - Flow Control: None
3. Once a connection is established, a serial console menu appears.
4. Type **2** to configure any of the following network settings:
   - Set eth speed
   - Choose using DHCP or defining an IP address
   - Type subnet mask
   - Type gateway IP address
   - Select default gateway

- Define primary DNS and secondary DNS

NOTE: The IP address on LAN port 1 must not change during operation of the appliance. Always configure LAN port 1 with a static IP address or, if using DHCP, ensure that the IP addresses are assigned with unlimited lease times. There is no restriction on how LAN port 2 can be configured. It is also possible to configure DNS on the HMX Manager appliance if it is required for administrator access through a web browser.

NOTE: If DHCP is selected, the HMX Manager appliance must be rebooted for the change to take effect.

5. Set the time and date on the serial menu.
6. Type **0** and press **Enter** to exit.

Launching the HMX Manager Appliance Web Interface

NOTE: The HMX Manager appliance operates using default Internet Explorer settings. In the event that the default Internet Explorer settings have been altered, SSL and Javascript must be enabled to successfully access the HMX Manager appliance.

To launch the HMX Manager Appliance web interface:

1. Launch Microsoft® Internet Explorer.
2. In the address field of the browser, enter the IP address assigned to the HMX Manager appliance LAN port 1. Use http://xxx.xx.xx.xx as the format.

NOTE: If DNS is enabled, the address is the fully qualified host name assigned to the HMX Manager appliance.

3. Press **Enter**. The HMX Manager appliance login screen appears.
4. Enter the login username and password. The first time you access the HMX Manager appliance, enter **admin** as the username and **password** as the password. For security reasons, you should change the default admin password. The admin account is authorized to perform all configuration and access all managed devices and cannot be removed or renamed. Click *Login* and the HMX Manager Explorer window appears.

NOTE: If you have forgotten your password, please see *Resetting the administrator password* on page 31.

The HMX Manager Explorer window

Once a user has been logged in and authenticated, the Explorer window is displayed. From the Explorer window, you can view, access and manage units and users via the HMX Manager appliance.

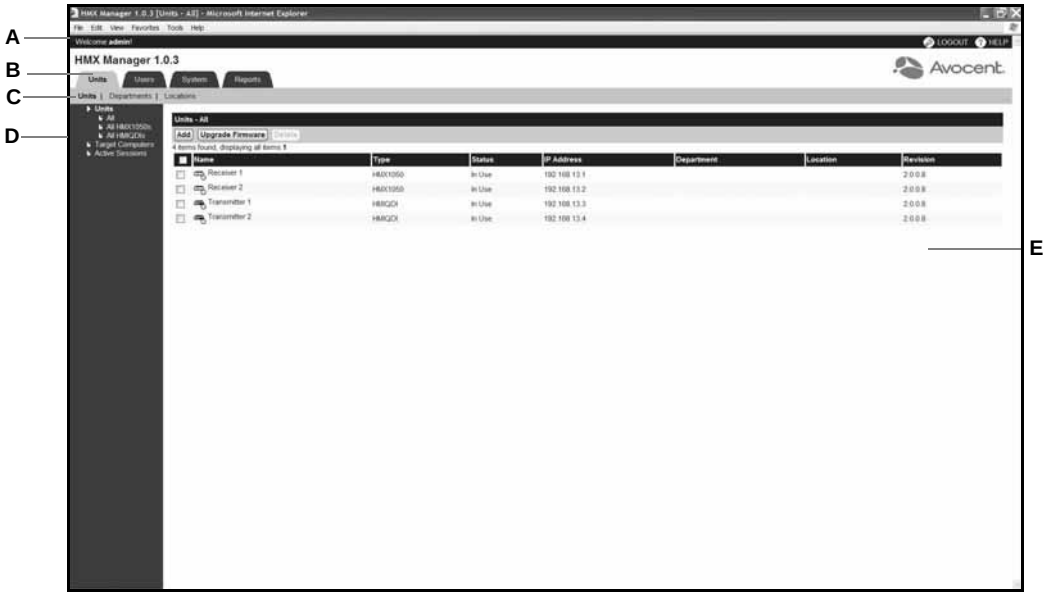


Figure 2.1: Explorer Window Areas

Table 2.1: Explorer Window Area Descriptions

Letter	Description
A	Top option bar - Use the top option bar to log out of a software session, or to access online help. The name of the logged in user is displayed on the left side of the top option bar.
B	Tab bar - Use the tab bar to display and manage units, user accounts, system settings and reports.
C	Top navigation bar - The options in the top navigation bar vary depending on the active tab in the tab bar. Topics relevant to each selection display in the side navigation bar.
D	Side navigation bar - Use the side navigation bar to select system information to display or edit in the content area.
E	Content area - The information specified by the tab bar, top navigation bar and side navigation bar selections is displayed and changed in the content area.

Using the side navigation bar

Use the side navigation bar to display windows or perform operations. The contents of the side navigation bar vary, depending on the tab and top navigation bar options that are in use.

NOTE: Menus are static and cannot be expanded or collapsed.

The arrows displayed in the side navigation bar indicate where sub-options are available. You can display these items by clicking the main link. Where no arrow is displayed, clicking the link brings you directly to the option you have selected.

Displaying pages

Multiple page windows contain menu options that may be used to navigate from one display to another. You can click the *Select All* checkbox to select all items on a page. Enabling this checkbox selects all the items listed on a page regardless of whether the entire page is visible. However, for multi-page displays, items listed on other pages will not be included in the selection. All screens that show lists, units, sessions and target computers automatically refresh every 10 seconds.

Using keyboard commands

In addition to using a mouse, you can use keyboard commands to select and change items in windows.

Table 2.2: General Keyboard Commands

Key	Description
Tab	Transfers focus to the next control in the window, including the calendar
Shift-Tab	Transfers focus to the previous HTML control

CHAPTER 3

Managing Units

Accessing the HMX Manager Appliance Web Interface

To access the HMX Manager appliance web interface:

1. Launch a web browser.
2. In the address field of the browser, enter the IP address or host name assigned to the HMX Manager appliance you wish to access. Use https://xxx.xx.xx.xx or https://hostname as the format.
3. When the browser makes contact with the appliance, enter your username and password, then click *Login*. The HMX Manager Explorer window appears.

NOTE: To access the HMX Manager appliance through a firewall, you must ensure that the firewall uses the default HTTPS port 44.

Using the Units Tab in the Explorer Window

From the Units tab in the HMX Manager Explorer, you can manage user operations such as adding and deleting units, changing unit properties and upgrading your firmware. When you click the *Units* tab, the Units - All window displays.

NOTE: In the HMX Manager Explorer, the term “units” refers to transmitters and/or user stations.

The Units All Window

The Units - All window displays the list of units added to the HMX Manager appliance database. You can use the checkbox to the left of each unit name to select/deselect the unit for an operation. The following fields will appear in Units - All window.

- Name - Name of the unit as defined in the HMX Manager appliance database. Click the name to display or change unit information.
- Type - Type of unit or session. Unit and session types cannot be changed.
- Status - Current operating status of a unit.

The table below lists and describes the possible values in the status field.

Table 3.1: Unit Status Values

Type	Status and Icon	Description
Managed Units	Idle	Unit is turned on, can be communicated with and is not associated with an active media session.
Managed Units	In Use	Unit is associated with a session.
Managed Units	Upgrading	Unit firmware is being upgraded.
Managed Units	Not Responding	The HMX Manager appliance cannot contact the unit.
Target Computers	Idle	Target computer is not associated with an active media session.
Target Computers	In Use	Target computer is associated with an active media session.
Active Session	Active	The active session is running and the units are responding.
Active Session	Not Responding	The units involved in the active session are not responding. If an active session does not respond for more than 20 minutes, it will be deleted.

- IP Address - The IP address of a managed unit.
- Department - The name of the department to which a managed unit has been assigned.
- Location - The name of the location to which a managed unit has been assigned.
- Revision - The current firmware version that is installed on a managed unit.

Commonly used Units windows

In the side navigation bar of the Units - All window is a list of Units windows. The most commonly accessed windows are:

- All: Click *Units* in the side navigation bar to display the managed units. The Units - All window will re-open. You can click on a link in the side navigation bar to view a summary of all units, all user stations or all transmitters.
- Target Computers: Click *Target Computers* in the side navigation bar to see a list of all target computers in the system.
- Active Sessions: Click *Active Sessions* in the side navigation bar to view a list of all the users that are accessing user stations, and which transmitters are being accessed by which users. The Active Sessions window also displays start times and session duration. An active session starts when a connection is made between a transmitter and a user station.

NOTE: An authorized pair is a pairing of a transmitter and a target computer that has been accepted by the administrator; an unauthorized pair has not been accepted by the administrator as a desired pairing. An unauthorized pairing can occur after initial discovery of a device pair, or if the transmitter was inserted into the wrong target computer.

Adding units via the Add Unit Wizard

Before you can manage units in the HMX Manager appliance, you must first add them to the HMX Manager appliance database. You can add units to the HMX Manager appliance database by clicking on *Add* in the Units - All window. The Add Unit Wizard will appear, allowing you to:

- Add a single unit
- Discover units within an IP address range
- Discover units on an IP subnet address

Adding a single appliance

This procedure is valid for transmitters and user stations.

NOTE: A unit can only be added to the HMX Manager appliance database if it is turned on and attached to the network.

To add a single unit that already has an IP address:

1. In a Units - All window containing managed units, click *Add*. The Add Unit Wizard Welcome Window will open. Click *Next*.
2. The Select Add Unit Procedure window will open. Click *Add a single unit*, then click *Next*.
3. The Select Unit Type window will open. Select a unit from the product list, then click *Next*.
4. The Select Address Configuration of Unit window will open. Select *Yes, the <Managed Unit Type> does have an address* and type the address of the unit. Click *Next*.
5. The Search Results window will open. The name and MAC address of the discovered unit will be displayed. Click *Next*.
6. The Completed Successfully window will open. To exit the Add Unit Wizard, click *Finish*.

To add a single unit that does not have an IP address:

1. In a Units - All window containing managed units, click *Add*. The Add Unit Wizard Welcome Window will open. Click *Next*.
2. The Select Add Unit Procedure window will open. Click *Add a single unit*, then click *Next*.
3. The Select Unit Type window will open. Select a unit from the product list, then click *Next*.
4. The Select Address Configuration of Unit window will open. Select *No, the <Managed Unit Type> does not have an address* and click *Next*.
5. The Configure Unit Network Settings window will open.
   a. Type the IP address and subnet mask, in standard dot notation (xxx.xxx.xxx.xxx), for the managed unit.
   b. Optionally, type a gateway in standard dot notation (xxx.xxx.xxx.xxx).
   c. Click *Next*.

6. The Add Discovered Unit window will open. Select the discovered unit from the list, then click *Next*.
7. The Completed Successfully window will open. To exit the Add Unit Wizard, click *Finish*.

Adding units from a range of IP addresses

This procedure is valid for transmitters and user stations.

To add a unit from a range of IP addresses:

1. In a Units - All window containing managed units, click *Add*. The Add Unit Wizard Welcome Window will open. Click *Next.*
2. The Select Add Unit Procedure window will open. Click *Discover units within an IP address range*, and then click *Next*.
3. The Enter IP Address Range window will open.
   a. Type the IP address, in standard dot notation (xxx.xxx.xxx.xxx), from which to begin and end the search.
   b. Click *Next*.
4. The HMX Manager appliance will search for managed units within the IP address range. When the search is completed, the Select Units to Add window will open, listing the results.
5. To add one or more managed units, select the managed units in the Units Found list, then click *Add*. The managed units will be moved to the Units to Add list.
6. To remove one or more managed units, select the managed units in the Units to Add list, then click *Remove*. The managed units will be moved to the Units Found list.
7. Click *Next*.
8. The Completed Successfully window will open. To exit the Add Unit Wizard, click *Finish*.

Adding units on an IP subnet

This procedure is valid for transmitters and user stations.

To add a unit from a subnet:

1. In a Units - All window containing managed units, click *Add*. The Add Unit Wizard Welcome Window will open. Click *Next.*
2. The Select Add Unit Procedure window will open. Click *Discover units on an IP subnet address* and then click *Next*. The Enter Subnet Address Window will open.
3. Type the IP address in standard dot notation (xxx.xxx.xxx.xxx) and click *Next*.
4. The HMX Manager appliance searches for managed units within the IP subnet address range. When the search is completed, the Select Units to Add window will open, listing the results.
5. To add one or more managed units, select the managed units in the Units Found list, then click *Add*. The managed units will be moved to the Units to Add list.

6. To remove one or more managed units, select the managed units in the Units to Add list, then click *Remove*. The managed units will be moved to the Units Found list.
7. Click *Next*.
8. The Completed Successfully window will open. To exit the Add Unit Wizard, click *Finish*.

Deleting units

When you delete a unit, it is removed from the HMX Manager appliance database and all associated connections will also be deleted. It is recommended that active sessions are deleted before units are deleted.

To delete a unit:

1. In a Units - All window, click to select the checkbox next to the unit name. To delete all units on the page, click to select the checkbox to the left of the Name field at the top of the list.
2. Click *Delete*. The unit(s) is immediately removed from the HMX Manager appliance database and disappears from the list.

The Unit Overview Window

To view a summary of all units managed by the HMX Manager appliance, click the *Units* tab. The Units - All window will open, showing all the units that are managed by the HMX Manager appliance. To view a list that contains only transmitters or only user stations, select the appropriate option in the side navigation bar.

To view information about individual user stations or transmitters, click on a specific unit listed in the Units - All window. The Unit Overview window opens.

When the Unit Overview window opens, the following information is displayed:

- For Managed Units (user stations and transmitters) - Name, Type, EID, MPN, Address, MAC address and status of the managed units and the tools that can be used to reboot and upgrade firmware. The available tasks depend on the type of managed unit.
- For Authorized Target Computers - Display Name, Type, Address and MAC address

The Unit Overview window also enables you to change the name of a unit, reboot a unit or upgrade the firmware of a unit. See *Managing firmware upgrades* on page 18 for more information on upgrading your firmware.

To change the name of a unit:

1. Click the *Units* tab. A list of all units managed by the HMX Manager appliance is displayed.
2. Click the unit name you wish to change. The Unit Overview window will open.
3. Type a new name for the managed unit.

NOTE: You cannot change the unit type.

4. Click *Save* and then click *Close*.

Changing unit properties

The HMX Manager appliance enables you to manage the department and location properties as well as the primary contact details for each unit.

To change the properties of a unit:

1. Click the *Units* tab. A list of all units managed by the HMX Manager appliance is displayed.
2. Click the unit name you wish to change. The Unit Overview window will open.
3. Select *Properties* from the side navigation bar.
4. The Unit Properties window will open. This window displays all the general properties of the unit. Edit the properties you wish to change.

NOTE: Part Number (MPN), Serial Number (EID) and model type are read-only values. These values are read from a unit during discovery and cannot be changed.

5. Click *Save* and then click *Close*.

Configuring network settings for a transmitter or user station

The administrator can use the HMX Manager appliance to change a unit's IP address, subnet mask, default gateway and DHCP status. These changes can be done from the Unit Settings menu available in the side navigation bar of the Unit Overview window. Once you have implemented the changes, the unit will reboot.

All configuration options under the Unit Settings menu in the side navigation window involve live communication with a transmitter or user station. The transmitter or user station must be turned on, discovered and added for the HMX Manager appliance to display its properties.

If the HMX Manager appliance cannot communicate with a transmitter or user station, it will display the following communication error: *An error was encountered communicating with the Unit. Please check the unit's network settings and connectivity*.

To change the network settings of a managed unit:

1. Click the *Units* tab. A list of all units managed by the HMX Manager appliance is displayed.
2. Click the unit name whose network settings you wish to change. The Unit Overview window will open.
3. Click *Network* under Unit Settings in the side navigation bar. The Unit Network Settings window will open.
   - Type an address, subnet and gateway in standard dot notation (xxx.xxx.xxx.xxx).
   - Enable or disable DHCP.
4. Click *Save* and then click *Close*.

Authentication server settings

Authentication server settings are applied only to user stations. The Authentication Servers menu item in the side navigation bar (under Unit Settings) will only be displayed if the unit type is a user station.

To change unit authentication server settings:

1. Click the *Units* tab. A list of all units managed by the HMX Manager appliance is displayed.
2. Click the user station name for which you require information. The Unit Overview window opens.
3. Click *Authentication Servers* under Unit Settings in the side navigation bar. The Unit Authentication Server Settings window displays the address of the authentication server used by the unit. To change information, type an address in standard dot notation (xxx.xxx.xxx.xxx).
4. Click *Save*.

Enabling Auto Login Mode for a user station

Auto Login Mode enables you to configure a user station to grant any user access to the target computer paired with that user station, without the need to enter a username or a password.

To enable or disable Auto Login Mode for a user station:

1. Click the *Units* tab. A list of all units managed by the HMX Manager appliance is displayed.
2. Click the user station name for which you require information. The Unit Overview window opens.
3. Under Unit Settings in the side navigation bar, click *Modes*. The Unit Auto Login/Operating Mode Settings window opens.
4. In the Unit Auto Login Mode section, choose *Disable* or *Enable*.
5. If Auto Login Mode is enabled, select a target computer from the Auto Login Mode Target Computer list-box. This is the target computer that will be connected during the auto login process.
6. Click *Save* and then click *Close*.

Viewing version information

To view version information for a unit:

1. Click the *Units* tab. A list of all units managed by the HMX Manager appliance is displayed.
2. Click the unit name for which you require information. The Unit Overview window opens.
3. Under Unit Settings in the side navigation bar, click *Versions*. The Unit Version Information window will open, containing the following information:
   - Release - The version release number.
   - Application - The application software version.

- Boot - The boot software version.
- FPGA - The FPGA version.

Rebooting a unit

To reboot a unit:

1. Click the *Units* tab. A list of all units managed by the HMX Manager appliance is displayed.
2. Click the unit name for which you require information. The Unit Overview window opens.
3. In the Tools section, click *Reboot*. The unit reboots to apply any changes.

Setting the Operating Mode for a user station

The HMX system can operate in two modes - Desktop Mode and Extender Mode. The operating mode of an HMX system can be set through the user station.

Extender Mode is the default factory setting for an HMX system. In Extender Mode, a user station automatically discovers and connects to its corresponding transmitter on the network. The HMX Manager appliance is not required as part of the system when in Extender Mode.

When in Desktop Mode, an HMX system can be managed and administered through the HMX Manager appliance.

To change the operating mode for a user station:

1. Click the *Units* tab. A list of all units managed by the HMX Manager appliance is displayed.
2. Click the appropriate user station name. The Unit Overview window opens.
3. Under unit settings in the side navigation bar, click *Modes*. The Unit Auto Login/Operating Mode Settings window opens.
4. In the Unit Operating Mode section, choose *Extender* or *Desktop*.
5. Click *Save* and then click *Close*.

Managing firmware upgrades

To upgrade the firmware on a single unit:

NOTE: You cannot perform a firmware upgrade unless a firmware upgrade file has been added to the HMX Manager appliance software repository. See *Firmware management* on page 31. Also, upgrading the unit firmware requires the unit to reboot; currently active sessions will be disconnected.

1. Click the *Units* tab. A list of all units managed by the HMX Manager appliance is displayed.
2. Click the appropriate unit name. The Unit Overview window will open.
3. In the Tools section, click the *Upgrade Firmware* icon. The Upgrade Unit Firmware wizard will launch.
4. Click *Next*. The Select Firmware Files window will open. To add a firmware file to the update list, select the file in the Available Firmware Files list, then click *Add*. The properties will be moved to the Firmware Files to Update list.

5. Select the firmware file you wish to use. Click *Next*. The unit reboots to apply the new settings. The Completed Successfully window will open.
6. Click *Finish*.

During a firmware upgrade, the unit status in the Units - All window will be set to Upgrading. The event log can also be used to monitor the status of a unit firmware update. When the firmware update is complete, the unit firmware revision field is updated and the unit reverts to the status Idle.

Viewing/changing target computer overview information

To view overview information for a target computer:

1. Click the *Units* tab. The Units - All window will open.
2. Select *Target Computers* from the side navigation bar. A list of all the target computers that are managed by the HMX Manager appliance is displayed.
3. Click the name of a target computer in the Target Computers - All window. The Target Computer Overview window will open.

To change overview information for a target computer:

1. After opening the Target Computer Overview window, type a name and a display name for the target computer.
2. Type a name for the Authorized Transmitter.
3. Click *Save* and then click *Close*.

Managing user access to target computers

To manage user access to target computers:

1. Click the *Units* tab. The Units - All window will open.
2. Select *Target Computers* from the side navigation menu. This displays a list of all target computers in the Target Computers - All window.
3. Choose the appropriate target computer. The Target Computer Overview window opens.
4. Select *Users* from the side navigation menu. The Target Computer User Configuration window opens. There are two list boxes in this window: Non Associated Users and Associated Users.
5. Select the required user from the Non Associated Users list box and add to the Associated Users list box by clicking the *Add* button. The target computer is now allocated to that user.
6. Click *Save*.

Changing target computer properties

The HMX Manager appliance enables you to change the following properties for each target computer:

- Part Number
- Serial Number

- Model Number
- Asset tag number
- Department
- Location
- Primary contact details (name, telephone number)

To change the properties of a target computer:

1. In the Target Computers - All window, click the name of the target computer to edit. The Target Computer Overview window will open.
2. Click *Properties* on the side navigation bar.
3. The Target Computer Properties window opens. This window displays the general properties of the target computer. Edit the properties you wish to change.
4. Click *Save*.

Active media sessions

An active media session is created when a user connects to a target computer by logging in through a user station. The HMX Manager appliance enables you to monitor the following properties of an active media session:

- Start time of the session
- Duration of the session
- Logged in username
- User station
- Transmitter
- Target computer
- Active Media Session status

NOTE: It is not possible to restrict the types of media available during an active media session. A connection will enable all media sessions: Video, Audio, Keyboard/Mouse and vMedia.

All active media sessions

To view a summary of all active sessions:

1. Click the *Units* tab. The Units - All window will open.
2. Click *Active Sessions* in the side navigation bar. The Active Media Sessions window opens, displaying a list of all the current active media sessions.

Performing a forced log-out

To disconnect an active media session:

1. Click the *Units* tab. The Units - All window will open.

2. Click *Active Sessions* in the side navigation bar. The Active Media Sessions window will open. A list is displayed of all the current active media sessions.
3. Click to select the checkbox to the left of the sessions. To disconnect all sessions, click the checkbox to the left of the Start Time field at the top of the list.

NOTE: If you do not have permission to disconnect an active session, you will not be able to select its checkbox or the checkbox at the top of the list.

4. Click *Disconnect*.

Departments and Locations Windows

The HMX Manager appliance also provides a means to attach logical location identifiers to units, making it easier for administrators to track and locate units within their organization. The Departments window identifies units that have been assigned to a department, while the Locations window identifies units that have been assigned to a location. Access the Departments window by clicking *Units* - *Departments* and access the Locations window by clicking *Units* - *Locations*.

To group units by department or location, you must create a department or location and then associate units with it. Departments or locations that contain units to which a user does not have access rights will not appear in the side navigation bar. The department or location must also have at least one unit associated with it to be displayed in the side navigation bar.

To add a department or location:

1. Click the *Units* tab.
2. To add a department, click *Departments* in the top navigation bar. The Departments window opens.

   - or -

   To add a location, click *Locations* in the top navigation bar. The Locations window opens.
3. Click *Add*. The Add Department or Add Location window will open.
4. Type a name, and then click *Add*. The Departments or Locations window will open.

To delete a department or location:

1. Click the *Units* tab.
2. To delete a department, click *Departments* in the top navigation bar. The Departments window opens.

   - or -

   To delete a location, click *Locations* in the top navigation bar. The Locations window opens.
3. Click to select the checkbox to the left of one or more departments/locations. To delete all departments/locations in the page, click to select the checkbox to the left of the Name field at the top of the list.

4. Click *Delete*. A confirmation dialog box will appear.
5. Confirm or cancel the deletion.

To change the name of a department or location:

1. Click the *Units* tab. The Units - All window will open.
2. To change the name of a department, click *Departments* in the top navigation bar. The Departments window opens.

   - or -

   To change the name of a location, click *Locations* in the top navigation bar. The Locations window opens.
3. Click the name of a department/location. The Department/Location Name window will open.
4. Type a new character name (1 - 64 characters).
5. Click *Save* and then click Close. The Departments or Locations window will open.

To associate or change the association of an existing unit to a department or location:

1. Click the *Units* tab.
2. Click the name of a unit. The Unit Overview window opens.
3. Click *Properties* in the side navigation bar.
4. From the drop-down lists, select the department and/or location to associate with the unit. If you do not wish to associate the unit with any site, department or location choose the top (empty) item from the menu.
5. Click *Save* and then click *Close*.

CHAPTER 4

Managing Users

Using the Users Tab in the Explorer Window

From the Users tab in the HMX Manager Explorer, you can carry out the following operations:

- Add, change and delete user accounts
- Enable/disable user accounts
- Specify user password policy restrictions
- Change user group membership
- Display user access rights to target transmitters and managed units

User Accounts windows

User accounts are displayed and managed through User Accounts - All window. This window shows information about each user account, including which type of authentication service is being used and the status of each account. A face icon will appear next to each user account listed. Options for the status of each account are listed in the following table.

Table 4.1: User Status Icons

Icon	Authentication Service Type	Status
Face	All	Enabled - The user can log in and use the HMX Manager appliance.
Face with a red X	Internal	Disabled - The user cannot log in to the HMX Manager appliance or user station.

To select a user account:

1. Click the *Users* tab in the HMX Explorer window. The User Accounts - All window is displayed.
2. To display the names of users in a user group, click *Users* in the side navigation bar. The User Accounts - All window opens.
3. To select a user, click a username in the User Accounts - All window.

Adding user accounts

Users

Users cannot log on to a user station and access a transmitter unless a User Station User Account has been created for them in the HMX Manager appliance. Only an HMX Manager appliance administrator can create a User Station User Account. User station users cannot access the HMX Manager appliance. User Station User Accounts are authenticated by an HMX Manager appliance internal authentication service. An HMX Manager administrator specifies which target computer a user station user is allowed to access.

HMX Manager appliance administrators

Only administrators can log in to the HMX Manager appliance. Administrators manage the HMX Manager appliance, control access for users and can also set up associations between users and user stations. Users and administrators can log in to a user station to access their computer. Both administrator and user accounts are authenticated by an HMX Manager appliance internal authentication service.

To add a new user or administrator:

1. Click the *Users* tab. The User Accounts - All window opens.
2. Click *Add*. The Add User Account Wizard Welcome Window will appear. Click *Next*.
3. The Select Authentication Service window will open. This window lists the Management Appliance internal service.
4. Select *Internal* and click *Next*.
5. The Type in User Credentials window opens.
   a. Type a username and password, then confirm the password for the user you are adding.

NOTE: A username must be unique and must contain between 1 and 64 alphanumeric characters. Usernames are case-sensitive. A password must contain between 1 and 64 alphanumeric characters.

   b. Click *Next*.
6. The Assign User to User Groups window opens. Select *Users* as the user group. Click *Add*.

   - or -

   Select *Administrators* as the user group and click *Next*.
7. The Completed Successful window will open. Click *Finish*. The new user account has been added to the system.

Deleting user accounts

To delete one or more user accounts:

1. Click the *Users* tab. The User Accounts - All window opens.

2. Click to select the checkbox to the left of the username(s). To delete all users on the page, click the checkbox to the left of the User Name field at the top of the list.
3. Click *Delete*. A confirmation dialog box will appear.
4. Confirm or cancel the deletion.

Enabling and disabling user accounts

To restrict the access to the system, you can disable a user's account within the HMX Manager appliance. You can re-enable the user's account at any time.

To disable or re-enable a user account:

1. Click the *Users* tab. The User Accounts - All window opens.
2. Click on the user account to be disabled.
3. Click *Restrictions* in the side navigation bar.
4. Select the *Disable user account* checkbox to disable the account.

   -or -

   De-select the *Disable user account* checkbox to re-enable the account.
5. Click *Save* and then click *Close*.

Managing user accounts

To view a summary of all user accounts:

1. Click the *Users* tab. A list is displayed of all the user accounts that are managed by the HMX Manager appliance.
2. To view a list that contains only the administrator accounts, select *Administrators* in the side navigation bar.

   - or -

   To view a list that contains only the User Station User Accounts, select *Users* in the side navigation bar.

To change or edit usernames or groups:

1. Click the *Users* tab. A list is displayed of all the user accounts that are managed by the HMX Manager appliance.
2. Click the user account name to edit. The User Account Overview window will open, allowing you to edit the following user information:
   - User Name (login)
   - Full Name
   - Group (user group)
3. Edit the properties you wish to change.

4. Click *Save*, then click *Close*. The updated user account overview information is displayed.

Managing user access to target computers

Except for pooling cases, if there are no transmitters selected as part of the user station configuration, then that user cannot log in from a user station. For more information on pooling, see Chapter 5.

To allocate target computers to a user station user:

1. Click the *Users* tab. The User Accounts - All window opens.
2. Click the appropriate username. The User Account Overview window will open.
3. Select *Target Computers* from the side navigation menu. The User Target Computer Configurations window will open. There are two radio buttons in this window: All Targets and Selected Targets. The default is Selected Targets; this lists all Available Target Computers.
4. Choose the required target computers by selecting from the list box and adding them to the Allocated Target Computers list box on the right-hand side of the window.
5. Click *Save*, then click *Close*.

User passwords

A user's password can only be changed by an administrator.

NOTE: A password must contain between 1 and 64 alphanumeric characters. With the exception of plus (+) and minus (-) all ASCII characters may be used.

To change a user password:

1. Click the *Users* tab. The User Accounts - All window opens.
2. Click the appropriate username. The User Account Overview window will open.
3. Click *Password* in the side navigation bar. The User Password window will open.
4. Type and verify the new user password.
5. Click *Save* and then click *Close*.

User contact details

You can add or edit a range of contact details for any existing user.

To add contact details for a user:

1. Click the *Users* tab. The User Accounts - All window opens.
2. Click a username. The User Account Overview window will open.
3. Click *Contact Details* in the side navigation bar. The User Contact Details window will open.
4. In each of the fields, type the information you wish to enter. You may also edit existing details.
5. Click *Save* and then click *Close*.

Internal user authentication services

You may set the internal authentication settings for users logging into the HMX Manager appliance. These settings relate to the minimum requirements that passwords must meet. You can set minimum length, a requirement that passwords contain both alpha and numeric characters, and a requirement that passwords contain both upper and lower case characters.

To set the internal user authentication settings:

1. Click the *Users* tab. The User Accounts - All window opens.
2. Click *Authentication Services* in the top navigation bar. The User Authentication Services window opens.
3. Click *Internal* to open the Authentication Service User Account Policies - Internal window.
4. Type a number to indicate the minimum password length in the Minimum Password Length field. The default minimum setting is six characters.
5. If required, click to select either or both of the following password options checkboxes:
   - Passwords must contain both alpha and numeric characters.
   - Passwords must contain both lower and upper case characters.
6. Click *Save*.
7. Click *Close* to exit the screen and return to the User Authentication Services window.

CHAPTER 5

Advanced Operations

Using the System Tab in the Explorer Window

From the System tab in the HMX Manager Explorer, you can enable target computer pooling, back up and restore your database, upgrade the software, manage firmware files and reset the administrator password.

Target computer pooling

The HMX Manager appliance allows you to "pool" transmitters so that they are accessible to multiple users. All discovered units that have not been allocated to a user and are not in use are assigned to a pool of transmitters. Each transmitter is assigned based on the order in which the users log in. When a user logs in at a user station, that user will connect to the transmitter that has been assigned to him/her. If no specific transmitter has been assigned, the user will then connect to the first available transmitter, if pooling is enabled.

To enable/disable target computer pooling:

1. Click the *System* tab.
2. Click *HMX Manager Server* in the top navigation bar. The Target Computer Pooling Properties window opens.
3. Click the *Enable target computer pooling* checkbox to select or de-select it.
4. Click *Save* and then *Close*.

Backup and restore

The HMX Manager appliance allows you to back up its database and to store it in a location of your choice. In addition, you can also restore the database from a file located on any machine accessible on the LAN on which the HMX Manager appliance is located.

To back up the HMX Manager appliance database:

1. Click the *System* tab.
2. Click *HMX Manager Server* in the top navigation bar.
3. In the side navigation bar, click *Backup and Restore*. The Data Backup and Restore window will open.

4. Click *Backup System*. The File Download dialog box appears.
5. Click *Save* and browse to the location where you want to store the system data.
6. Click *Save* and then click *Close*.

To restore the HMX Manager appliance database:

1. Click the *System* tab.
2. Click *HMX Manager Server* in the top navigation bar.
3. In the side navigation bar, click *Backup and Restore*. The Data Backup and Restore window will open.
4. Click *Data Restore*. The Data Restore Wizard opens.
5. Click *Next.*
6. Click *Browse* and browse to the location of the file.
7. Click *Next*. A dialog box appears to warn you that you are about to upload a stored database to the HMX Manager appliance.
8. Click *OK*. A message indicating that the database has been successfully restored appears.

HMX Manager appliance upgrade

When upgrades of the HMX Manager appliance software are available, you can upgrade via the Upgrade HMX Manager Software Wizard.

CAUTION: All data must be backed up in advance of any software upgrade as all data files are overwritten during the upgrade process and all data will be lost.

To upgrade your HMX Manager appliance software:

1. Click the *System* tab.
2. Click *HMX Manager Server* in the top navigation bar and then click *Management Appliance Upgrade* in the side navigation bar.
3. The Upgrade Management Appliance Software Wizard appears. Click *Next*.
4. Click *Browse* and browse to the location of the software upgrade files.
5. Click *Next*. A dialog box appears and warns you that you are about to install a new version of the software and that all data should be backed up before proceeding.
6. Click *OK*. The new software version is installed.

Firmware management

The firmware files for transmitters and user stations can be added, viewed and deleted using the Unit Firmware Files window. Once a firmware file(s) has been added, you may use the file(s) to upgrade the managed unit.

To add a firmware file:

1. Click the *System* tab. The Unit Firmware Files window opens.
2. Click *Add*. The Add Firmware File Wizard will appear.
3. Click *Next*. The Select Firmware File to Import window will open.
4. Enter the directory and filename (or browse to the location) of the firmware file you want to add to the HMX Manager appliance Unit Files repository.
5. Type a description of the firmware file in the Description field.
6. Click *Next*. The firmware is added and the Completed Successful window appears.
7. Click *Finish*. The Unit Firmware Files window will open.

To display firmware information:

1. Click the *System* tab. The Unit Firmware Files window opens.
2. Click the version of a firmware file. The Firmware File Properties window will open. If you wish, you may change the description of the firmware file in the Description field.
3. Click *Save* and then click *Close*. The Unit Firmware Files window will re-open and contain the firmware information if you saved the changes.

To delete firmware:

1. Click the *System* tab. The Unit Firmware Files window opens.
2. Click to select the checkbox next to the firmware you want to delete.
3. Click *Delete*. A confirmation dialog box will appear.
4. Confirm or cancel the deletion.

Resetting the administrator password

To reset the administrator password:

NOTE: You must log out as an adminstrator before resetting the adminstrator password. You must also log out of the HMX Manager Appliance Web Interface before accessing the reset password URL, listed below.

1. Enter the following URL: https://IP Address/dtview/system/reset/reset.html in the address bar. Press **Enter**. The Security Alert box appears.
2. Click *Yes*. The Management Appliance Server Administrator Password Reset Utility screen opens. This screen contains two text fields - Request Code and Reset Code. The Request Code box contains a unique key.

3. Send the request code to Technical Support at Avocent. Technical Support will generate a reset code and send it to the administrator. For information on catacting Avocent Technical Support, see *Technical Support* on page 36.
4. Enter this reset code in the Reset Code text box and click *Submit* to reset the password.
5. At the Management Appliance login page, select *User*. The text listed in the Password box will reset to the correct password. To ensure security, enter a new password.

CHAPTER 6

Events and Event Logs

Using the Reports Tab in the Explorer Window

When an enabled, defined event occurs in the HMX Manager appliance, it is saved in the event log. Events are classified by severity and category. You can display the event log content or view details about an individual event log entry. If you wish, you can also export event logs to Microsoft Excel for further analysis. It is also possible to change the event log's retention period and export the event log's content. Event logs can be managed from the Reports tab in the HMX Explorer.

NOTE: It is not possible to manually delete event logs. The HMX Manager appliance automatically deletes logs which have expired.

You can customize event log displays either by displaying all events in the log, or displaying events of a particular severity or a particular category.

Event log display fields

Click the *Reports* tab to display the Event Log - All window. The following fields are displayed:

- Severity - Clicking an entry under this field will display a window which contains details about the event.

Table 6.1: Event Severity Levels

Severity	Description
Debug	Abnormal events that require correcting at a later time.
Information	General events that are neither periodic nor problematic and require no specific action.
Warning	Requires attention, but will not result in failures of tasks or communication.
Error	Serious in nature - requires immediate attention.
Fatal	Requires immediate corrective action.

- Date/Time - Displays the date and time of an event in the appliance's time zone.
- Description - Short description of an event.

Changing the event log retention period

By default, an event log is retained for seven days.

NOTE: Event log information is stored in the HMX Manager appliance database. Increasing the event log retention time may impact the performance of the HMX Manager appliance.

To change the event log retention period:

1. Click the *Reports* tab.
2. Click *Log Configuration* in the side navigation bar. The Event Log Retention Time window will open.
3. Type a number of days in the Days field, or select it using the menu.
4. Click *Save*, then click *Close.*

Creating an event log .csv file

All or selected columns of the event log can be exported as a comma separated values (.csv) file. The output event log file is named eventlog.csv by default, but you may change the name when it is saved. The .csv file may be viewed in a text editor or spreadsheet application.

To create an event log.csv file:

1. Click the *Reports* tab The Event Log - All window opens.
2. Click the *Export* button at the top of the window.
3. The File Download dialog will open. Click *Save.*
4. Browse to the location where you want to save the log and click *Save.*
5. The Completed Successful window will display.
6. Click *Close*.

APPENDICES

Appendix A: Technical Specifications

Table A.1: HMX Manager Appliance Specifications

Network Connection	
Number	2
Type	Ethernet, 10BaseT, 100BaseT, GigE
Connector	RJ-45
Serial Port	
Number	1
Type	RS-232 serial
Connector	DB9 male
Mechanical	
H x W x D	4.3 x 42.7 x 35.6 cm (1.7 x 16.8 x 14 in), 1 U form factor
Weight	5.9 kg (13 lb)
Power	
AC Input Voltage	100 to 240 VAC
Rated Input Current	4A maximum
Rated Input Frequency	50 to 60 Hz
Rated Output Power	260 W maximum
Rated Output Voltages	+3.3 V (15 A), +5 V (25 A), +12V (18A), -12 V (1A)
BTU Rate	1400 Bus/hour (for rated output power of 260 W)
Environmental	
Temperature	0° to 35° Celsius (32° to 95° Fahrenheit) operating
Humidity	10 to 90% noncondensing operating
Safety and EMC Approvals and Markings	USA (UL, FCC), Canada (cUL), Germany (TUV), European Union (CE), Japan (VCCI), Russia (GOST) and Korea (MIC)
NOTE: Safety certifications and EMC certifications for this product are obtained under one or more of the following designations: CMN (Certification Model Number), MPN (Manufacturer's Part Number) or Sales Level Model designation. The designation that is referenced in the EMC and/or safety reports and certificates are printed on the label applied to this product.	

Appendix B: Technical Support

Our Technical Support staff is ready to assist you with any installation or operating issues you encounter with your Avocent product. If an issue should develop, follow the steps below for the fastest possible service.

To resolve an issue:

1. Check the pertinent section of this manual to see if the issue can be resolved by following the procedures outlined.
2. Visit www.avocent.com/support and use one of the following resources:

   Search the knowledge base or use the online service request.
   -or-
   Select *Technical Support Contacts* to find the Avocent Technical Support location nearest you.

License Information

This product includes various software programs that are copyrighted and released under the GNU General Public License (GPL), the GNU Lesser General Public License (LGPL), and other licenses that permit copying, modification, and redistribution of source code (such licenses referred to as Public Licenses), in particular the software program “mtd”. A machine-readable copy of the source code protected by these Public Licenses is available from Avocent on a medium customarily used for software interchange for a period of three years from date of purchase of this product by contacting Avocent Corporation at www.Avocent.com/support. AVOCENT CORPORATION AND ITS LICENSORS MAKE NO WARRANTY (EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE) OF ANY KIND REGARDING THE SOFTWARE PROGRAMS LICENSED UNDER ANY PUBLIC LICENSE, AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, AVOCENT CORPORATION AND ITS LICENSORS DISCLAIM ANY AND ALL OTHER WARRANTIES AND CONDITIONS WITH RESPECT TO THE SOFTWARE PROGRAMS LICENSED UNDER ANY PUBLIC LICENSE.

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc. 51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation’s software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author’s protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors’ reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone’s free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The “Program”, below, refers to any such program or work, and a “work based on the Program” means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term “modification”.) Each licensee is addressed as “you”.

   Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

   You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

   a. You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

   b. You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

   c. If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

   These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

   Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

   In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

   a. Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

   b. Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

   c. Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

   The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

   If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free

redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

   Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and “any later version”, you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

Avocent®

The Power of Being There®

For Technical Support:

www.avocent.com/support

590-820-501B