DVI KVM Over IP Extender
KE6900 / KE6940
User Manual

www.aten.com

FCC, CE Information

FEDERAL COMMUNICATIONS COMMISSION INTERFERENCE STATEMENT: 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 Matrix Managerof 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.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

CE Warning: This is a class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

RoHS

This product is RoHS compliant.

SJ/T 11364-2006

The following contains information that relates to China.

部件名称	有毒有害物质或元素					
	铅	汞	镉	六价铬	多溴联苯	多溴二苯醚
电器部件	●	○	○	○	○	○
机构部件	○	○	○	○	○	○

○: 表示该有毒有害物质在该部件所有均质材料中的含量均在SJ/T 11363-2006规定的限量要求之下。

●: 表示符合欧盟的豁免条款，但该有毒有害物质至少在该部件的某一均质材料中的含量超出SJ/T 11363-2006的限量要求。

×: 表示该有毒有害物质至少在该部件的某一均质材料中的含量超出SJ/T 11363-2006的限量要求。

User Information

Online Registration

Be sure to register your product at our online support center:

International	http://eservice.aten.com

Telephone Support

For telephone support, call this number:

International	886-2-8692-6959
China	86-10-5255-0110
Japan	81-3-5615-5811
Korea	82-2-467-6789
North America	1-888-999-ATEN ext 4988
United Kingdom	44-8-4481-58923

User Notice

All information, documentation, and specifications contained in this manual are subject to change without prior notification by the manufacturer. The manufacturer makes no representations or warranties, either expressed or implied, with respect to the contents hereof and specifically disclaims any warranties as to merchantability or fitness for any particular purpose. Any of the manufacturer's software described in this manual is sold or licensed *as is*. Should the programs prove defective following their purchase, the buyer (and not the manufacturer, its distributor, or its dealer), assumes the entire cost of all necessary servicing, repair and any incidental or consequential damages resulting from any defect in the software.

The manufacturer of this system is not responsible for any radio and/or TV interference caused by unauthorized modifications to this device. It is the responsibility of the user to correct such interference.

The manufacturer is not responsible for any damage incurred in the operation of this system if the correct operational voltage setting was not selected prior to operation. PLEASE VERIFY THAT THE VOLTAGE SETTING IS CORRECT BEFORE USE.

Package Contents

Basic Package

The basic KE6900 / KE6940 package consists of:

1 KE6900T / KE6940T DVI KVM Over IP Extender

1 KE6900R / KE6940R DVI KVM Over IP Extender

2 Power Adapters

1 USB KVM Cable

1 DVI-D Cable 2m (KE6940 only)

1 Mounting Kits

1 User Instructions*

Check to make sure that all of the components are present and in good order. If anything is missing, or was damaged in shipping, contact your dealer.

Read this manual thoroughly and follow the installation and operation procedures carefully to prevent any damage to the switch or to any other devices on the KE6900 / KE6940 installation.

***** Features may have been added to the KE6900 / KE6940 since this manual was published. Please visit our website to download the most up-to-date version.

Manual Part No.
F/W Version:
Manual Date: 2014-12-31

Contents

Chapter 7.
Device Management

Chapter 8.
User Management

Chapter 9.
System

About This Manual

This User Manual is provided to help you get the most from your KE6900 / KE6940 system. It covers all aspects of installation, configuration and operation. An overview of the information found in the manual is provided below.

Chapter 1, Introduction, introduces you to the KE6900 / KE6940 System. Its purpose, features and benefits are presented, and its front and back panel components are described.

Chapter 2, Hardware Setup, provides step-by-step instructions for setting up your installation, and explains some basic operation procedures.

Chapter 3, OSD Operation, explains the fundamental concepts involved in operating the KE6900 / KE6940 system, and provides a complete description of the On Screen Displays (OSDs) and how to work with them.

Chapter 4, Matrix Manager Installation, explains the administrative procedures that are required to download and install the Matrix Manager software.

Chapter 5, Browser Operation, explains how to log in to the Matrix Manager with a web browser, and describes the features, functions, and how to work with the browser's interface.

Chapter 6, Dashboard, explains how to use the Matrix Manager's Dashboard tab to view connection, session, and device events.

Chapter 7, Device Management, explains how to add, configure, and organize the Transmitter and Receiver devices that will be managed over the network, as well as how to create Targets and Profiles for matrix connections.

Chapter 8, User Management, describes how to add, modify and delete user accounts; create user groups and assign users to them; specify access rights for users and groups; and specify user authentication.

Chapter 9, System, explains the Matrix Manager's global settings, and ANMS settings for LDAP/AD, RADIUS, and TACACS+ authentication and authorization.

Chapter 10, Logs, explains how to access, filter, and search the various logs that are kept by the Matrix Manager.

Chapter 11, Maintenance, explains how to use the Matrix Manager's Maintenance tab to backup, restore, upgrade firmware, install certificates, and set user preferences.

Chapter 12, Firmware Upgrade Utility, explains how to download and use the Firmware Upgrade Utility to install new firmware on the devices.

An Appendix, at the end of the manual provides technical and troubleshooting information.

Conventions

This manual uses the following conventions:

Monospaced	Indicates text that you should key in.
[ ]	Indicates keys you should press. For example, [Enter] means to press the **Enter** key. If keys need to be chorded, they appear together in the same bracket with a plus sign between them: [Ctrl+Alt].
1.	Numbered lists represent procedures with sequential steps.
♦	Bullet lists provide information, but do not involve sequential steps.
→	Indicates selecting the option (on a menu or dialog box, for example), that comes next. For example, Start → Run means to open the *Start* menu, and then select *Run*.
	Indicates critical information.

Product Information

For information about all ALTUSEN products and how they can help you connect without limits, visit ALTUSEN on the Web or contact an ALTUSEN Authorized Reseller. Visit ALTUSEN on the Web for a list of locations and telephone numbers:

International	http://www.aten.com
North America	http://www.aten-usa.com

This Page Intentionally Left Blank

Chapter 1
Introduction

Overview

The KE6900 / KE6940 DVI KVM Over IP Extender is an IP based matrix extender that allows access to a computer system from a remote USB KVM console anywhere over a LAN. The KE6900 series is a single view extender that supports one DVI display at each end. The KE6940 series is a dual view extender that supports two DVI displays at each end, allowing the video output to display across two monitors.

The KE6900 / KE6940 consists of a transmitter that connects to the computer and a receiver that provides console access from a separate location. The computer is accessed from the remote console via a standard TCP/IP network or direct Ethernet cable connection. This is perfect for any installation where you need to place the console where it is convenient, but you want the computer to reside in a secure location - away from the keyboard, mouse and display.

As a matrix extender it can connect one or more: computers-to-consoles in several ways: one-to-one (Extender mode), one-to-many (Splitter mode), many-to-one (Switch mode), or many-to-many (Matrix mode).

The KE6900 / KE6940 has a local On Screen Display (OSD) on the receiver to configure both units - for easy setup and operation. Using the transmitter and receiver over a standard TCP/IP network (optional) via Cat 5e cable allows point-to-point, point-to-multipoint, and multipoint-to-multipoint administration without needing a KVM switch. Both the transmitter and receiver have RS-232 ports to connect to a serial terminal for configuration or serial devices such as touchscreens and barcode scanners.

The Matrix Manager® software provides advanced features for username and password authentication, auto-detection of devices on the same LAN segment, management of devices, and setup of Splitter, Switch, and Matrix modes. New security features also provide extra protection with remote login security, a username and password can be required when the receiver connects to the transmitter.

With the OSD, network access, RS-232 port, software administration, and Auto MDIX, the KE6900 / KE6940 is the most cost-effective and convenient way to get a full digital extension from anywhere on the LAN.

Features

- Remote KVM console access of computers over LAN or Ethernet cable connection
- Dual console operation – control your system from both the Transmitter and Receiver by USB keyboard, monitor, and mouse
- RS-232 serial ports[1] – allows you to connect to a serial terminal for configuration, and serial devices such as touchscreens and barcode scanners
- Superior video quality – up to 1920 x 1200 @ 60 Hz; 24-bit color depth
- Supports standard VGA resolutions from 640 x 480 to 1920 x 1200 at 60Hz
- OSD (On Screen Display) on the Receiver configures both units
- Supports AP GUI operation
- Supports Web GUI[2] administration
- Remote login security
- DVI digital and analog monitor support
- Built-in ESD protection and surge protection
- Supports stereo speakers and microphone
- Auto-MDIX - automatically detects cable type
- Supports widescreen formats
- Supports High-Quality Video streaming
- Virtual Media Support
- Hot pluggable
- Rack Mountable
- Upgradeable firmware

Note: 1. RS-232 serial ports support Tx/Rx/CTS/RTS/DTR/DSR signals only.

2. The Matrix Manager web GUI can be downloaded from the ATEN website (www.aten.com).

Requirements

Console

- (KE6900) One DVI compatible monitors capable of the highest possible resolution
- (KE6940) Two DVI compatible monitors capable of the highest possible resolution
- A USB mouse
- A USB keyboard
- Microphone and speakers

Computers

The following equipment must be installed on each computer that is to be connected to the system:

- (KE6900) One DVI port
- (KE6940) Two DVI ports
- USB Type A port
- Audio ports

Cables

- For optimal signal integrity and to simplify the setup, we strongly recommend that you only use the high quality custom USB KVM Cable that is provided with this package.

Software

The minimum hardware and software requirements for the computer running the Matrix Manager software are:

- Processor: Intel or AMD processor 1 GHz or above
- RAM: 2GB or above
- HDD: 16GB or above
- Web browser
- Java Runtime Environment (JRE) 6 with update 11 or higher

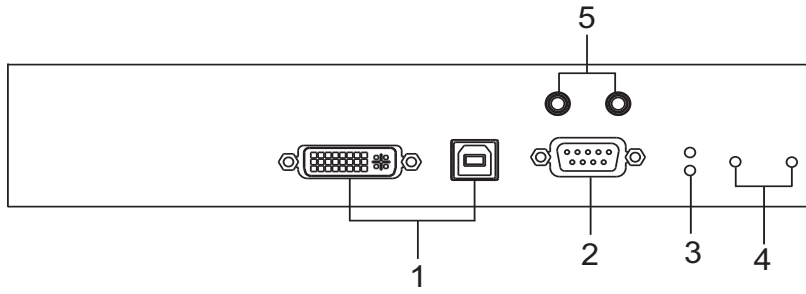
Operating Systems

Supported operating systems are shown in the table, below:

OS		Version
Windows		2000 and higher
Linux	RedHat	6.0 and higher
	SuSE	8.2 and higher
	Mandriva (Mandrake)	9.0 and higher
UNIX	AIX	4.3 and higher
	FreeBSD	3.51 and higher
	Sun	Solaris 8 and higher
Novell	Netware	5.0 and higher
Mac		OS 9 and higher

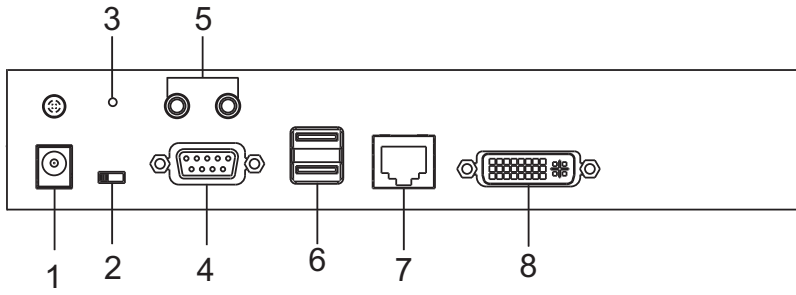
Components

KE6900T (Transmitter) Front View



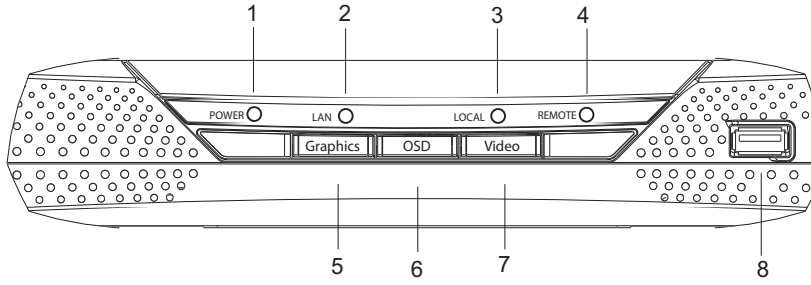
No.	Component	Description
1	KVM Ports	The USB KVM cable supplied with the package that links the Transmitter to the computer plugs into these ports.
2	RS-232 Port	This RS-232 serial port is for connecting to the computer for serial control.
3	Remote / Local LED	Lights Green to indicate which side of the installation (Local or Remote) currently has KVM control of the computer.
4	LAN / Power LED	The unit has two LEDs to indicate Status and Power.
5	Audio Ports	These mini stereo ports are for the speakers (green) and microphone (pink).

KE6900T (Transmitter) Rear View



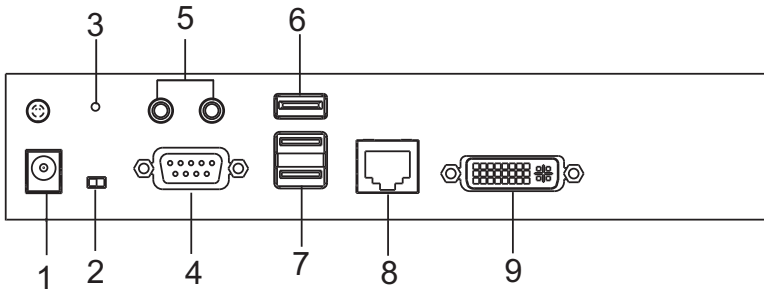
No.	Component	Description
1	Power Jack	The cable from the DC Power adapter connects here.
2	Function Switch	Use this slide switch to set the unit's mode to: ◆ **Config**ure: The device is ready to configure. ◆ **Local**: Only the local Transmitter has KVM control of the computer. The Receivers KVM access to the computer is locked. ◆ **Auto**: Shared KVM control of the computer, one at a time, with the Transmitter and Receiver consoles.
3	Reset	This switch must be pushed with a thin object, such as the end of a paper clip. ◆ Press and release to reboot the device. ◆ Power off, hold reset then power on the device while pressing reset to recover from a firmware upgrade failure. ◆ Press and hold it in for more then three seconds resets the unit back to its factory default settings.
4	RS-232 Port	This RS-232 serial port is for connecting to a serial terminal.
5	Audio Ports	These mini stereo ports are for the speakers (green) and microphone (pink).
6	Console Ports	The unit's USB keyboard and USB mouse plug into these ports.
7	LAN Port	The cable that connects the unit to the LAN plugs in here.
8	DVI-I Output	The cable from the local DVI monitor plugs in here.

KE6900R (Receiver) Front View



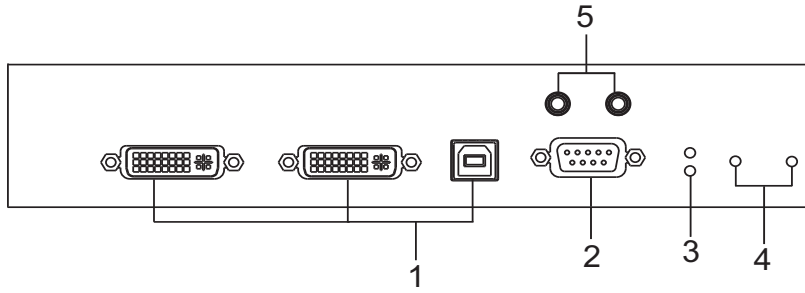
No.	Component	Description
1	Power LED	Lights blue to indicate the module is turned on.
2	LAN LED	Lights to indicate the network status: ◆ Lights Green when connected to the LAN. ◆ Off when not connected to the LAN. ◆ Blinks Green when the Ethernet connection is active. ◆ Lights Orange to indicate high network bandwidth (for ultra-high video) is being used.
3	Local LED	Lights green to Indicate the Transmitter has KVM access of the computer.
4	Remote LED	Lights green to Indicate the Receiver has KVM access of the computer.
5	Graphics Pushbutton	Sets the displays image quality to the highest possible grade, so that images are optimized.
6	OSD Pushbutton	Use this pushbutton to open the OSD menu.
7	Video Pushbutton	Sets the displays image quality to a grade that is optimized for video playback.
8	USB Port	Use this port for virtual media or a USB peripheral device. **Note:** When using a USB disk plugged into this port, see *USB Mode*, page 62.

KE6900R (Receiver) Rear View



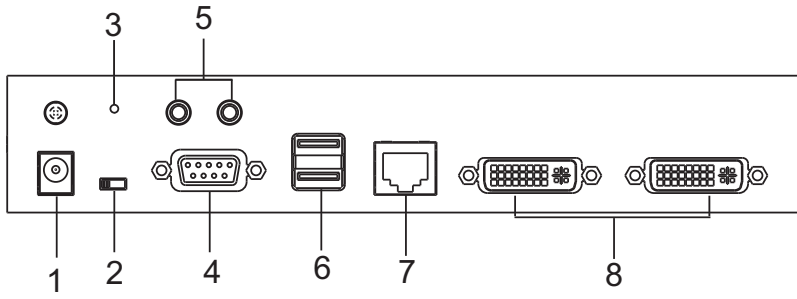
No.	Component	Description
1	Power Jack	The cable from the DC Power adapter connects here.
2	Function Switch	Use this slide switch to set the unit's mode: ◆ **Configure**: The device is ready to configure. ◆ **Auto**: KVM control of the remote computer.
3	Reset	This switch must be pushed with a thin object, such as the end of a paper clip. ◆ Press and release to reboot the device. ◆ Power off, hold reset then power on the device while pressing reset to recover from a firmware upgrade failure. ◆ Press and hold it in for more then three seconds resets the unit back to its factory default settings.
4	RS-232 Port	This RS-232 serial port is for connecting to a serial terminal.
5	Audio Ports	These mini stereo ports are for the local speakers (green) and microphone (pink).
6	USB Port	Use this port for virtual media or a USB peripheral device. **Note:** When using a USB disk plugged into this port, see *USB Mode*, page 62.
7	Console Ports	The unit's USB keyboard and USB mouse plug into these ports. When using a keyboard or mouse with special functions, see *USB Mode*, page 62
8	LAN Port	The cable that connects the unit to the LAN plugs in here.
9	DVI-I Output	The cable from the local DVI monitor plugs in here.

KE6940T (Transmitter) Front View



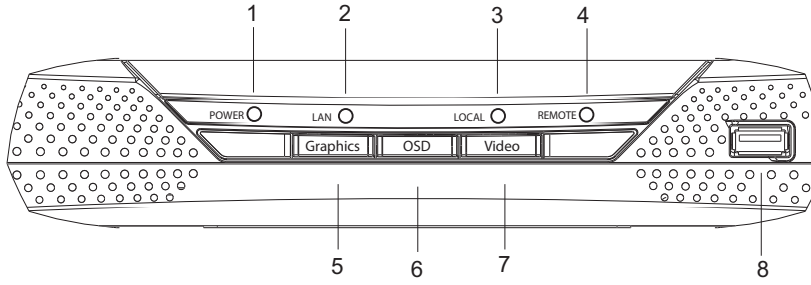
No.	Component	Description
1	KVM Ports	The USB KVM cable supplied with the package that links the Transmitter to the computer plugs into these ports.
2	RS-232 Port	This RS-232 serial port is for connecting to the computer for serial control.
3	Remote / Local LED	Lights Green to indicate which side of the installation (Local or Remote) has KVM control of the computer.
4	LAN / Power LED	The unit has two LEDs to indicate Status and Power.
5	Audio Ports	These mini stereo ports are for the speakers (green) and microphone (pink).

KE6940T (Transmitter) Rear View



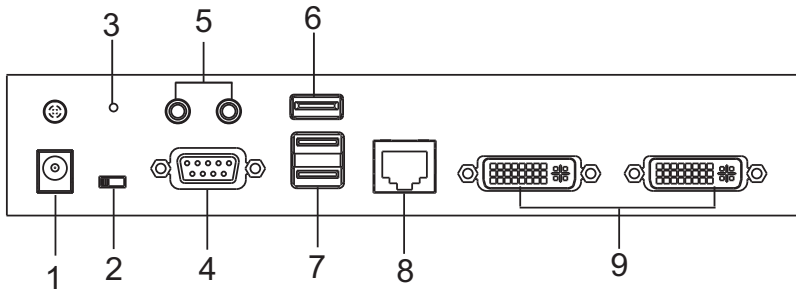
No.	Component	Description
1	Power Jack	The cable from the DC Power adapter connects here.
2	Function Switch	Use this slide switch to set the unit's mode to: ◆ **Configure**: The device is ready to configure. ◆ **Local**: Only the local Transmitter has KVM control of the computer. The Receivers KVM access to the computer is locked. ◆ **Auto**: Shared KVM control of the computer, one at a time, with the Transmitter and Receiver consoles.
3	Reset	This switch must be pushed with a thin object, such as the end of a paper clip. ◆ Press and release to reboot the device. ◆ Power off, hold reset then power on the device while pressing reset to recover from a firmware upgrade failure. ◆ Press and hold it in for more then three seconds resets the unit back to its factory default settings.
4	RS-232 Port	This RS-232 serial port is for connecting to a serial terminal.
5	Audio Ports	These mini stereo ports are for the local speakers (green) and microphone (pink).
6	Console Ports	The unit's USB keyboard and USB mouse plug into these ports.
7	LAN Port	The cable that connects the unit to the LAN plugs in here.
8	DVI-I Output	The cable from the local DVI monitor plugs in here.

KE6940R (Receiver) Front View



No.	Component	Description
1	Power LED	Lights blue to indicate the module is turned on.
2	LAN LED	Lights to indicate the network status: ◆ Lights Green when connected to the LAN. ◆ Off when not connected to the LAN. ◆ Blinks Green when the Ethernet connection is active. ◆ Lights Orange to indicate high network bandwidth (for ultra-high video) is being used.
3	Local LED	Lights green to Indicate the Transmitter has KVM access of the computer.
4	Remote LED	Lights green to Indicate the Receiver has KVM access of the computer.
5	Graphics Pushbutton	Sets the displays image quality to the highest possible grade, so that images are optimized.
6	OSD Pushbutton	Use this pushbutton to open the OSD menu.
7	Video Pushbutton	Sets the displays image quality to a grade that is optimized for video playback.
8	USB port	Use this port for virtual media or a USB peripheral device. **Note:** When using a USB disk plugged into this port, see *USB Mode*, page 62.

KE6940R (Receiver) Rear View



No.	Component	Description
1	Power Jack	The cable from the DC Power adapter connects here.
2	Function Switch	Use this slide switch to set the unit's mode: ◆ **Configure**: The device is ready to configure. ◆ **Auto**: KVM control of the computer.
3	Reset	This switch must be pushed with a thin object, such as the end of a paper clip. ◆ Press and release to reboot the device. ◆ Power off, hold reset then power on the device while pressing reset to recover from a firmware upgrade failure. ◆ Press and hold it in for more then three seconds resets the unit back to its factory default settings.
4	RS-232 Port	This RS-232 serial port is for connecting to a serial terminal.
5	Audio Ports	These mini stereo ports are for the local speakers (green) and microphone (pink).
6	USB Port	Use this port for virtual media or a USB peripheral device. **Note:** When using a USB disk plugged into this port, see *USB Mode*, page 62.
7	Console Ports	The unit's USB keyboard and USB mouse plug into these ports.
8	LAN Port	The cable that connects the unit to the LAN plugs in here.
9	DVI-I Output	The cable from the local DVI monitors plug in here.

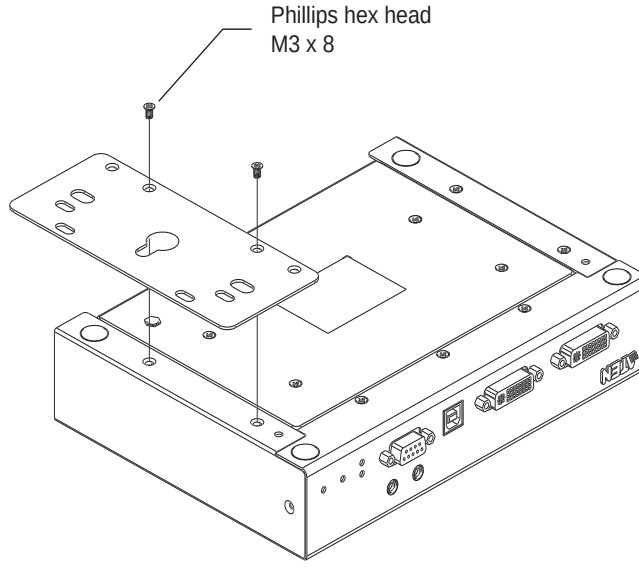
Chapter 2
Hardware Setup

1. Important safety information regarding the placement of this device is found on page 131. Please review it before proceeding.
2. Make sure that the power to all devices connected to the installation is turned off. You must unplug the power cords of any computers that have the Keyboard Power On function.

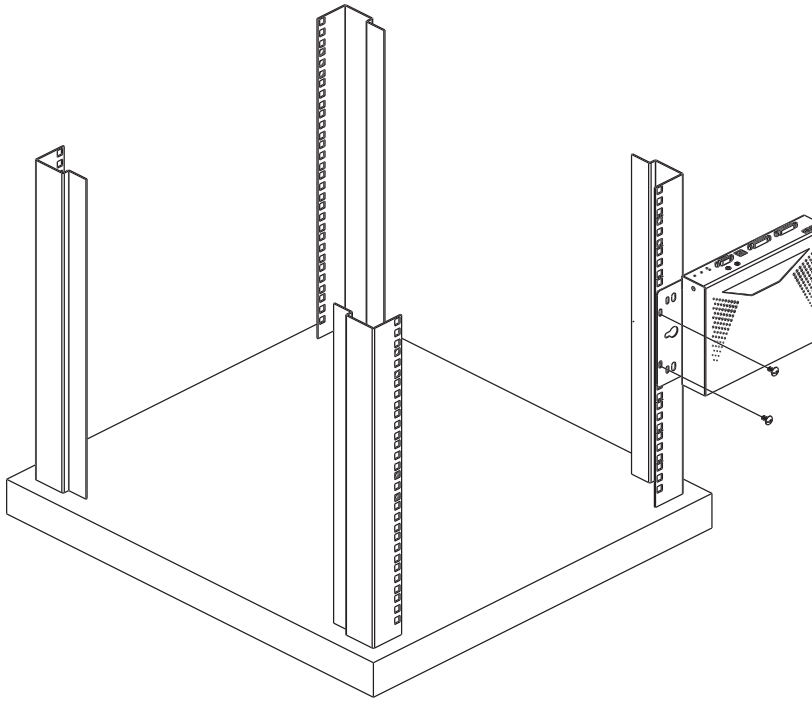
Rack Mounting

For convenience and flexibility, the Transmitter can be mounted on system racks. To rack mount a unit do the following:

1. Using the screws provided in the Mounting Kit, screw the mounting bracket into the bottom of the Transmitter as show in the diagram below:



2. Screw the bracket into a convenient location on the rack.

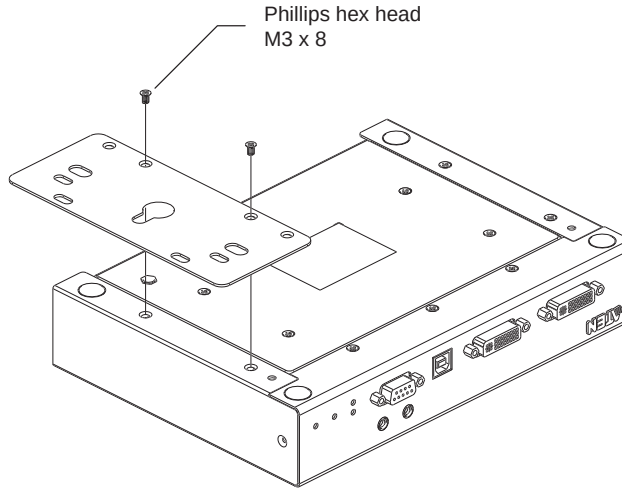


Note: These screws are not provided. We recommend that you use M5 x 12 Phillips Type I cross recessed type screws.

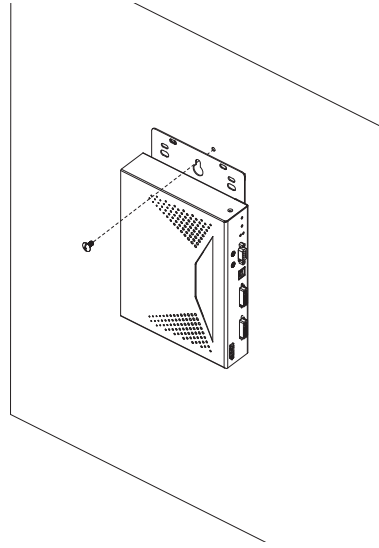
Wall Mounting

For convenience the Transmitter can be mounted to a wall.

1. Using the screws provided in the Mounting Kit, screw the mounting bracket into the bottom of the Transmitter as show in the diagram below:



2. Use the center hole to screw the bracket to a secure wall surface.



Setting Up a Point-to-Point Installation

Setting up the KE6900 / KE6940 system in a point-to-point configuration is simply a matter of plugging in the cables.

Note: In a point-to-point configuration, no administrator setup is necessary.

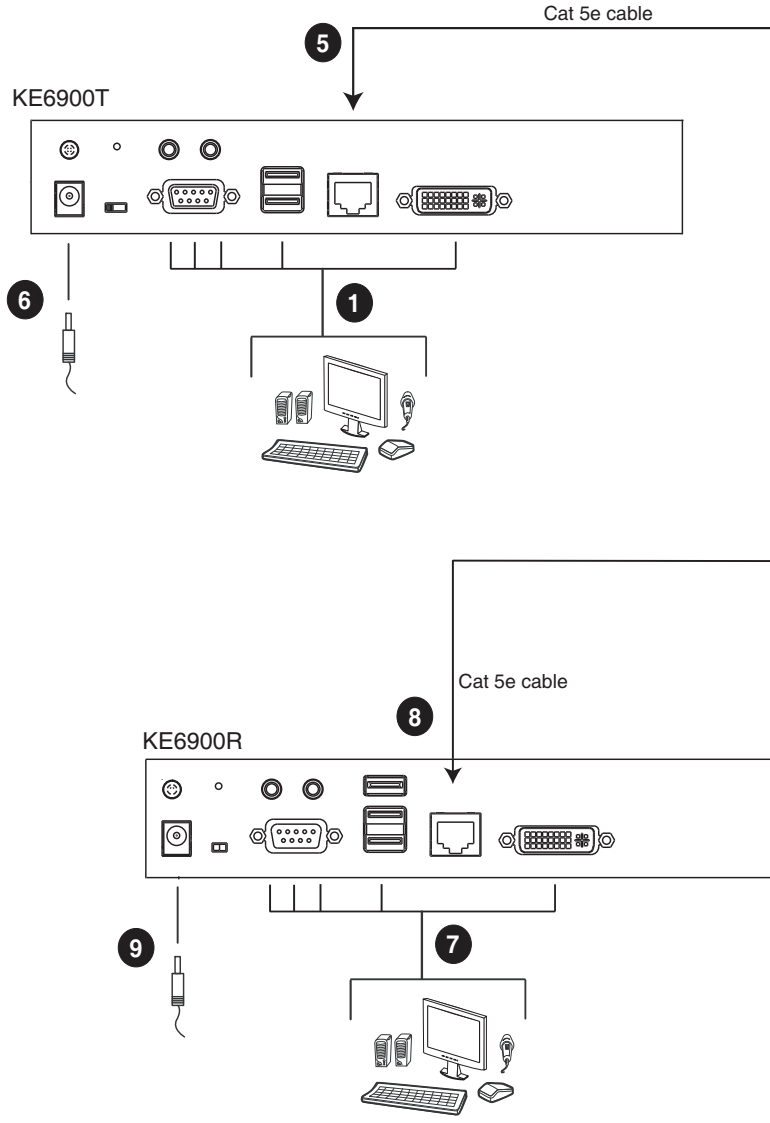
Make sure that all the equipment is powered off. Refer to the installation diagrams on the next two pages and do the following:

1. On the Transmitter side, plug the mouse, keyboard, DVI monitor, microphone and speakers into the ports on the Console section of the KE6900T / KE6940T*. Each port is marked with an appropriate icon to indicate itself.
2. Connect the USB KVM cable provided to the KVM Ports on the front of the KE6900T / KE6940T.
3. Connect the other end of the USB KVM cable to the keyboard, video, mouse, speaker and microphone ports on the computer.
4. For control of serial devices, connect the RS-232 serial port on the Transmitter to a serial port on the computer.
5. Connect a Cat 5e cable to the KE6900T / KE6940T's LAN port.
6. Plug the power adapter into an AC source; and plug the other end into the KE6900T / KE6940T's Power Jack.
7. On the Receiver side, plug the mouse, keyboard, DVI monitor, microphone, and speakers into the ports on the Console section of the KE6900R / KE6940R*.
8. Connect the other end of the Cat 5e cable to the KE6900R / KE6940R's LAN port.
9. Plug the second power adapter into an AC source; and plug the other end into the KE6900R / KE6940R's Power Jack.
10. Power on the computer.

Note: 1. If installing the KE6940 with two DVI monitors, connect the second DVI monitor and KVM DVI cable into the additional ports on the KE6940 and computer.

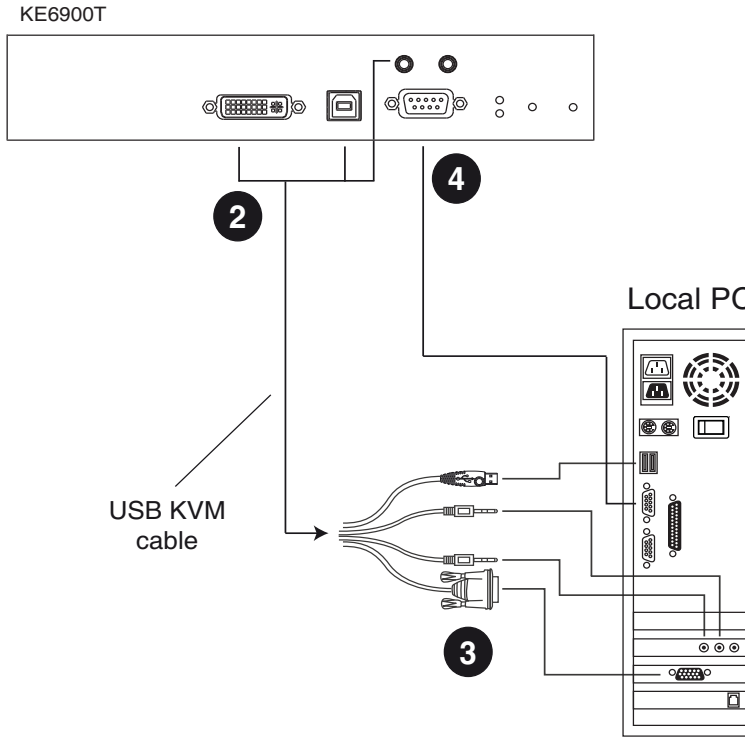
2. A keyboard or mouse with special functions may need to use the USB ports for advanced features to work (see *USB Mode*, page 62).

Point-to-Point Installation 1 of 2



Note: The diagram above shows the KE6900T and KE6900R. The KE6940 installation is the same except that an additional DVI monitor can be connected at each end for a dual-view display setup.

Point-to-Point Installation 2 of 2



Note: The serial port on the Transmitter (shown above) connects to the computer; the serial port on the Receiver (not shown) connects to a serial device (optional).

Setting Up a LAN Installation

Setting up the units on a network allows point-to-point, point-to-multipoint, and multipoint-to-multipoint computer to console operation by connecting multiple KE6900 / KE6940 devices on the same TCP/IP LAN.

Note: 1. The units are preconfigured with factory-default network settings. If you install only one set of KE6900 / KE6940 units, you do not need to change these default network settings. See *Default IP Addresses*, page 24, for further details.

2. In a network setup with multiple units, each Transmitter and Receiver must be configured with a unique IP address. See *Network Configuration*, page 23, for further details.

3. We recommended using 1000Mbps Gigabit Ethernet switches between KE69xx devices installed on different LAN segments. 10/100Mbps switches might cause poor performance.

4. In multipoint configurations, the IGMP and flow control function of your network switches/hubs must be enabled to avoid the deterioration of data throughput. To ensure functionality use a layer 3 switch that supports IGMP queries.

5. If your network uses cascaded switches, please check to ensure the data throughput is sufficient.

6. To get the best performance, we suggest creating a private network for KE69xx devices, as they are bandwidth-intensive devices.

Make sure that all the equipment is powered off. Refer to the installation diagram on the following page, and do the following:

1. On the Transmitter side, plug the mouse, keyboard, DVI monitor, microphone and speakers into the ports on the Console section of the KE6900T / KE6940T*. Each port is marked with an appropriate icon to indicate itself.

2. Connect the USB KVM cable provided to the KVM Ports on the front of the KE6900T / KE6940T.

3. Connect the other end of the USB KVM cable to the keyboard, video, mouse, speaker and microphone ports on the computer.

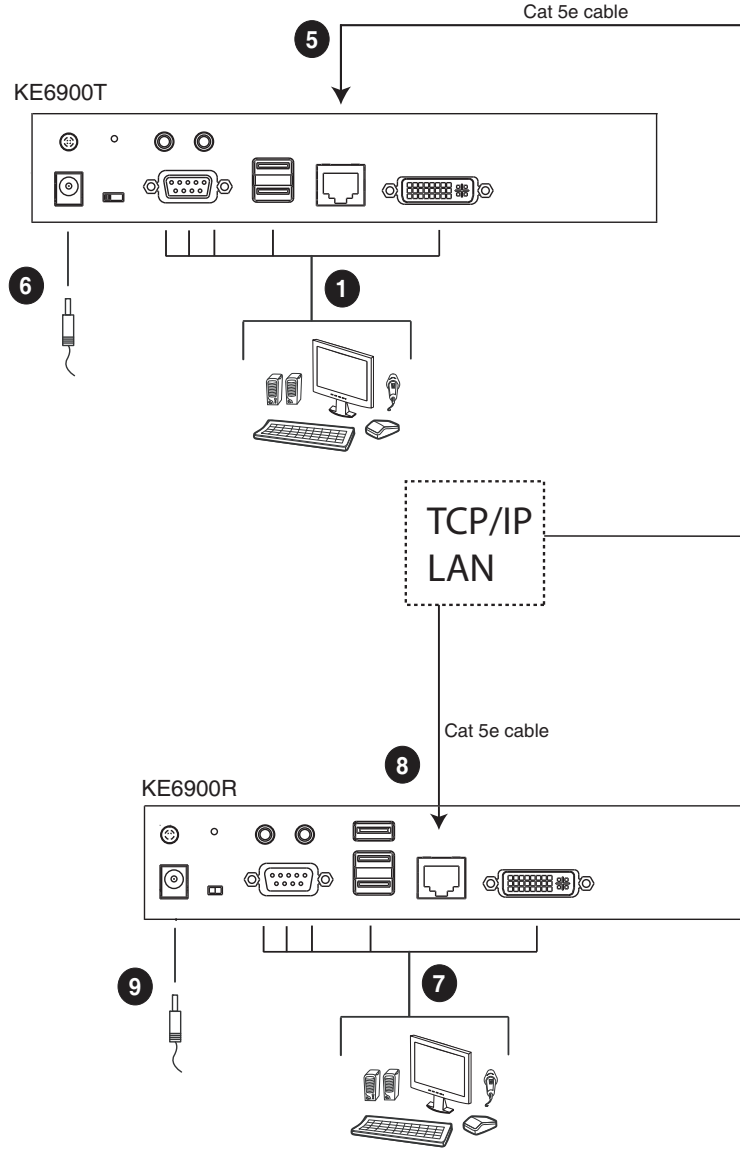
4. For control of serial devices, connect the RS-232 serial port on the Transmitter to a serial port on the computer.

5. Use a Cat 5e cable to connect the KE6900T / KE6940T's LAN port to the local area TCP/IP network.
6. Plug the power adapter into an AC source; and plug the other end into the KE6900T / KE6940T's Power Jack.
7. On the Receiver side, plug the mouse, keyboard, DVI monitor, microphone, and speakers into the ports on the Console section of the KE6900R / KE6940R*.
8. Use a Cat 5e cable to connect the KE6900R / KE6940R's LAN port to the local area TCP/IP network.
9. Plug the second power adapter into an AC source; and plug the other end into the KE6900R / KE6940R's Power Jack.
10. Use the OSD on the Receiver to configure the network settings for both devices (See *Network Configuration*, page 23).
11. Repeat these steps for each Transmitter and Receiver you wish to install on the network.
12. Power on the computer(s).

Note: 1. If installing the KE6940 with two DVI monitors, connect the second DVI monitor and KVM DVI cable into the additional ports on the KE6940 and computer.

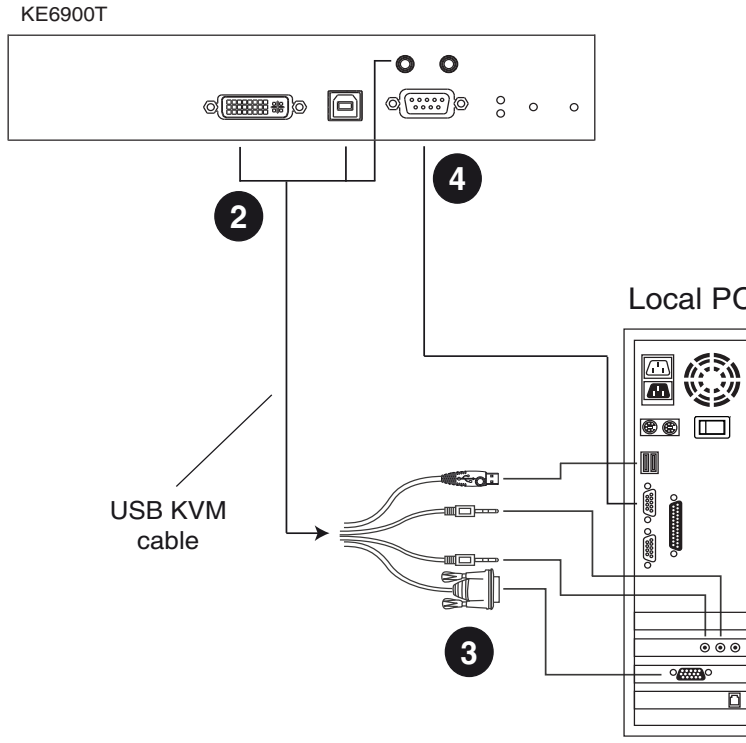
2. A keyboard or mouse with special functions may need to use the USB ports for advanced features to work (see *USB Mode*, page 62).

Network Installation Diagram 1 of 2



Note: The diagram above shows the KE6900T and KE6900R. The KE6940 installation is the same except that an additional DVI monitor can be connected at each end for a dual-view display setup.

Network Installation Diagram 2 of 2



Note: The serial port on the Transmitter (shown above) connects to the computer; the serial port on the Receiver (not shown) connects to a serial device (optional).

Network Configuration

This section provides instructions to configure the network settings with a fixed IP address, subnet mask, and default gateway. To use the **IP Installer** to configure the IP address, see *IP Installer*, page 137.

Note: 1. Both devices are preconfigured with factory-default network settings. If you install only one set of KE6900 / KE6940 units, you do not need to change these default network settings. See *Default IP Addresses*, page 24, for further details.

2. In a network setup with multiple units, each KE6900T / KE6940T and KE6900R / KE6940R must be configured with a unique IP address. See *Network Configuration*, page 23, for further details.

3. We recommended using 1000Mbps Gigabit Ethernet switches between KE69xx devices installed on different LAN segments. 10/100Mbps switches might cause poor performance.

4. In multipoint configurations, the IGMP and flow control function of your network switches/hubs must be enabled to avoid the deterioration of data throughput. To ensure functionality use a layer 3 switch that supports IGMP queries.

5. If your network uses cascaded switches, please check to ensure the data throughput is sufficient.

6. To get the best performance, we suggest creating a private network for KE69xx devices, as they are bandwidth-intensive devices.

To configure the network settings, do the following:

1. Setup the hardware and connect the Transmitter and Receiver to the local area network (See *Setting Up a LAN Installation*, page 19, for details).
2. From the Receiver, tap the **Scroll Lock** key twice to invoke the OSD.
3. Select the *User Station* or *Transmitter* from the Sidebar menu.
4. Enter the password and click **Configure**.

   The default password is: `password`.
5. From the *Network* tab select **Set IP address manually** and enter the following:
   - *IP Address*– sets the IP address for the KE6900 / KE6940. Key in a valid unique IP address.

Note: See *Default IP Addresses*, page 24, for the preconfigured factory-default settings.

- *Subnet Mask* – sets the subnet mask for the KE6900 / KE6940. Key in a valid subnet mask value.

Note: The default setting is `255.255.255.0`

- *Default Gateway*– sets the default gateway for the KE6900 / KE6940. Key in a valid default gateway.

6. Click **Save**.

Return

To exit the OSD, press **[Esc]** on the keyboard, click **Logout**; tap the **Scroll Lock** key twice; or return to the OSD main page and press the front panel OSD pushbutton (Receiver only).

At this point the User Station can connect to the Transmitter to access the remote computer (see *Connecting*, page 38 for instructions).

Default IP Addresses

The preconfigured factory-default IP addresses for the KE6900 / KE6940 units are as follows:

KE6900T / KE6940T – `192.168.0.61`

KE6900R / KE6940R – `192.168.0.60`

Chapter 3
OSD Operation

Overview

This chapter provides instructions to configure and operate the KE6900 / KE6940 using the local On Screen Display (OSD). To configure the network settings with the OSD, see *Network Configuration*, page 23.

LED Display

Both the Transmitter and Receiver have front panel LEDs to indicate their operating and power status, as explained in the table below:

LED	Indication
LAN	◆ Lights when LAN is connected. ◆ Off when LAN is not connected. ◆ Blinks when Ethernet is active. ◆ Lights Green to indicate high network bandwidth (ultra-high video) is in use.
Power	◆ OFF when power is off. ◆ Lights Blue when the unit is powered on
Local	◆ Lights Green to Indicate the Transmitter has KVM focus of the computer
Remote	◆ Lights Green to Indicate the Receiver has KVM focus of the computer.

Invoking the OSD

The On Screen Display (OSD) is a keyboard/mouse-driven application on the receiver used to configure the transmitter and receiver settings. Once the receiver has discovered the transmitter over a network* or direct Ethernet cable connection, you can use the OSD on the receiver to configure the transmitter's settings.

To invoke the OSD, press the OSD pushbutton on the front of the receiver, or from the keyboard tap the **Scroll Lock** key twice. The *OSD* main page will appear (see *OSD Interface*, page 27).

To exit the OSD, press **[Esc]** on the keyboard; click **Logout**; tap the **Scroll Lock** key twice; or return to the OSD main page and press the OSD pushbutton on the front of the receiver. The OSD disappears and the computer desktop screen or the System Login prompt is displayed.

Note: 1. For the Receiver to discover the Transmitter over a network, both must be on the same subnet of the LAN.

2. You can change the OSD hotkeys. See *User Preferences*, page 37 for details.

3. If the keyboard/mouse won't work when the OSD is invoked, see *USB Mode*, page 62.

OSD Interface

After you invoke the OSD, the main page appears:

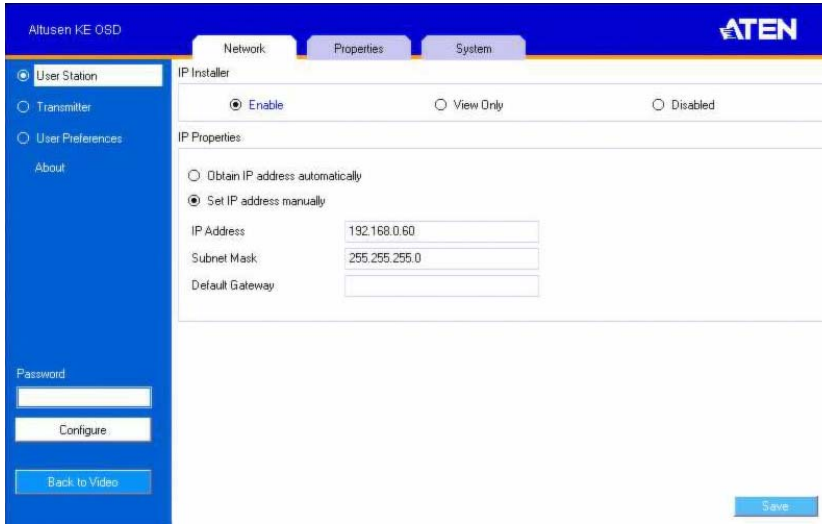
Note: A password is required to enter the OSD. The default password is: *password*. For security purposes, we recommend you change this to something unique.

The OSD components are described in the table, below:

No.	Item	Description
1	User Station (Receiver)	Select this radio button, enter a password, and click Configure to enter the *User Station Configuration* screen.
2	Transmitter	Select this radio button, enter a password, and click Configure to enter the *Transmitter Configuration* screen. **Note:** Receiver must first discover the transmitter over the network for this option to be available.
3	User Preferences	Select this radio button, enter a password, and click Configure to enter the *User Preferences* screen.
4	About	About provides information regarding the OSD version.
5	Password	Input the OSD password and click Configure to enter the selected configuration screen. See note for password.
6	Configure	After entering a password, click **Configure** to enter the selected configuration screen.
7	Back to Video	Clicking this button exits the OSD and returns you to the computer's video display.

User Station Configuration

When you select the *User Station* radio button and click **Configure** to login, the Network tab appears:



Network

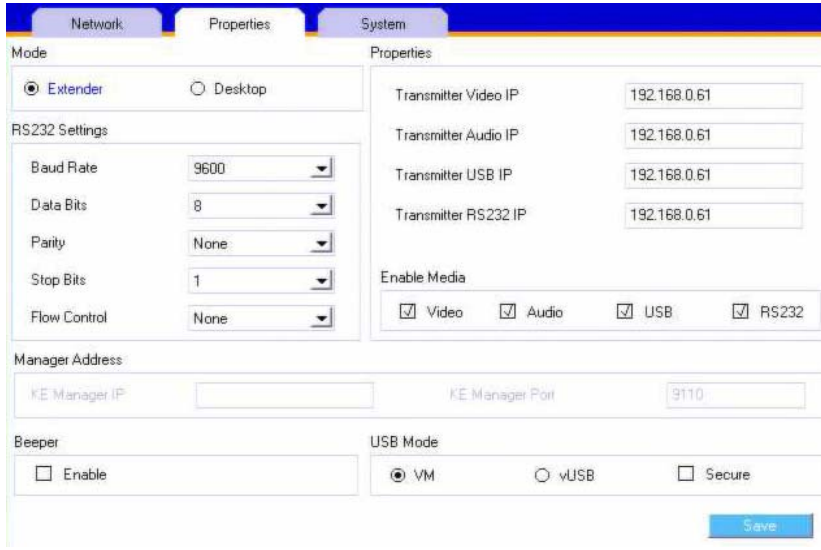
The Network tab allows you to configure the User Station's IP address settings:

Item	Description
IP Installer	The IP Installer is an external Windows-based utility for assigning an IP address to the device. Click one of the radio buttons to select **Enable**, **View Only**, or **Disable** for the IP Installer utility. See *IP Installer*, page 137 for instructions. **Note:** For security, we strongly recommend that you set this to *View Only* or *Disable* after each use.
Network Configuration	For dynamic IP address assignment (DHCP), select the **Obtain IP address automatically** radio button. To specify a fixed *IP Address*, *Subnet Mask*, and *Default Gateway* select the **Set IP address manually** radio button and fill in the fields with values appropriate for your network. For help configuring network settings with the OSD, See *Network Configuration*, page 23.

After entering the information, click **Save**.

Properties

The *Properties* tab allows you to configure the User Station's extender settings:



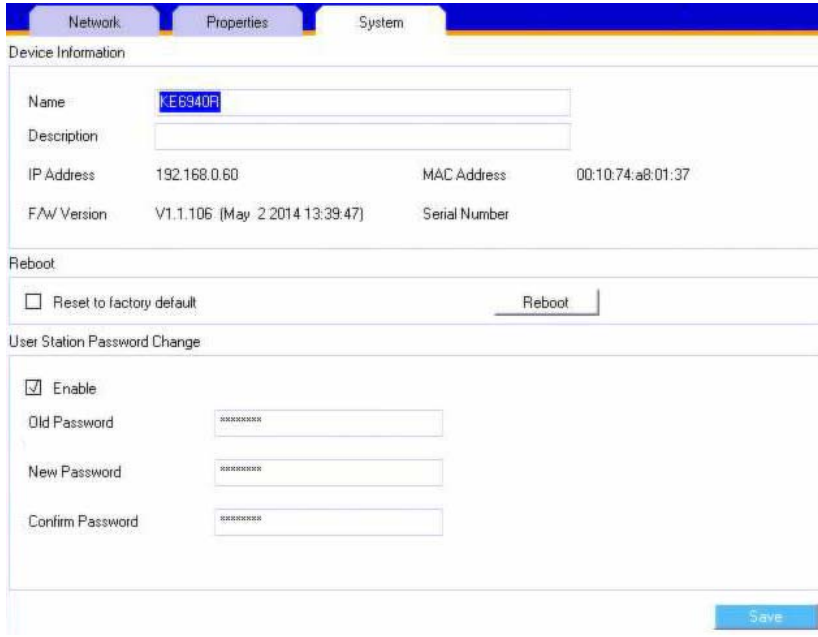
Item	Description
Mode	Select **Extender** mode for simple one-to-one (Transmitter to User Station) setups that are managed with the Receiver's OSD menu. Select **Desktop/Matrix** mode to manage devices and connections from the Matrix Manager web GUI. This mode is for advanced administration of Transmitter to User Station connections. (See *Target Connections*, page 74)
Properties	If you selected **Extender** mode (above) set the Transmitter IP address for the User Station's Video, Audio, USB, and RS232 source signals. If you selected **Desktop/Matrix** mode (above) the *Properties* will be grayed out. Use Targets to configure the Transmitter connections. (See *Target Connections*, page 74)

Item	Description
RS232 Settings	Configure the serial device settings for the User Station. The default settings are: Baud Rate: 9600 Parity: None Data Bits: 8 bits Stop bits: 1 bit Flow Control: None
Enable Media	Select which type of media the User Station can stream from Transmitters: Video, Audio, USB, and RS232.
Manager Address	Set the **IP** address and **Port** number of the computer running the Matrix Manager software. The default port number is 9110.
Beeper	Check this box to allow the User Station to beep when configuration changes are made to it.
USB Mode	Select the type of USB device you will connect to the USB ports: **vUSB**: Use this option to plug USB peripherals into the USB ports. This option also allows a keyboard and mouse with special functions to plug into the USB ports for console use. Use this only if the special functions of the keyboard or mouse are required but do not work when plugged into the console ports. When the keyboard and mouse are plugged into the USB ports, they will not work within the OSD menus. To work within the OSD menus, the keyboard and mouse must be plugged into the console ports. **VM** (Virtual Media): Only select this option if you are plugging a USB disk into the USB ports. This will give you the highest data transfer speeds but will not allow other USB devices plugged into the USB ports to work. **Secure**: Check this box to encrypt USB drives plugged into the USB ports.

After entering the information, click **Save**.

System

The *System* tab allows you to configure the User Station's general settings:

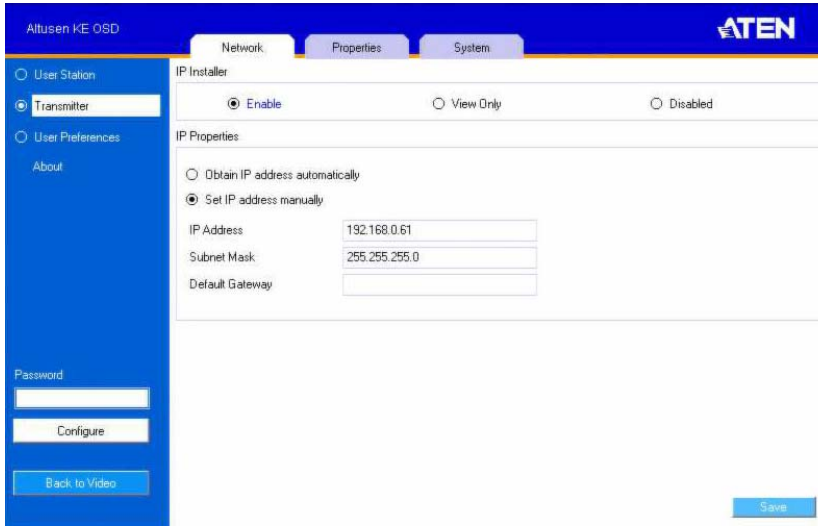


Item	Description
Device Information	Enter the **Name**, **Location**, and **Description** of the User Station. It also displays the *IP Address*, *MAC Address*, *F/W Version*, *Serial Number*, and *Model Number* of the User Station.
Reboot	Check the box and click **Reboot** to reset the User Station's settings back to the factory default. All custom settings will be lost.
User Station Password Change	Check **Enable** to require a password for access to the User Station's OSD configuration screen. Enter the Old Password, enter a New Password, and confirm the new password in the Confirm Password box.

After entering the information, click **Save**.

Transmitter Configuration

When you select the *Transmitter* radio button and click **Configure** to login, the Network tab appears:



Network

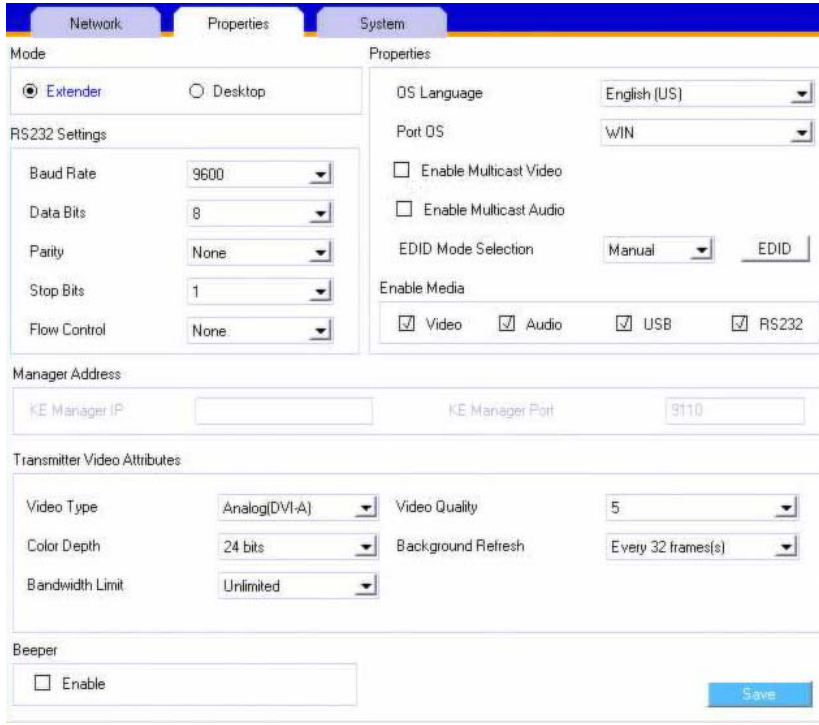
The *Network* tab allows you to configure the Transmitter's IP address settings:

Item	Description
IP Installer	The IP Installer is an external Windows-based utility for assigning an IP address to the device. Click one of the radio buttons to select **Enable**, **View Only**, or **Disable** for the IP Installer utility. See *IP Installer*, page 137 for instructions. **Note:** For security, we strongly recommend that you set this to *View Only* or *Disable* after each use.
Network Configuration	For dynamic IP address assignment (DHCP), select the **Obtain IP address automatically** radio button. To specify a fixed *IP Address*, *Subnet Mask*, and *Default Gateway* select the **Set IP address manually** radio button and fill in the fields with values appropriate for your network. For help configuring network settings with the OSD, See *Network Configuration*, page 23.

After entering the information, click **Save**.

Properties

The *Properties* tab allows you to configure the Transmitter's extender settings:



Item	Description
Mode	Select **Extender** mode for simple one-to-one (Transmitter to User Station) setups that are managed with the Receiver's OSD menu. Select **Desktop/Matrix** mode to manage devices and connections from the Matrix Manager web GUI. This mode is for advanced administration of Transmitter to User Station connections. (See *Target Connections*, page 74)

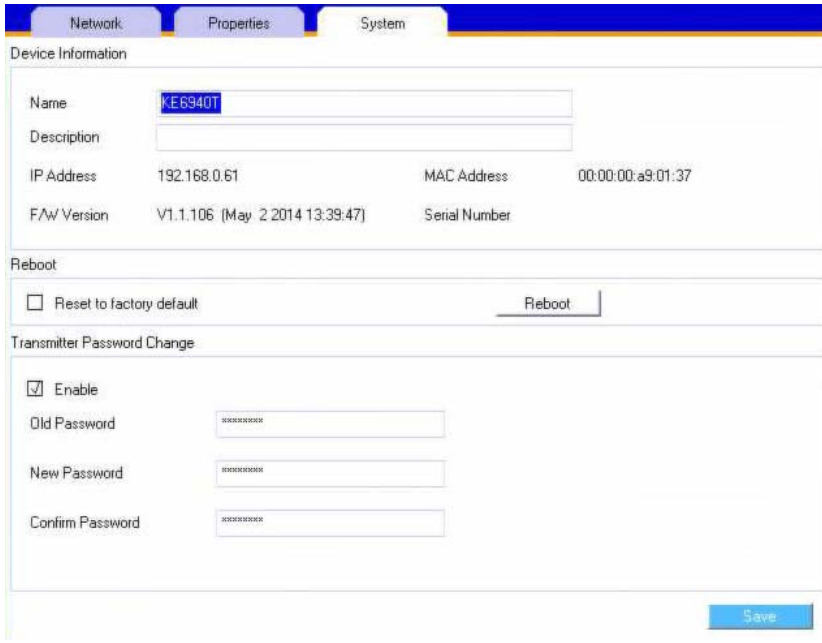
Item	Description
Properties	**Port OS:** Use the drop-down menu to select the operating system of the computer connected to the Transmitter. **OS Language:** Use the drop-down menu to select the operating system language of the computer connected to the Transmitter. **Enable Multicast Video:** Check this box to allow a broadcast of the Transmitter's video signal to be sent out to multiple User Stations. **Enable Multicast Audio:** Check this box to allow a broadcast of the Transmitter's audio signal to be sent out to multiple User Stations. **EDID Mode Selection**: EDID contains a display's basic information and is used by the source device to utilize the best resolution across different monitors. Select how you want the source device to acquire the display's EDID: ◆ **Default**: EDID is set to the default ATEN configuration. ◆ **Auto**: Checks the EDID of all connected displays and uses the best resolution for all displays. ◆ **Manual**: Manually set the EDID configuration from the Connections Page (see page 39). ◆ **Remix**: Checks the EDID of all connected displays and the source device uses the best common resolution for all displays.
Enable Media	Select which type of media the Transmitter can stream to User Stations: Video, Audio, USB, and RS232.
RS232 Settings	Configure the serial device settings for the Transmitter. The default settings are: Baud Rate: 9600 Parity: None Data Bits: 8 bits Stop bits: 1 bit Flow Control: None
Manager Address	Set the **IP** address and **Port** number of the computer running the Matrix Manager software. The default port number is 9110.

Item	Description
Transmitter Video Attributes	To set the Transmitter's video settings: **Video Type**: Select the DVI video connector being used by the display: Digital (DVI-D) or Digital (DVI-I). **Color Depth**: Select the number of bits to use for the color depth: 24, 16, or 8. This is the number of bits used to describe the color of a single pixel. A bit depth determines the number of colors that can be displayed at one time. **Bandwidth Limit:** Select the maximum bandwidth that the Transmitter can use to transmit video over the network. A lower bandwidth setting transmits lower quality video; a higher bandwidth setting sends higher quality video but this can affect network speed. **Video Quality:** Select the video quality to use. 5 is the highest video quality, and 1 is the lowest video quality. Options are: 1~5. **Background Refresh:** Sets how often the Transmitter refreshes the background image on the connected display. Options are to refresh every 256,128, 64, 32,16, or 0 frames.
Beeper	Check this box to allow the device to beep every time a configuration change is made.
Occupy Timeout	Set a time threshold for devices whose Access Mode has been set to Occupy (see *Allowed Access Mode*, page 100). If there is no activity from the User Station occupying the port for the amount of time set here, the User Station is timed out and the port is released. The first User Station to send keyboard or mouse input after the port has been released gets to occupy the port. Input a value from 1 to 240 seconds.

After entering the information, click **Save**.

System

The *System* tab allows you to configure the Transmitter's general settings:

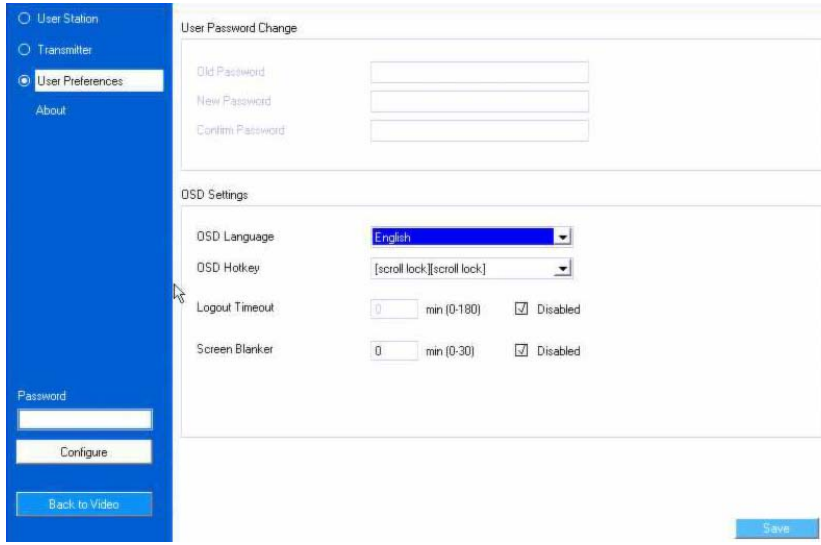


Item	Description
Device Information	Enter the **Name**, **Location**, and **Description** of the Transmitter. It also displays the *IP Address*, *MAC Address*, *F/W Version*, *Serial Number*, and *Model Number* of the Transmitter.
Reboot	Check the box and click **Reboot** to reset the Transmitter's settings back to the factory default. All custom settings will be lost.
Transmitter Password Change	Check **Enable** to require a password for access to the Transmitter's OSD configuration screen. Enter the Old Password, enter a New Password, and confirm the new password in the Confirm Password box.

After entering the information, click **Save**.

User Preferences

When you select the *User Preferences* radio button and click **Configure** to login, the configuration screen appears:

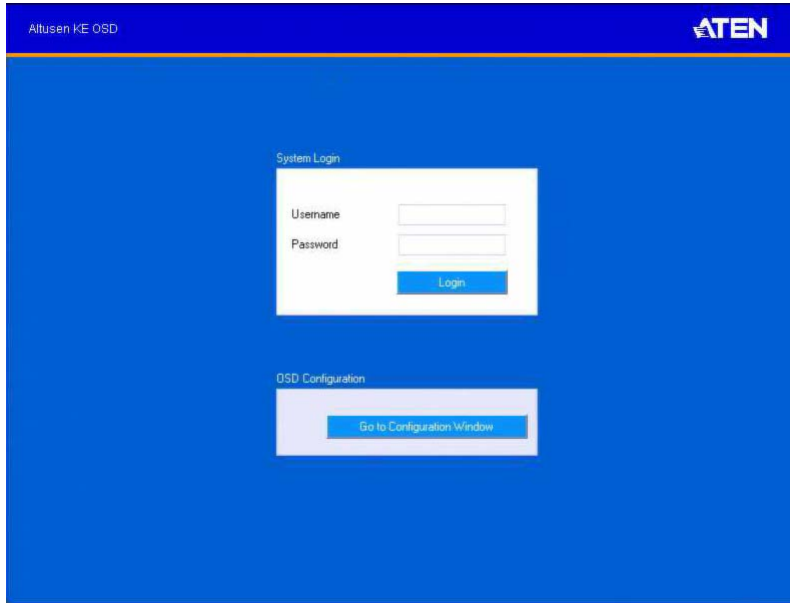


Item	Description
User Password Change	This section allows you to change the OSD password: 1. Key in the old password in the Old password field. 2. Key in the new password in the New password field. 3. Key in the new password again in the Confirm password field.
OSD Language	Click the drop-down menu to select the language you want to use for OSD sessions. Choices are: English, Chinese (Simplified), Chinese (Traditional), Japanese, Korean, Dutch, French, Spanish, Portuguese, and Russian.
OSD Hotkey	Select the hotkey combination to invoke the OSD screen.
Logout Timeout	If there is no user input for the amount of time set with this function, the user is automatically logged out of the OSD. A login is necessary before the OSD can be accessed again.
Screen Blanker	Set how many minutes the OSD waits when a session is idle before turning off the display.

When you have made your choices, Click **Save**.

Connecting

If the User Station is set to **Extender** mode, the video screen of the remote computer will appear automatically when you exit the OSD (tap the **Scroll Lock** key twice). In **Desktop/Matrix** mode you will see the *System Login* screen, which provides access to the *Connection Page* by entering a username and password:



Note: 1. The administrator account can be used to log in for the first time. Username: *administrator* | Password: *password*. For security purposes, we recommend you change this to something unique (see *User Management*, page 85).

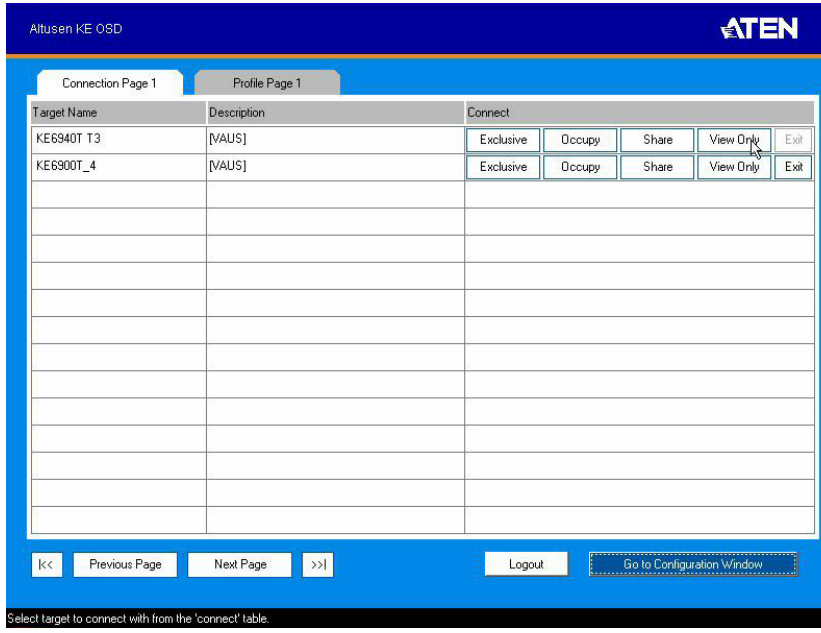
2. If the User Station does not require a login, click *Login to system* (see *Login Required*, page 62).

3. For information about Extender and Desktop/Matrix modes see *Mode*, page 29.

After you login the *Connection Page* appears, as shown on the next page.

Connections Page

After you have successfully logged in the *Connection Page* appears:



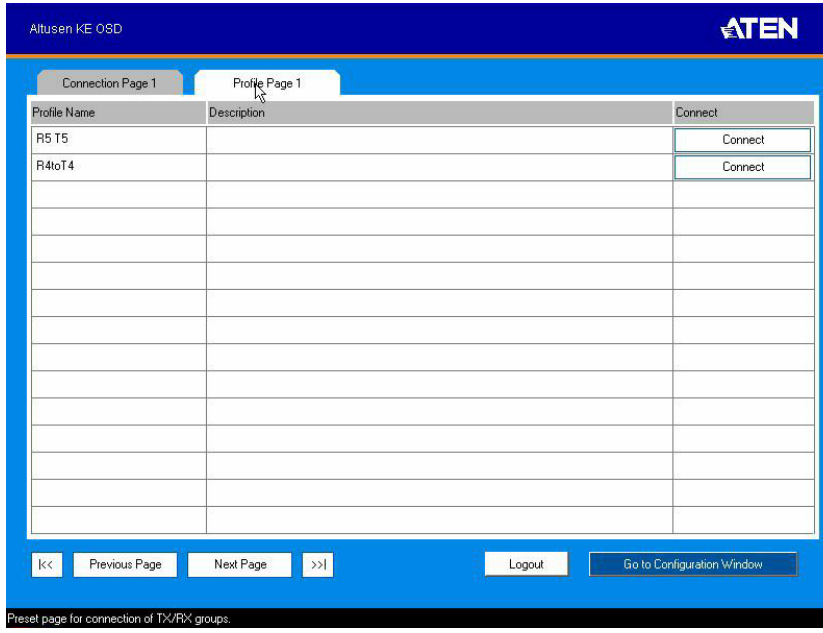
The *Connection Page* components are described in the table, below:

No.	Item	Description
1	Target Name	Lists the Target connections available for the User Station. A Target is a defined connection to Transmitters, created in the Device Management tab of the Matrix Manager (see *Targets*, page 75).
2	Description	This field provides a description of the Target, entered when it was created.

No.	Item	Description
3	Connect	To connect the User Station to a Target, click the access type: **Exclusive**: The first User Station to access the Target has exclusive control over the Target. No other User Stations can view the Target. The Timeout function does not apply to this setting. **Occupy**: The first User Station to access the Target has control over the Target. However, additional User Stations may view the Target's video display. If the User Station controlling the Target is inactive for longer than the time set in the Timeout box, control is transferred to the first User Station to move the mouse or strike the keyboard. **Share**: Can simultaneously share control over the Target. Input from the User Stations is placed in a queue and executed chronologically. **View Only**: User Station connects with view only access to the Targets video display.
4	Next Page	Use this button to navigate to the next page if there are more Targets than can be listed on one page.
5	Previous Page	Use this button to navigate to the previous page if there are more Profiles than can be listed on one page.
6	Manual EDID	If the EDID is set to Manual, the Manual EDID button appears. Click **Manual EDID** to adjust the EDID setting locally. When the Operation Successful box appears, click OK. (See *Properties*, page 34, for details)
7	Logout	Click this button to log out of the Connection Page.
8	Go to Configuration Window	Click this button to return to the main OSD screen.

Profile Page

Click the *Profile Page* tab and the following screen appears:



The *Profile Page* components are described in the table, below:

No.	Item	Description
1	Profile Name	Lists the Profiles available. Profiles give User Stations access to Targets and allow you to push the connection.
2	Description	The field provides a description of the Profile that was entered when it was created.
3	Connect	Click **Connect** and the User Station will re-connect with the settings of that Profile (see *Profiles*, page 81).
4	Next Page	Use this button to navigate to the next page if there are more Profiles than can be listed on one page.
5	Previous Page	Use this button to navigate to the previous page if there are more Profiles than can be listed on one page.
6	Logout	Click this button to log out of the Connection Page.
7	Go to Configuration Window	Click this button to return to the main OSD screen.

This Page Intentionally Left Blank

Chapter 4
Matrix Manager Installation

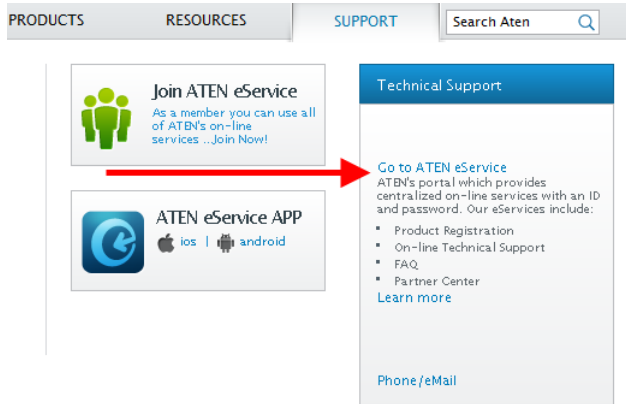
Overview

The *Matrix Manager* is a browser based GUI that provides management of KE6900 / KE6940 devices over a network . Download and install the software to begin managing the KE6900 / KE6940 devices from a computer using a web browser.

Download

To download the Matrix Manager Lite software, do the following:

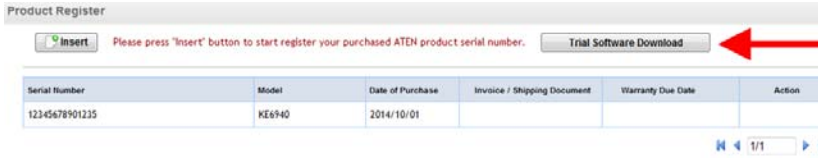
1. Visit our website and click *Support* → **Go to ATEN eService**.



2. Create an account and login to ATEN eService.

3. Register the KE690x device(s) you have purchased.

4. After you have registered the KE device(s), click **Trial Software Download**.



Note: The trial software includes full functions to setup and configure single device installations. The trial version will not expire. If you would like to purchase the advanced software, please contact your ATEN reseller.

5. Click the software version you would like to download, then click **Save**.

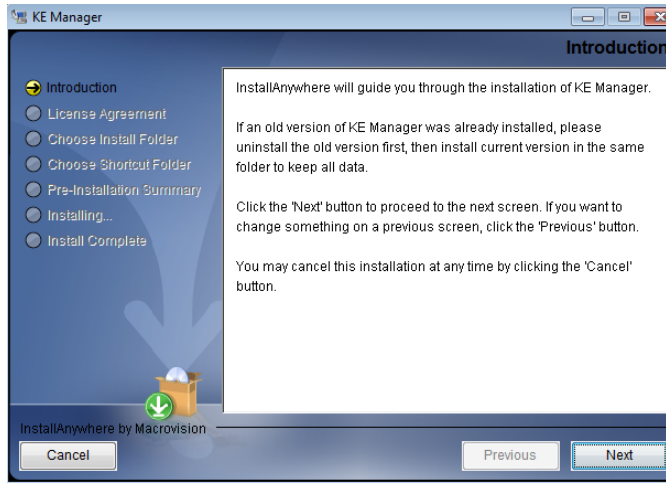
6. Unzip the *Matrix_Manager_Lite.zip* file and double click the *.exe file to start the installation.

7. Follow the instructions on the next page to install the software.

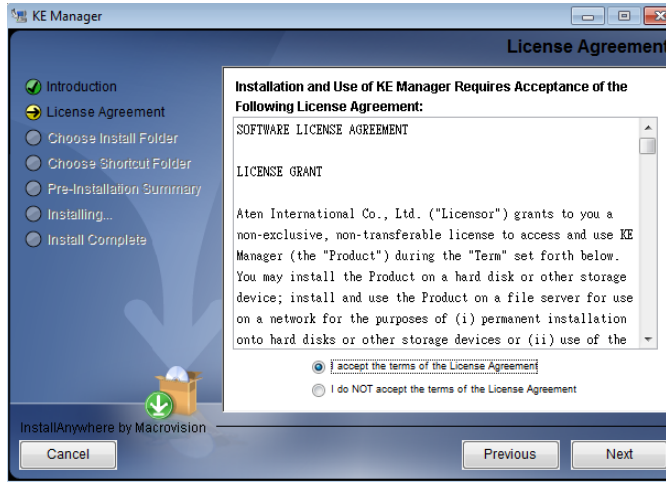
Matrix Manager Install

The following are instructions to install the full version of the Matrix Manager software. For software requirements, see *Software*, page 3.

1. Insert the USB license key into a USB port on your computer.
2. Double click the *MatrixManagerSetup* file to start the setup. When the *Introduction* screen appears, click **Next**.:

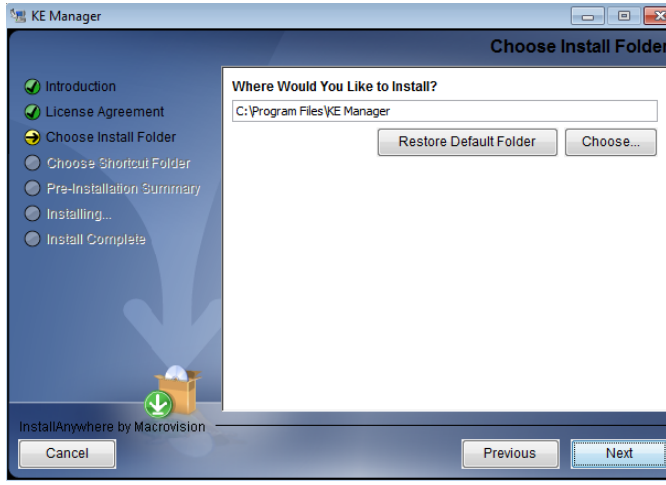


3. The *License Agreement* appears:



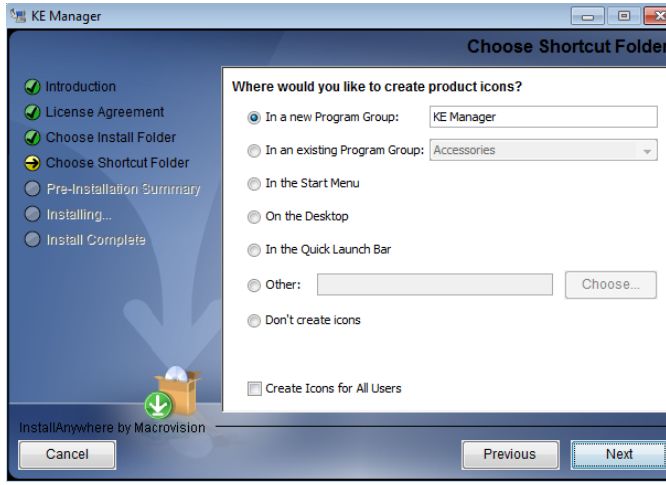
If you agree with the License Agreement, select *I accept the terms of the license agreement*, and click **Next**.

4. The *Choose Install Folder* screen appears:



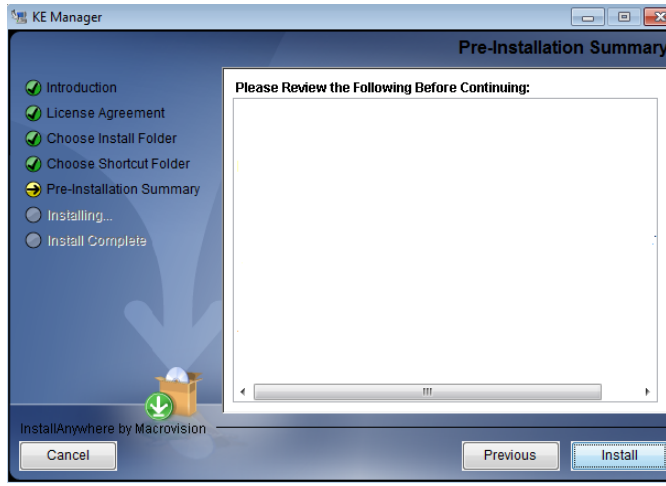
Select where you would like to install the program, and click **Next**.

5. The *Choose Shortcut Folder* screen appears:



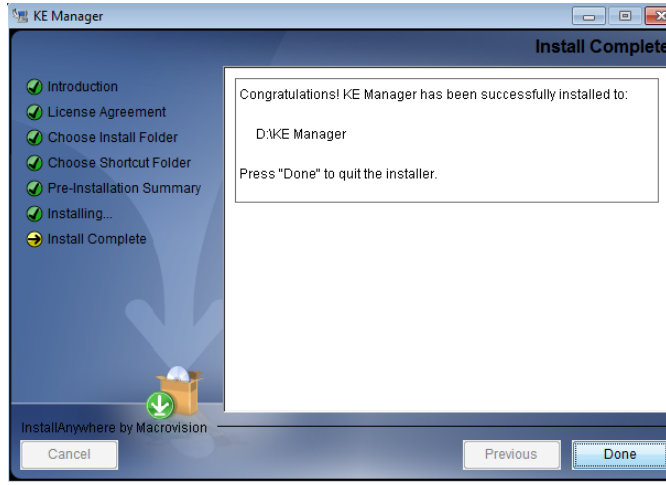
Select where to create shortcuts for the program by selecting the options provided, and click **Next**.

6. The *Pre-Installation Summary* screen appears:



Confirm the settings you've selected. If you want to make a change click **Previous** to go back, or click **Install** to begin the software installation.

7. When the process is done, the *Install Complete* screen appears:



Click **Done**.

Note: If you are installing the Matrix Manager on a second computer for redundancy (see *Redundancy*, page 107) – remove the USB License key and plug it into the primary computer running the Matrix Manager software.

This Page Intentionally Left Blank

Chapter 5
Browser Operation

Overview

The *Matrix Manager* software can be accessed through most standard web browsers. Once users log in and are authenticated, the browser GUI comes up. This chapter explains the login procedure and web browser components.

Logging In

To log into the Matrix Manager, do the following:

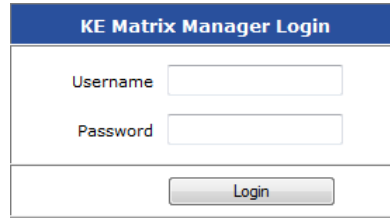
1. Open the browser and specify the IP address of the computer installed with the Matrix Manager software, in the browser's URL location bar.

   Note: If the administrator has configured the HTTP or HTTPS port setting as something other than the default, you must include **http://** or **https://** before the IP address, and specify the port number along with the IP address. For example:

   ```
   https://192.168.1.20:8443
   ```

   Where *8443* is the https port number, and a colon is inserted between it and the IP address.

2. If a Security Alert box appears, accept the certificate – it can be trusted (See *Trusted Certificates*, page 138 for details). The Login page appears:

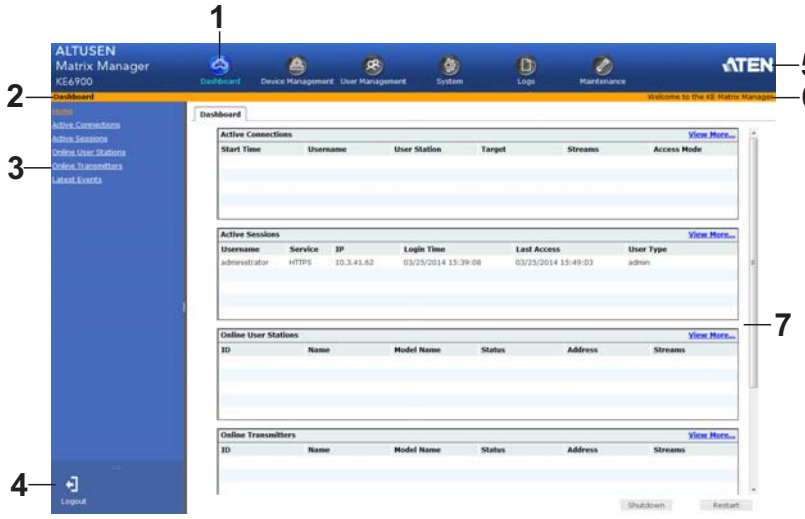


3. Enter the *Username* and *Password*, and click **Login**.

   Note: The administrator account can be used to log in for the first time. Username: *administrator* | Password: *password*. For security purposes, we recommend you change this to something unique.

The Matrix Manager Main Page

After you have successfully logged in, the web browser's main page appears:



Web Components

The web components are described in the table, below:

No.	Item	Description
1	Tab Bar	The tab bar contains the Matrix Manager's main operation categories: Dashboard, Device Management, User Management, System, Logs, and Maintenance.
2	Menu Bar	The menu bar contains operational sub-categories that pertain to the item selected in the tab bar.
3	Sidebar	The Sidebar provides a tree view and listing of items that relate to the various tab bar and menu bar selections. Clicking an item in the Sidebar brings up a page with the details that are relevant to it.
4	Logout	Click this button to log out of your Matrix Manager web session.
5	ATEN Logo	Click this button to open a new browser window that opens on the ATEN website.
6	Welcome Message	If this function is enabled (see *Preferences*, page 123) a welcome message displays here.
7	Interactive Display Panel	This is your main work area. The screens that appear reflect your menu choices and Sidebar item selection.

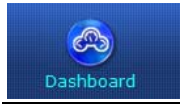
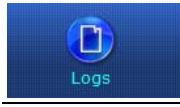
Tree View Considerations

On some pages there will be a sidebar menu with options that can be expanded:

- A plus (+) sign in front of an item means that there are additional items nested inside of it. Click the plus sign to expand the view and show the nested items.
- The plus sign changes to a minus sign (-)when an item is expanded. Click the minus sign to collapse the view and hide the nested items.
- For devices, if the device is on line, its icon is in GREEN; if it is off line, its icon is ORANGE.

The Tab Bar

The functions associated with each of the tabs are explained in the table below:

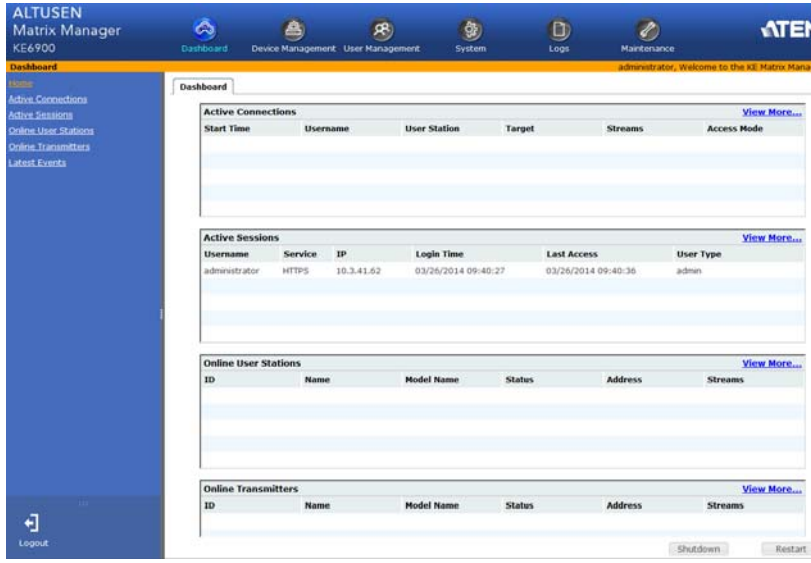
Icon	Function
	**Dashboard:** The Dashboard is used to view information about current connections, sessions, and device events. The first page provides an overview and the sidebar provides a link to view details about each section. The Dashboard is discussed on page 53.
	**Device Management:** The Device Management page is used to configure and control the overall operation of the devices added to the Matrix Manager. Device Management is discussed on page 57.
	**User Management:** The User Management page is used to create and manage Users and Groups. It is also used to assign permissions to them. User Management is discussed on page 115.
	**System:** The System page is used to configure the Matrix Manager's global settings and setup ANMS authorization and authentication. The System page is discussed on page 98.
	**Logs:** The Log page displays the contents of the log file. The Log page is discussed on page 111.
	**Maintenance:** The Maintenance page is used to install firmware; backup and restore configuration information, install certificates, and set preferences. The Maintenance page is discussed on page 115.

Chapter 6
Dashboard

Overview

The *Dashboard* tab is used to view events about connections, sessions, and online devices. The **Home** page provides an overview of the information provided in each section. The Sidebar menu provides a link to each section for a more detailed view of each item.

The Dashboard opens on the *Home* page, as shown here:

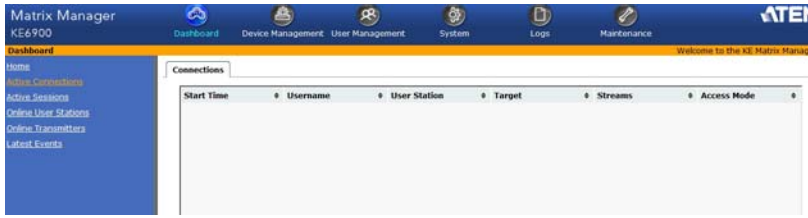


At the bottom of the page, click **Shutdown*** to stop the KeManager service; or **Restart** to stop/restart the service. Both options will logout all user web sessions.

Note: Clicking **Shutdown** stops the KeManager service, and web sessions will not be available until the KeManager service is restarted.

Active Connections

The *Active Connections* page lets an administrator see the active Target connections (User Stations connected to Transmitters) and provides information about each of their sessions.

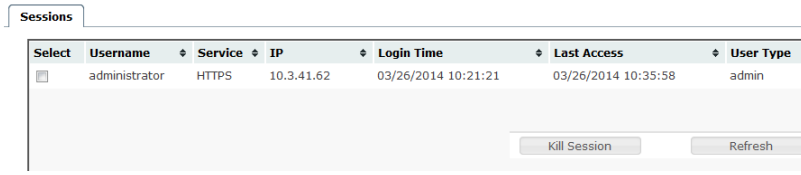


The meanings of the headings at the top of the page are straightforward.

- *Start Time* refers to the date/time the connection between the User Station and Transmitter began.
- *Username* refers to the user that logged into the User Station to establish the connection.
- *User Station* refers to the Receiver that is being used to access the Target connection.
- *Target* refers to the defined Transmitter connections in use by the User Station.
- *Streams* refers to the type of source the connection is streaming: **V**ideo, **A**udio, **U**SB, or **S**erial.
- *Access Mode* refers to the type of access (Exclusive, Occupy, Share, View only) that the User Station is connecting with.

Active Sessions

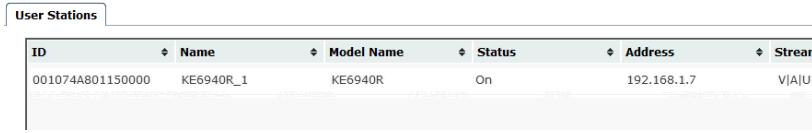
The *Active Sessions* page lets the administrator see all of the users logged into the Matrix Manager and provides information concerning the "who, where and when" of each session.



This page also gives the administrator the option of forcing a user logout by selecting the user and clicking **Kill Session** from the bottom of the page.

Online User Stations

The *Online User Stations* page lets the administrator see all of the Receivers that are currently available on the network and provides information about each device.

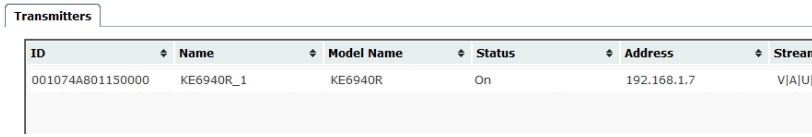


The meanings of the headings at the top of the page are straightforward.

- *ID* refers to the identification number assigned by the system.
- *Name* refers to the name entered on the User Stations's *System* page.
- *Model Name* refers to the Receiver model number.
- *Status* refers to the User Station's online status.
- *Address* refers to the IP address of the User Station.
- *Streams* refers to the source type that the User Station is configured to stream: **V**ideo, **A**udio, **U**SB, and **S**erial.

Online Transmitters

The *Online Transmitters* page lets the administrator see all of the Transmitters that are currently available on the network and provides information about each device.

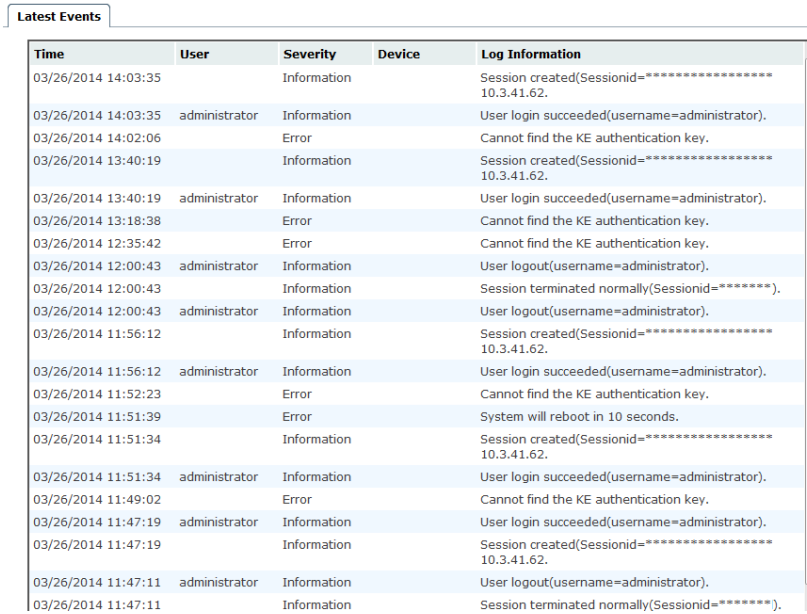


The meanings of the headings at the top of the page are straightforward.

- *ID* refers to the identification number assigned by the system.
- *Name* refers to the name entered on the Transmitter's *System* page.
- *Model Name* refers to the Transmitter model number.
- *Status* refers to the Transmitter's online status.
- *Address* refers to the IP address of the Transmitter.
- *Streams* refers to the source type that the Transmitter is configured to stream: **V**ideo, **A**udio, **U**SB, or **S**erial.

Latest Events

The *Latest Events* page lets the administrator see the most recent Dashboard events that relate to the current connections and sessions, and provides details about each.



Latest Events

Time	User	Severity	Device	Log Information
03/26/2014 14:03:35		Information		Session created(Sessionid=********** 10.3.41.62.
03/26/2014 14:03:35	administrator	Information		User login succeeded(username=administrator).
03/26/2014 14:02:06		Error		Cannot find the KE authentication key.
03/26/2014 13:40:19		Information		Session created(Sessionid=********** 10.3.41.62.
03/26/2014 13:40:19	administrator	Information		User login succeeded(username=administrator).
03/26/2014 13:18:38		Error		Cannot find the KE authentication key.
03/26/2014 12:35:42		Error		Cannot find the KE authentication key.
03/26/2014 12:00:43	administrator	Information		User logout(username=administrator).
03/26/2014 12:00:43		Information		Session terminated normally(Sessionid=*******).
03/26/2014 12:00:43	administrator	Information		User logout(username=administrator).
03/26/2014 11:56:12		Information		Session created(Sessionid=********** 10.3.41.62.
03/26/2014 11:56:12	administrator	Information		User login succeeded(username=administrator).
03/26/2014 11:52:23		Error		Cannot find the KE authentication key.
03/26/2014 11:51:39		Error		System will reboot in 10 seconds.
03/26/2014 11:51:34		Information		Session created(Sessionid=********** 10.3.41.62.
03/26/2014 11:51:34	administrator	Information		User login succeeded(username=administrator).
03/26/2014 11:49:02		Error		Cannot find the KE authentication key.
03/26/2014 11:47:19	administrator	Information		User login succeeded(username=administrator).
03/26/2014 11:47:19		Information		Session created(Sessionid=********** 10.3.41.62.
03/26/2014 11:47:11	administrator	Information		User logout(username=administrator).
03/26/2014 11:47:11		Information		Session terminated normally(Sessionid=*******).

The meanings of the headings at the top of the page are straightforward.

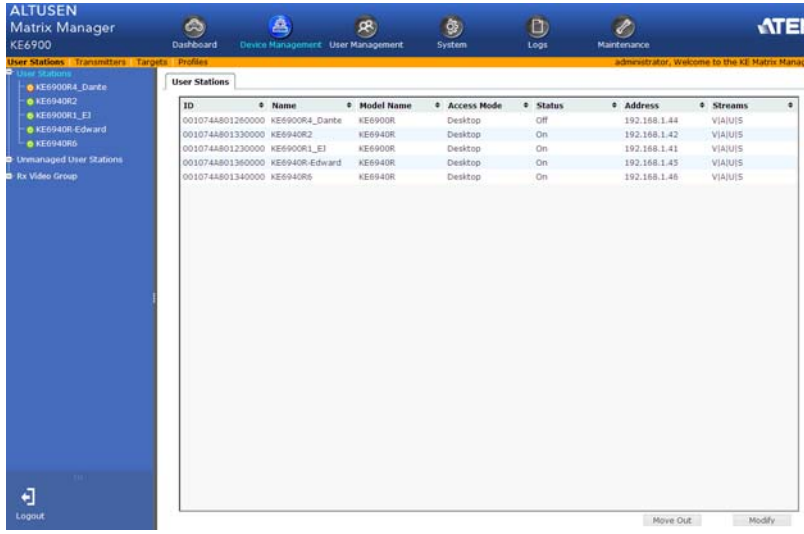
- *Time* refers to the date and time that the event occurred.
- *User* refers to the username that the event relates to. If no username appears, the event is general system information.
- *Severity* refers to the event's severity type: Information, Error, or Warning
- *Device* refers to the Transmitter or User Station that relates to the event. If no device is listed the event refers to the Matrix Manager.
- *Log Information* provides detailed information about each event.

Chapter 7
Device Management

Overview

The *Device Management* tab contains four menu bar items: **User Stations**, **Transmitters**, **Targets**, and **Profiles**. Each page provides a way to add, configure, and managed Transmitters, Receivers, and connections. Before Transmitters and Receivers can be added they must be connected to the network with an IP address.

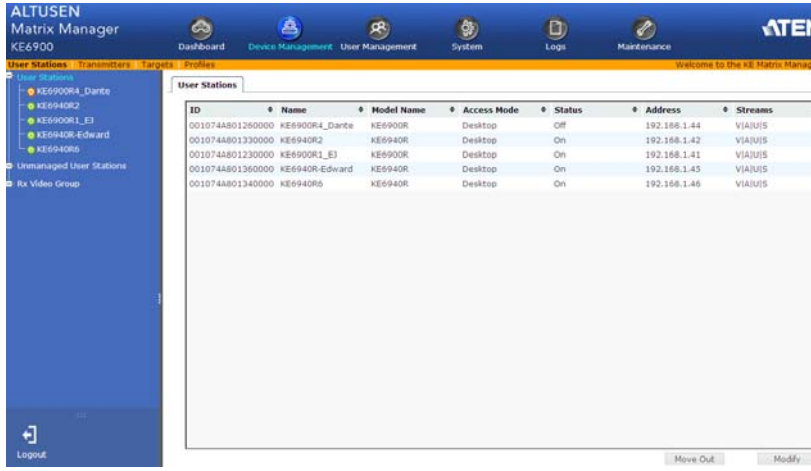
The Device Management tab opens on the *User Stations* page, as shown here:



User Stations

The *User Stations* page allows you to add, configure, and delete Receivers. The Sidebar provides three menu options: **User Stations**, **Unmanaged User Stations**, and **Rx Video Group**. User Stations are Receivers that have been added to the Matrix Manager. Unmanaged User Stations are Receivers on the network that haven't been added to the Matrix Manager. For the Matrix Manager to discover a Receiver, it must be connected to the local network with an IP address. Rx Video Group lists Transmitters that have been grouped to share the video from one computer to multiple User Stations.

Click **User Stations** from the menu bar and the following screen appears:



The main page provides an overview of each *User Station*. The Sidebar provides a link with a more detailed view of each.

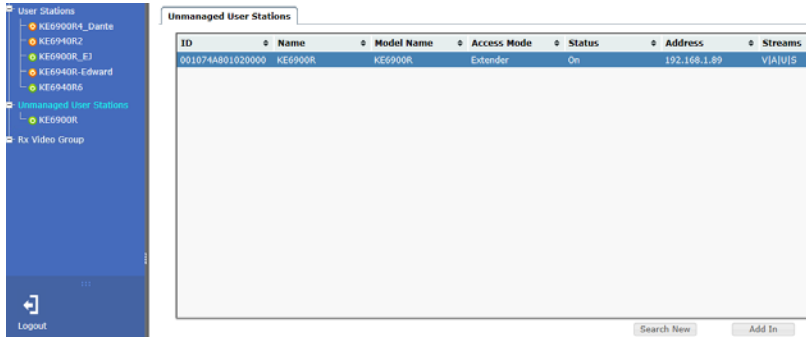
The meanings of the headings at the top of the page are straightforward.

- *ID* refers to the identification number assigned by the system.
- *Name* refers to the name entered on the User Stations's *System* page.
- *Model Name* refers to the Receiver model number.
- *Access Mode* refers to the User Station's mode set in the *Properties*.
- *Status* refers to the User Station's online status.
- *Address* refers to the IP address of the User Station.
- *Streams* refers to the source type that the User Station is configured to stream: **V**ideo, **A**udio, **U**SB, and **S**erial.

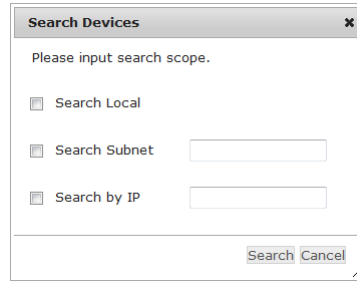
Adding a User Station

To add a User Station, do the following:

1. From *Unmanaged User Stations*, select a User Station and click **Add in**:

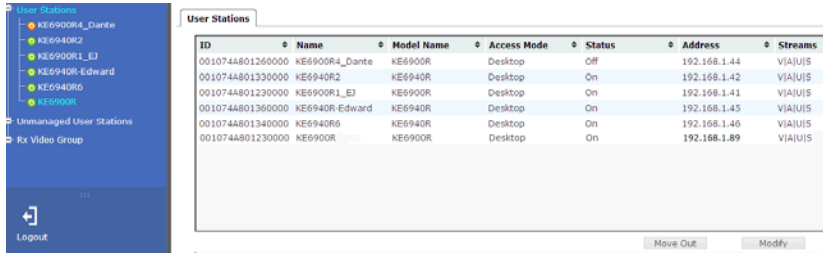


or click **Search New:**



You can search for a device by *Local*, *Subnet*, or *IP* address. Select a scope, enter the information and click **Search**.

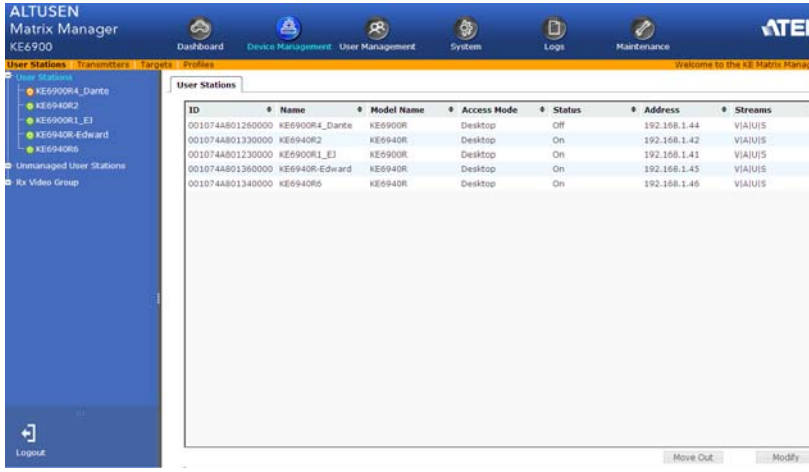
2. Once added, the User Station appears on the *User Stations* main page and in Sidebar menu:



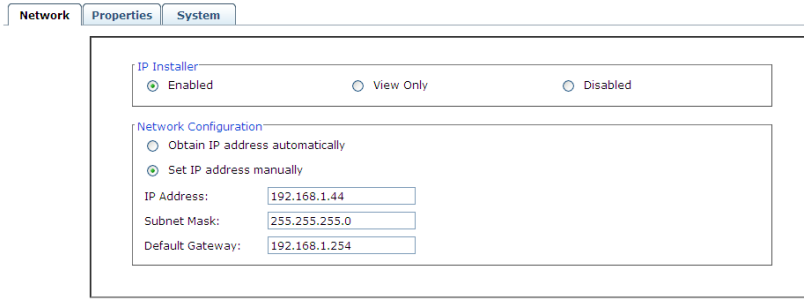
Configuring a User Station

A User Station's settings can be modified from the *User Stations* main page. Changes that are saved are updated on the User Station device across the network. To configure a User Station:

1. Select a User Station and click **Modify**.



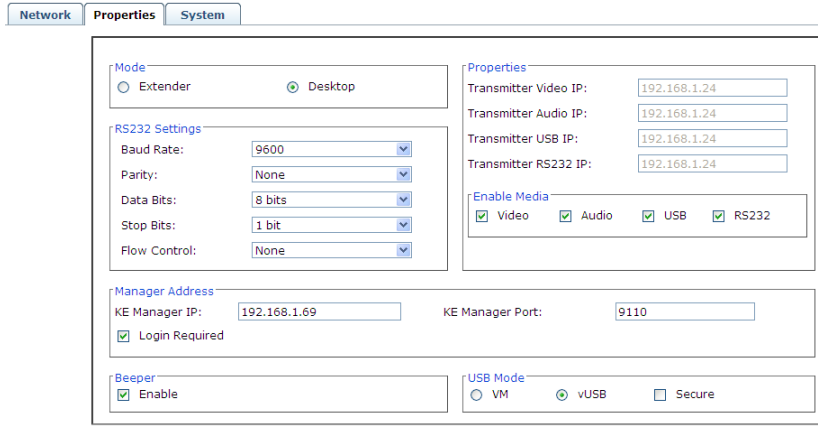
2. The **Network** tab appears with the User Station's IP address settings:



Item	Description
IP Installer	The IP Installer is an external Windows-based utility for assigning IP addresses to the device. Click one of the radio buttons to select **Enable**, **View Only**, or **Disable** for the IP Installer utility. See *IP Installer*, page 137 for details. For security, we strongly recommend that you set this to View Only or Disable after each use.

Item	Description
Network Configuration	For dynamic IP address assignment, select the **Obtain IP address automatically** radio button. To specify a fixed IP Address, Subnet Mask, and Default Gateway select the **Set IP address manually** radio button and fill in the fields with values appropriate for your network. For information to configure the network settings locally on the device see *Network Configuration*, page 23.

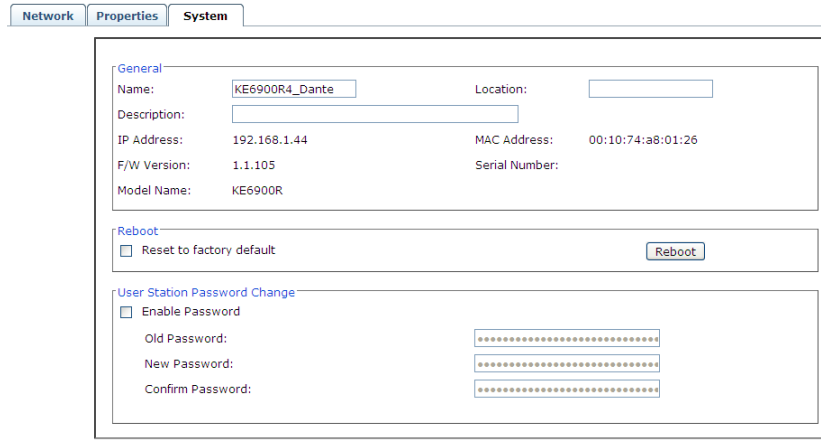
3. Click the **Properties** tab to configure the User Station's properties:



Item	Description
Mode	Select **Extender** mode for simple one-to-one (Transmitter to User Station) setups that are managed with the Receiver's OSD menu. Select **Desktop/Matrix** mode to manage devices and connections from the Matrix Manager. This mode is for advanced administration of Transmitter to User Station connections. (See *Target Connections*, page 74)
Properties	If you selected **Extender** mode (above) set the Transmitter IP address for the User Station's Video, Audio, USB, and RS232 source signals. If you selected **Desktop/Matrix** mode (above) the *Properties* will be grayed out. Use Targets to configure the Transmitter connections. (See *Target Connections*, page 74)

Item	Description
RS-232 Settings	Configure the settings for the serial device the User Station will be connecting to. The default settings are: Baud Rate: 9600 Parity: None Data Bits: 8 bits Stop bits: 1 bit Flow Control: None
Enable Media	Select which source type the User Station can stream : Video, Audio, USB, and RS232.
Manager Address	Set the **IP** address and **Port** number of the computer running the Matrix Manager software. The default port number is 9110.
Login Required	Check this box to require a username and password on the User Station's OSD to access the *Connection Page (see page 38).* **Note:** WARNING! If you uncheck *Login Required* you must select an **Anonymous User** in *Global Settings*. Otherwise a system login error may occur on the User Station's OSD. (See *User Station Login Settings*, page 100)
Beeper	Check this box for the Receiver to beep when configuration changes are made.
USB Mode	Select the type of USB device you will connect to the USB ports: **vUSB**: Use this option to plug USB peripherals into the USB ports. This option also allows a keyboard and mouse with special functions to plug into the USB ports for console use. Use this only if the special functions of the keyboard or mouse are required but do not work when plugged into the console ports. When the keyboard and mouse are plugged into the USB ports, they will not work within the OSD menus. To work within the OSD menus, the keyboard and mouse must be plugged into the console ports. **VM** (Virtual Media): Select this option only if you are plugging a USB disk drive (including USB HDD/optical disk) into the USB ports. This will give you the highest data transfer speeds but will not allow other USB devices to work when plugged into the USB ports. **Secure**: Check this box to encrypt USB disk drives plugged into the USB ports.

4. Click the **System** tab to configure the general settings:



Item	Description
General	Enter the **Name**, **Location**, and **Description** of the User Station. This section also displays the User Station's *IP Address*, *MAC Address*, *F/W Version*, *Serial Number*, and *Model Number*.
Reboot	Check the box and click **Reboot** to reset the User Station's settings back to the factory default. All custom settings will be lost.
User Station Password Change	Check **Enable** to require a password to access the User Station's OSD configuration screens (see page 27). Enter the *Old Password*, enter a *New Password*, and confirm the new password in the *Confirm Password* box.

5. After entering the information, click **Save**.

Deleting a User Station

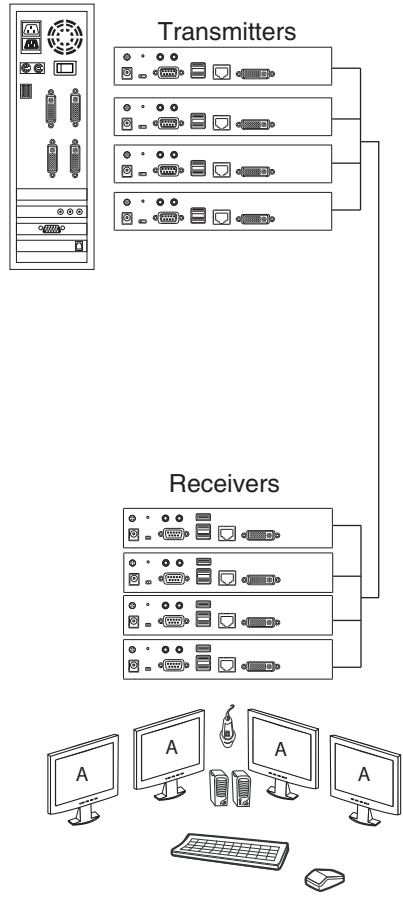
To delete a User Station:

1. Select the User Station you want to delete.
2. Click **Move Out**.

The device list updates with the remaining User Stations. The User Station you deleted will appear on the *Unmanaged User Stations* main page and Sidebar menu.

Rx Video Group

Creating an *Rx Video Group* allows you to cascade up to four Transmitters connected to separate video cards on one computer and share the video with four User Stations – while giving the first User Station keyboard and mouse access. The image below provides an example of the setup without the actual physical connections or possible device connections.



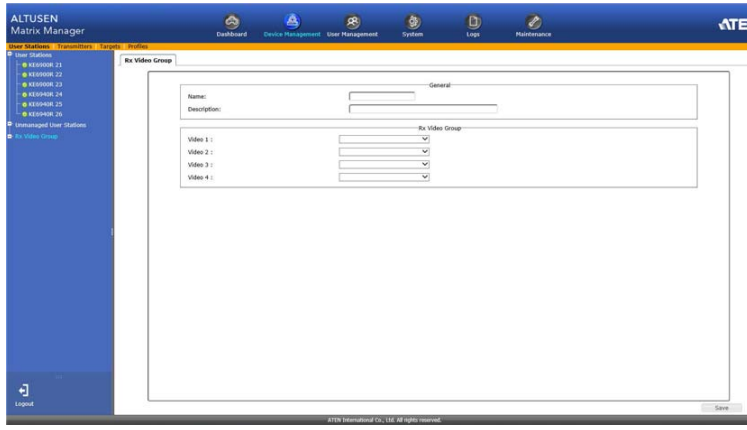
Hardware Setup

1. Connect each Transmitter to the network and to a DVI port on the computer.

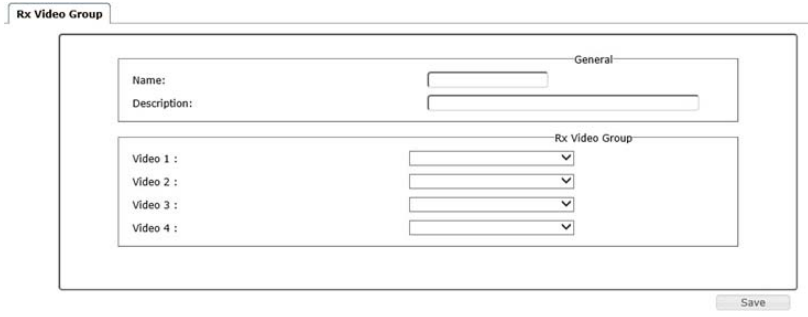
2. Connect one Transmitter's – console & KVM ports to their respective device (keyboard/mouse/computer).
3. Setup the Receivers as you normally would. All Receivers can have a keyboard and mouse but only one (Video 1) can work on the computer for the group.
4. Note the Receiver and Transmitter with keyboard and mouse access (to the computer) so they can be set in the *Rx Video Group* (as **Video 1**) and in the *Target* (as **KVM Transmitter**).

Adding an Rx Video Group

1. Add the User Stations (*Adding a User Station*, page 59) and Transmitters (*Adding a Transmitter*, page 68) to the Matrix Manager.
2. On the left Sidebar select **Rx Video Group**.



3. Provide a **Name** and **Description** for the group.



4. Use the **Video 1** drop-down menu to select the Receiver that will have keyboard and mouse access to the computer.

Note: All Receivers can switch KVM access to other Transmitters but only **Video 1** has keyboard and mouse access to the computer for the group.

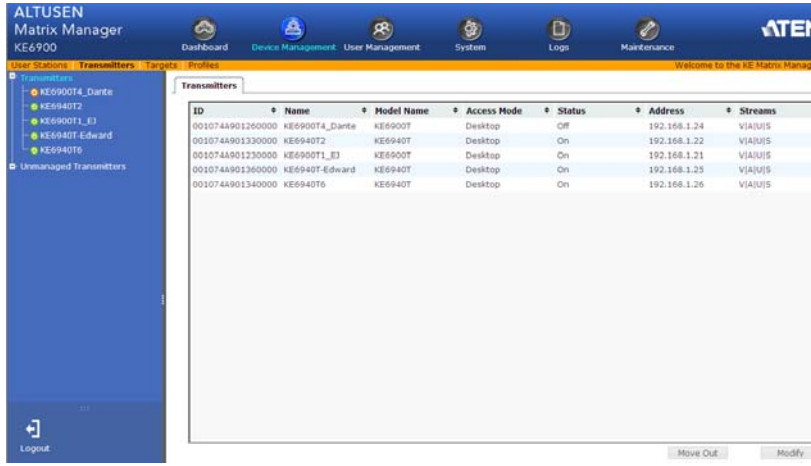
5. Use the **Video 2**, **Video 3** and **Video 4** drop-down menus to select the other Receivers for the group.
6. Click **Save**. The group appears in the Sidebar.
7. On the menu bar, go to **Targets**.
8. Add a new **Target**.

9. Set the **Source Stream** to map the Transmitters to the *Rx Video Group* Receivers, as such: KVM Transmitter → Video 1; Video 2 → Video 2; Video 3 → Video 3; Video 4 → Video 4.
   - Use the **KVM Transmitter** drop-down menu to select the Transmitter connected to the computer's keyboard and mouse ports.
   - Use the **Video 2**, **Video 3** and **Video 4** drop-down menus to select the other Transmitters connected to the computer.
   - Use the **Audio**, **USB** and **Serial** drop-down menus to select the Transmitter for each source signal. The Transmitter selected sends the signal to the Receiver set with the same Video #.
10. Configure the remaining Target settings (see *Adding a Target*, page 76).
11. Click **Save**.

Transmitters

The *Transmitters* page allows you to add, configure, and delete Transmitters. The Sidebar provides two options: **Transmitters** and **Unmanaged Transmitters**. Unmanaged Transmitters are Transmitters on the network that haven't been added to the Matrix Manager. For the Matrix Manager to discover a Transmitter, it must be connected to the local network with an IP address.

Click **Transmitters** from the menu bar and the following screen appears:



The main page provides an overview of each *Transmitter*. The Sidebar provides a link with a more detailed view of each.

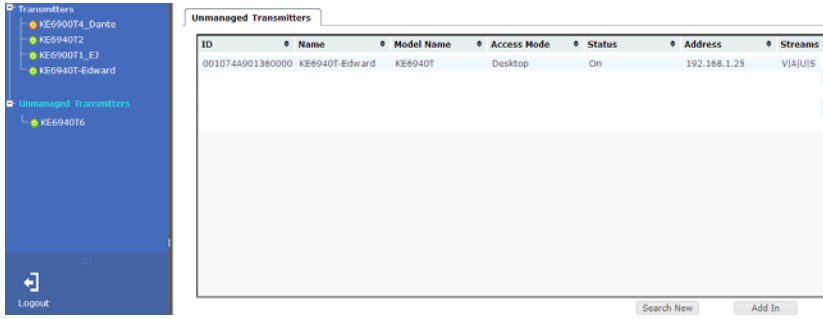
The meanings of the headings at the top of the page are straightforward.

- *ID* refers to the identification number assigned by the system.
- *Name* refers to the name entered on the Transmitter's *System* page.
- *Model Name* refers to the Transmitter's model number.
- *Access Mode* refers to the Transmitter's mode set in the *Properties*.
- *Status* refers to the Transmitter's online status.
- *Address* refers to the IP address of the Transmitter.
- *Streams* refers to the source type that the Transmitter is configured to stream: **V**ideo, **A**udio, **U**SB, or **S**erial.

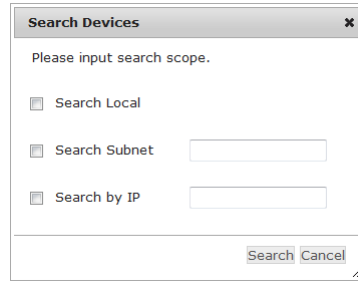
Adding a Transmitter

To add a Transmitter, do the following:

1. From *Unmanaged Transmitters*, select a Transmitter and click **Add in**:

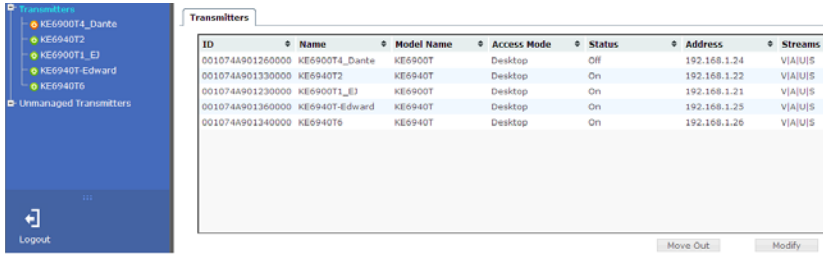


or click **Search New:**



You can search for a device by *Local*, *Subnet*, or *IP* address. Select a scope, enter the information and click **Search**.

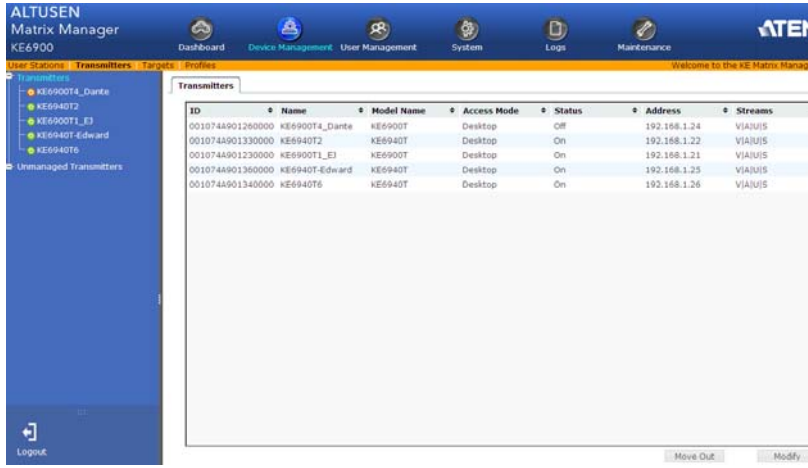
2. Once added, the Transmitter appears on the *Transmitters* main page and Sidebar menu:



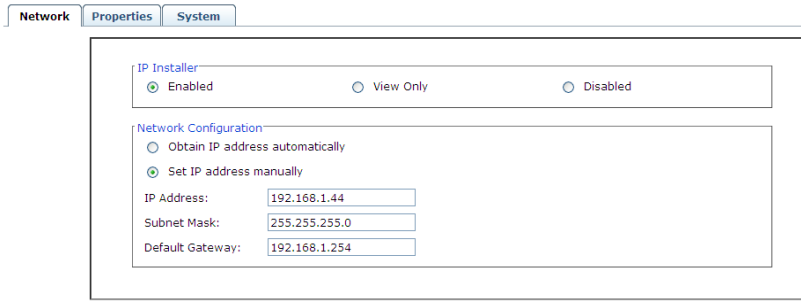
Configuring a Transmitter

A Transmitter's settings can be modified from the *Transmitters* main page. Changes that are saved are updated on the Transmitter device across the network. To configure a Transmitter:

1. Select a Transmitter and click **Modify**.



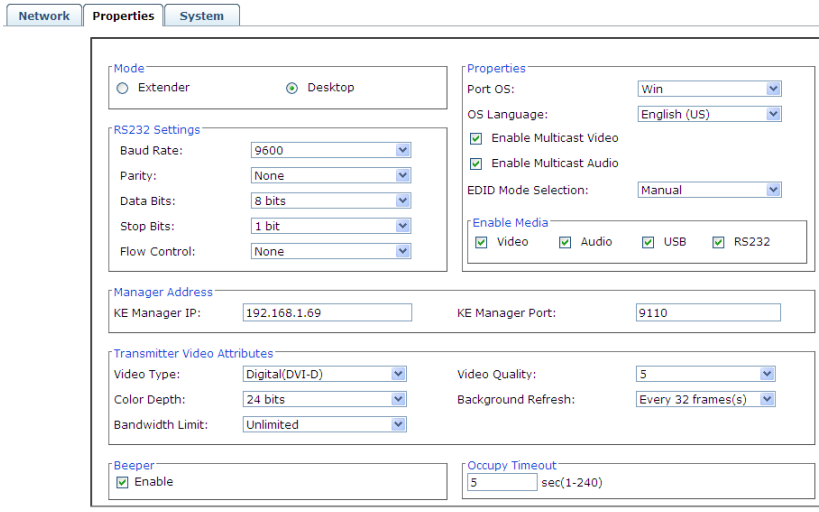
2. The **Network** tab appears with the Transmitter's IP address settings:



Item	Description
IP Installer	The IP Installer is an external Windows-based utility for assigning IP addresses to the device. Click one of the radio buttons to select **Enable**, **View Only**, or **Disable** for the IP Installer utility. (See *IP Installer*, page 137) For security, we strongly recommend that you set this to View Only or Disable after each use.

Item	Description
Network Configuration	For dynamic IP address assignment, select the **Obtain IP address automatically** radio button. To specify a fixed IP Address, Subnet Mask, and Default Gateway, select the **Set IP address manually** radio button and fill in the fields with values appropriate for your network. For information to configure the network settings locally on the device see *Network Configuration*, page 23.

3. Click the **Properties** tab to configure the Transmitter's properties:

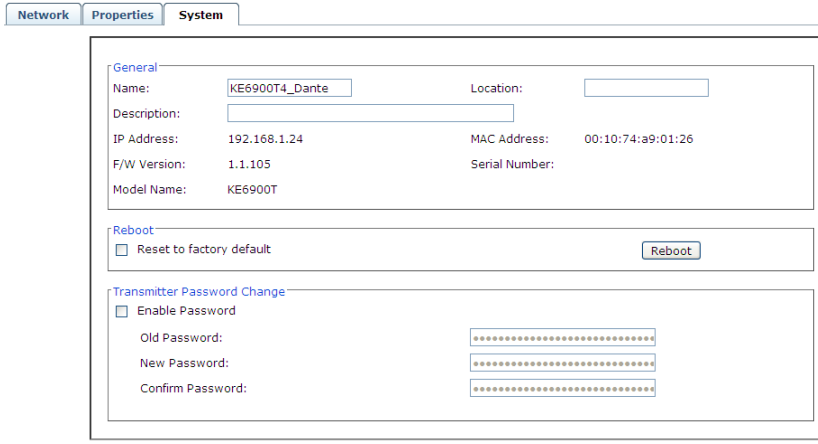


Item	Description
Mode	Select **Extender** mode for simple one-to-one (Transmitter to User Station) setups that are managed with the Receiver's OSD menu. Select **Desktop/Matrix** mode to manage devices and connections from the Matrix Manager. This mode is for advanced administration of Transmitter to User Station connections. (See *Target Connections*, page 74)

Item	Description
Properties	**Port OS:** Use the drop-down menu to select the operating system of the computer connected to the Transmitter. **OS Language:** Use the drop-down menu to select the operating system language of the computer connected to the Transmitter. **Enable Multicast Video:** Check this box to allow a broadcast of the Transmitter's video signal to be sent to multiple User Stations. **Enable Multicast Audio:** Check this box to allow a broadcast of the Transmitter's audio signal to be sent to multiple User Stations. **EDID Mode Selection**: EDID contains a display's basic information and is used by the source device to utilize the best resolution across different monitors. Select how you want the source device to acquire the display's EDID: ◆ **Default**: EDID is set to the default ATEN configuration. ◆ **Auto**: Checks the EDID of all connected displays and uses the best resolution for all displays. ◆ **Manual**: Manually set the EDID configuration from the User Station's OSD (see *Manual EDID*, page 40). ◆ **Remix**: Checks the EDID of all connected displays and the source device uses the best common resolution for all displays.
Enable Media	Select which source type the Transmitter can stream: Video, Audio, USB, and RS232.
RS-232 Settings	Configure the serial device settings for the Transmitter. The default settings are: Baud Rate: 9600 Parity: None Data Bits: 8 bits Stop bits: 1 bit Flow Control: None
Manager Address	Set the **IP** address and **Port** number of the computer running the Matrix Manager software. The default port number is 9110.

Item	Description
Transmitter Video Attributes	These refer to the Transmitter's video settings: **Video Type**: Select the DVI video connector being used by the display: Digital (DVI-D) or Digital (DVI-I). **Color Depth**: Select the number of bits to use for the color depth: 24, 16, or 8. This is the number of bits used to describe the color of a single pixel. A bit depth determines the number of colors that can be displayed at one time. **Bandwidth Limit:** Select the maximum bandwidth that the Transmitter can use to transmit video over the network. A lower bandwidth transmits lower quality video; a higher bandwidth sends higher quality video but this can affect network speed. **Video Quality:** Select the video quality to use. 5 is the highest video quality, and 1 is the lowest video quality. Options are: 1~5. **Background Refresh:** Sets how often the Transmitter refreshes the background image on the connected display. Options are to refresh every 256,128, 64, 32,16, or 0 frames.
Beeper	Check this box for the Transmitter to beep when a configuration change is made.
Occupy Timeout	Set a time threshold for User Stations whose Access Mode has been set to Occupy If there is no activity from the User Station occupying the port for the amount of time set here, the User Station is timed out and the port is released. The first User Station to send keyboard or mouse input after the port has been released gets to occupy the port. Input a value from 1 to 240 seconds.

4. Click the **System** tab configure the general settings:



Item	Description
General	Enter the **Name**, **Location**, and **Description** of the Transmitter. This section also displays the *IP Address*, *MAC Address*, *F/W Version*, *Serial Number*, and *Model Number*.
Reboot	Check the box and click **Reboot** to reset the Transmitter's settings back to the factory default. All custom settings will be lost.
Transmitter Password Change	Check **Enable** to require a password to access to the Transmitter's OSD configuration screens (see page 27). Enter the *Old Password*, enter a *New Password*, and confirm the new password in the *Confirm Password* box.

5. After entering the information, click **Save**.

Deleting a Transmitter

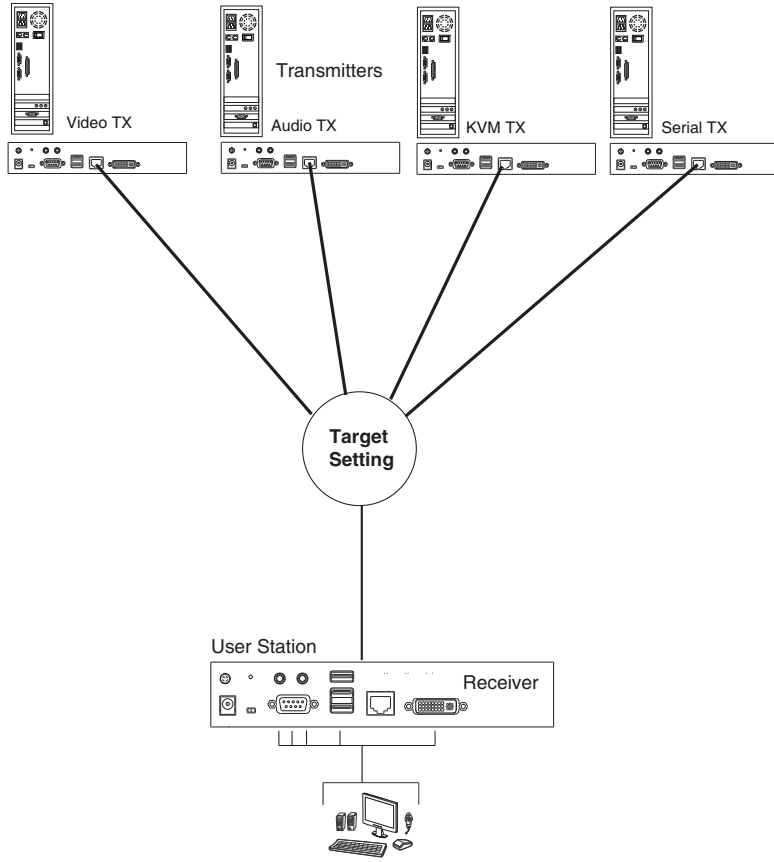
To delete a Transmitter:

1. Select the Transmitter you want to delete.
2. Click **Move Out**.

The device list updates with the remaining Transmitters. The Transmitter you deleted will appear on the *Unmanaged User Stations* main page and Sidebar menu.

Target Connections

With *Target* connections a User Station can connect to multiple Transmitters, individually or simultaneously and stream the **Video**, **Audio**, **USB**, and **Serial** source from different Transmitters. For example: you can create a Target that connects to four Transmitters to access a different source on each computer, as shown below:

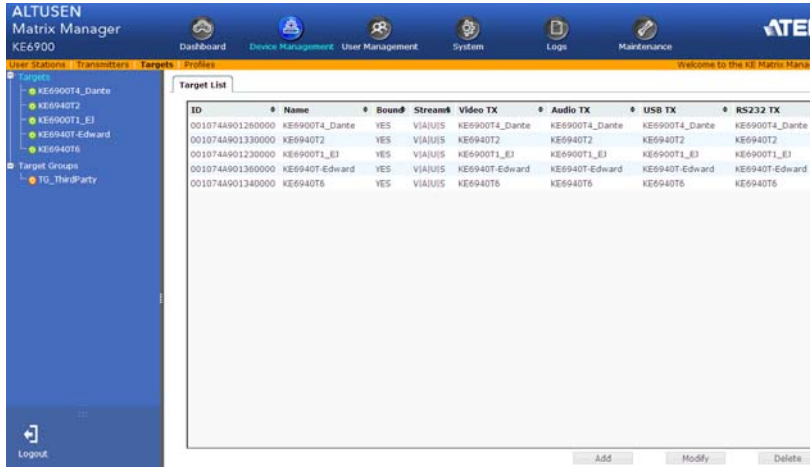


Create Targets to allow User Stations to connect to any Transmitters you have setup- individually or simultaneously. The Target defines the connection to the sources. At the User Stations you can select the Target connections you create. To setup Targets: first create a **Target** that defines the connection, then create a **Profile** to give the *User Station(s)* access to the *Target*. Instructions are provided on the pages that follow.

Targets

A *Target* defines the Transmitter connections for a User Station. This allows a User Station to connect to different Transmitters and stream sources from different Transmitters, depending on how the Target is defined. Once Targets are created you can select them from the User Station's *Connection Page* (see *Connecting*, page 38).

Click **Targets** from the menu bar and the following screen appears:



The main page provides an overview of each *Target*. The Sidebar provides a link with a more detailed view of each.

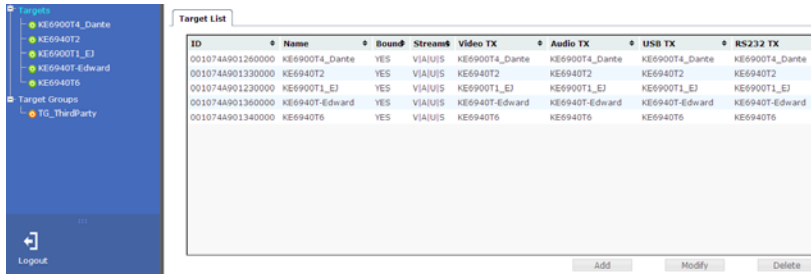
The meanings of the headings at the top of the page are straightforward.

- *ID* refers to the identification number assigned by the system.
- *Name* refers to the name entered on the Target's *Info* page.
- *Bound* states whether the Target's connections are all bound to the same Transmitter.
- *Streams* refers to the source type that the Target is configured to stream: **V**ideo, **A**udio, **U**SB, or **S**erial.
- *Video TX*, *Audio TX*, *USB TX*, *RS232 TX* lists the Transmitter's name for each source stream.
- Click **Modify** to change the selected Target's settings.
- Click **Add** to create a new Target.
- Click **Delete** to remove the selected Target.

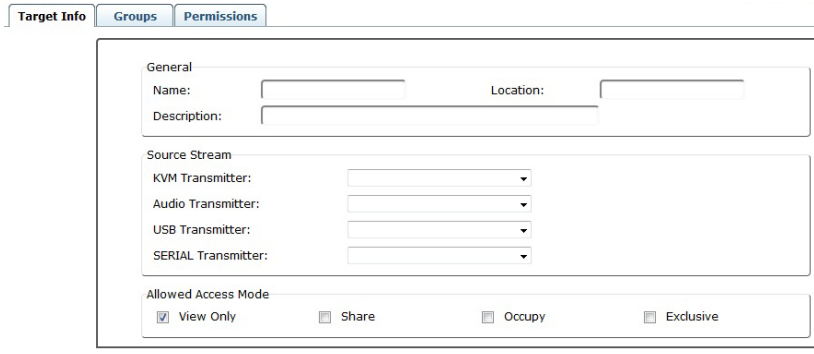
Adding a Target

To add a Target, do the following:

1. From the *Targets* main page, click **Add**:



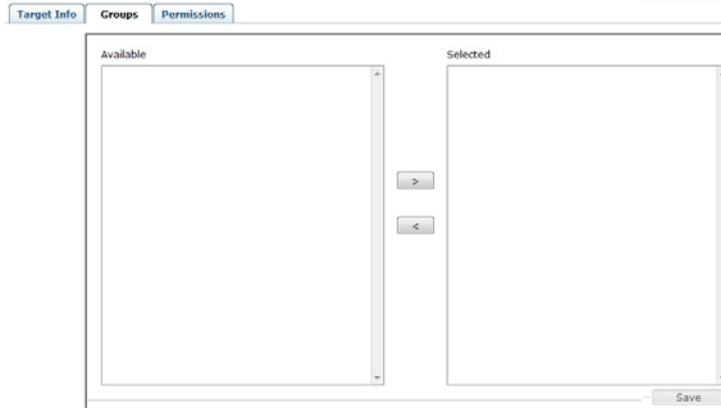
2. The *Target Info* tab appears with the general settings:



Item	Description
General	Enter a **Name**, **Location**, and **Description** for the Target.
Source Stream	Use the drop-down menu to select the Transmitter to use for each of the Target's source stream: KVM (keyboard/video/ mouse), Audio, USB, and Serial.

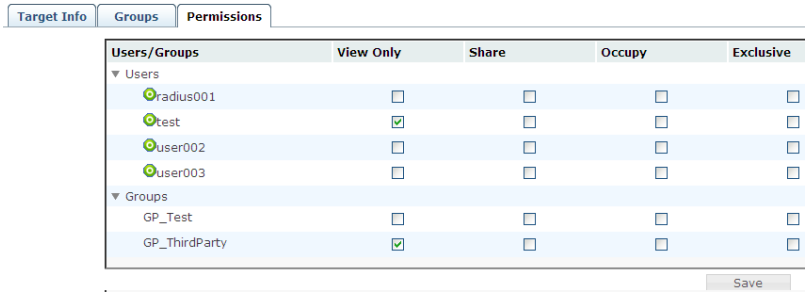
Item	Description
Allowed Access Mode	Check the box for the type of access mode you want to allow on this Target. This defines how the Target can be accessed when multiple users access it. **View Only**: Users only have view access to the Target's video display. **Share**: Users simultaneously share control over the Target. Input from the users is placed in a queue and executed chronologically. **Occupy**: The first user to access the Target has control over the Target. However, additional users may view the Target's video display. If the user who controls the Target is inactive for longer than the time set in the Timeout box (see *Occupy Timeout*, **page 72**), Target control is transferred to the first user to move the mouse or strike the keyboard. **Exclusive**: The first user to access the Target has exclusive control over the Target. No other users can view the Target. The Timeout function does not apply to Targets which have this setting.

3. Click the **Groups** tab to add the Target to Target Groups:



Select a Target Group from the *Selected* column and use the **left arrow** to add the Target to the group. Select a Target Group from the *Available* column and use the **right arrow** to remove the Target from the group. See *Target Groups*, page 79 for details.

4. Click the **Permissions** tab to set the Targets access rights:



Item	Description
Users/Groups	You can assign individual access rights to Users and Groups for the Target by checking the appropriate boxes: **View Only**: Only has view access to the Target's video display. **Share**: Can simultaneously share control over the Target. Input from the users is placed in a queue and executed chronologically. **Occupy**: The first user to access the Target has control over the Target. However, additional users may view the Target's video display. If the user who controls the Target is inactive for longer than the time set in the Timeout box (see *Occupy Timeout*, **page 72**), Target control is transferred to the first user to move the mouse or strike the keyboard. **Exclusive**: The first user to access the Target has exclusive control over the Target. No other users can view the Target. The Timeout function does not apply to Targets which have this setting.

5. After entering the information, click **Save**.

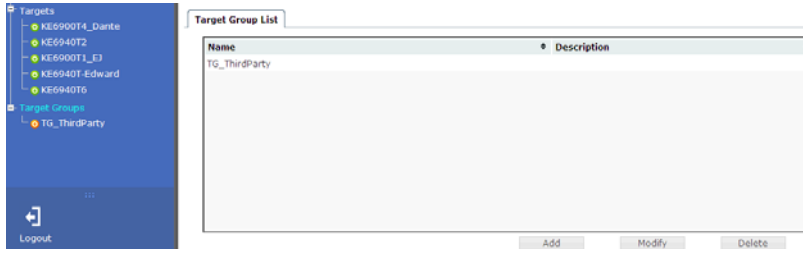
Target Groups

Target Groups allow administrators to easily and efficiently manage users and Targets. Since Target Group access rights apply to any Target that is a member of the group, administrators need only set them once for the group, instead of having to set them for each Target individually. Multiple groups can be defined to allow some users access to specific Targets, while restricting other users from accessing them.

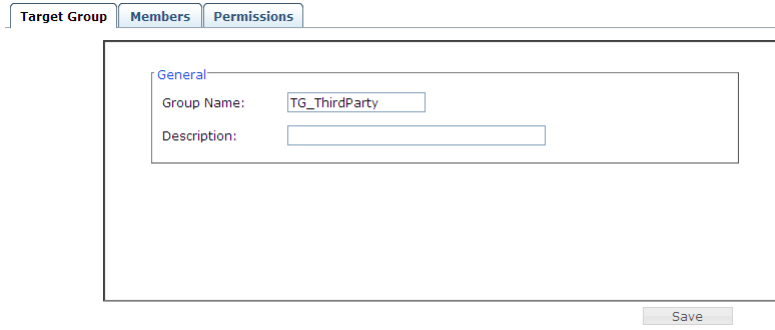
Adding a Target Group

To add a Target Group, do the following:

1. Select *Target Groups* from the Target Sidebar menu, and click **Add**:

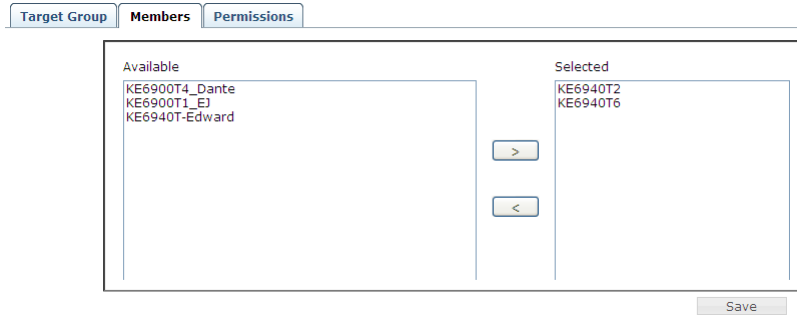


2. The *Target Group* tab appears with the general settings:



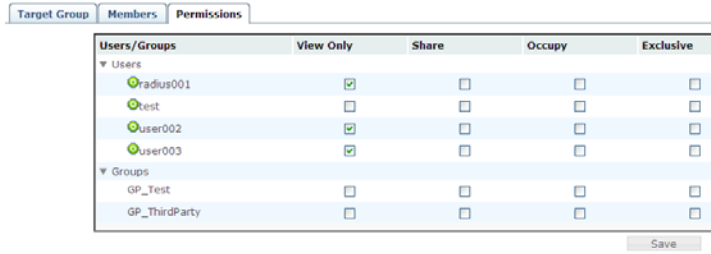
Item	Description
General	Enter a **Name** and **Description** for the Target Group.

3. Click the **Members** tab to add Targets to the group:



Select a Target from the *Selected* column and use the **left arrow** to add it to the group. Select a Target from the *Available* column and use the **right arrow** to remove it from the group.

4. Click the **Permissions** tab to set the group access rights:



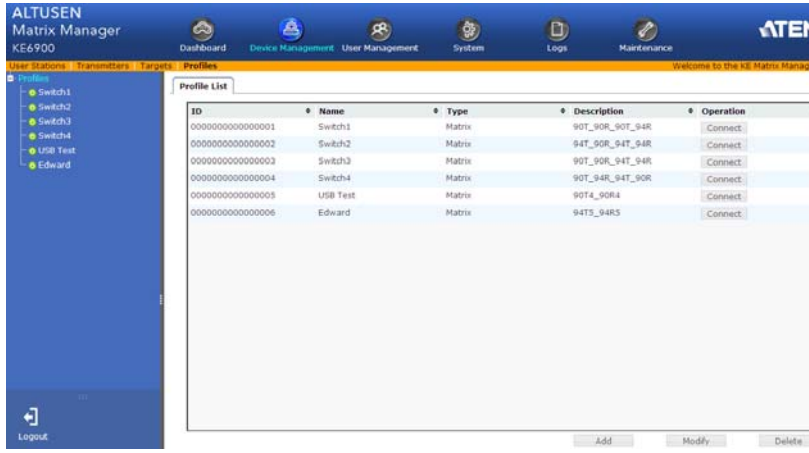
Item	Description
Users/Groups	You can assign the access rights to Users and Groups for the Target Group by checking the appropriate boxes: **View Only**: Has view access to the Target video display. **Share**: Simultaneously share control of the Target. Input from the users is placed in a queue and executed chronologically. **Occupy**: The first user to access the Target has control over the Target. However, additional users may view the Target's video display. If the user who controls the Target is inactive for longer than the time set in the Timeout box (see *Occupy Timeout*, **page 72**), Target control is transferred to the first user to move the mouse or strike the keyboard. **Exclusive**: The first user to access the Target has exclusive control. No other users can view the Target. The Timeout function does not apply to Targets which have this setting.

5. After entering the information, click **Save**.

Profiles

Profiles are created for Targets to allow individual User Station access to the connection. Create a Profile for the Target and assign access for each User Station.

Click **Profiles** from the menu bar and the following screen appears:



The main page provides an overview of each *Profile*. The Sidebar provides a link with a more detailed view of each Profile.

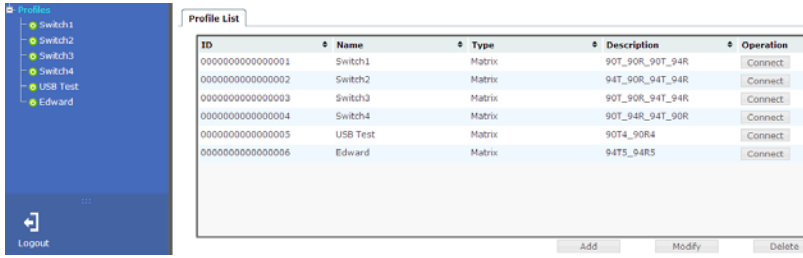
The meanings of the headings on the *Profile List* are straightforward.

- *ID* refers to the identification number assigned by the system.
- *Name* refers to the name entered on the Profile's *Settings* page.
- *Type* refers to the connection type.
- *Description* refers to the description entered on the Profile's *Settings* page.
- *Operation* allows you to click **Connect** to send a Profile's settings to the Transmitters and User Stations.
- Click **Modify** to change the selected Profile's settings.
- Click **Add** to create a new Profile.
- Click **Delete** to remove the selected Profile.

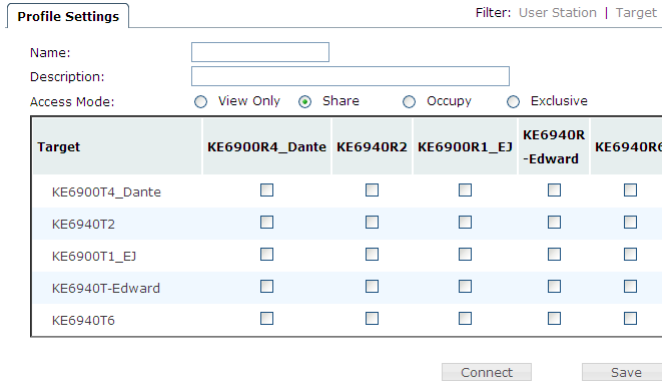
Adding a Profile

To add a Profile, do the following:

1. From the *Profile* main page, click **Add**:



2. The *Profile Settings* tab appears with the Profile and access settings:



Item	Description
Name/ Description	Enter a **Name** and **Description** for the Target.

Item	Description
Access Mode	This defines how the Target in the Profile can be accessed by User Stations when multiple users access it. **View Only**: Users only have view access to the Targets video display. **Share**: Users simultaneously share control over the Target. Input from the users is placed in a queue and executed chronologically. **Occupy**: The first user to access the Target has control over the Target. However, additional users may view the Target's video display. If the user who controls the Target is inactive for longer than the time set in the Timeout box (see *Occupy Timeout*, **page 72**), Target control is transferred to the first user to move the mouse or strike the keyboard. **Exclusive**: The first user to access the Target has exclusive control over the Target. No other users can view the Target. The Timeout function does not apply to Targets which have this setting.
Target	This table lists all the Targets and User Stations available. Checking a box enables the User Station to use the Target connection, listed to the left. The Target will appear on the User Station's Connection Page (See *Connections Page*, page 39), allowing you to connect to it.
Connect	Clicking **Connect** will send the Profile settings to the Transmitters and User Stations and will connect the devices accordingly.

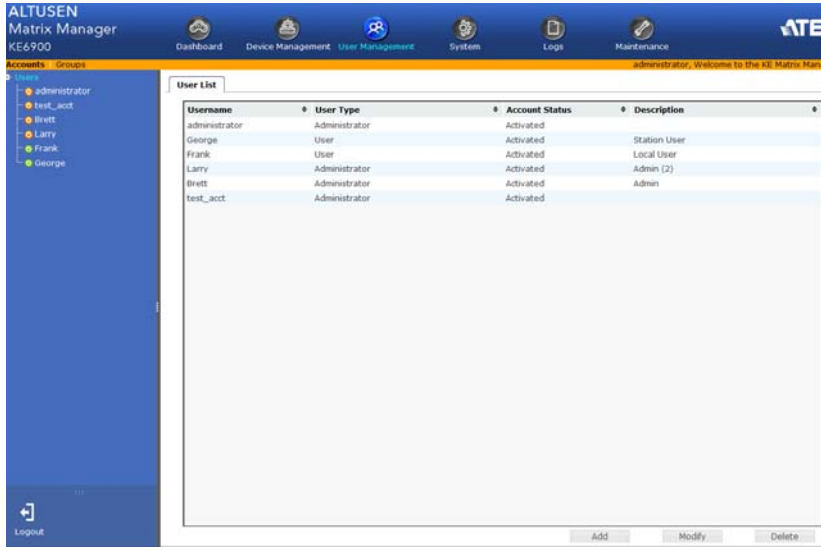
3. After entering the information, click **Save**.

This Page Intentionally Left Blank

Chapter 8
User Management

Overview

User Management has two menu bar items used to create **Accounts** and **Groups**. The User Management tab opens on the *Accounts* page, as shown here:



The page is organized into two main areas: the Sidebar at the left, and the large main panel at the right.

- Users and groups appear in the panel at the left of the page. The large panel at the right provides more detailed information at-a-glance for each.
  - There are menu bar entries for Accounts (Users) and Groups. Depending on the menu item selected, either Users or Groups are listed in the Sidebar.
- The sort order of the information displayed can be changed by clicking the main panel column headings.
- The buttons below the main panel are used to manage users and groups, as shown in the sections that follow.

Users

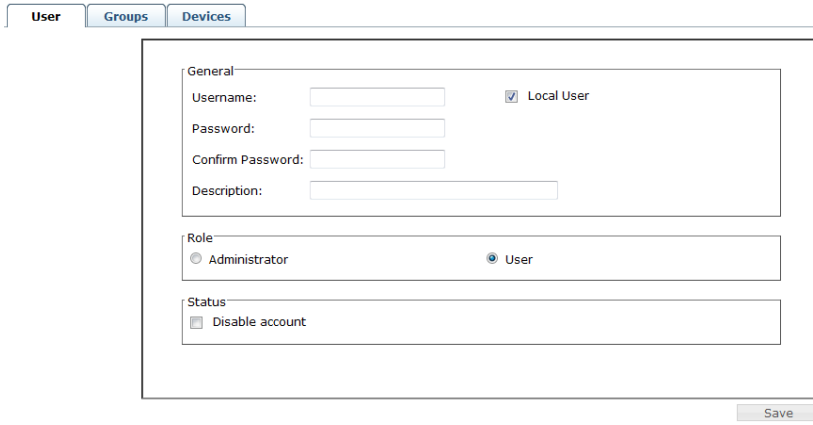
The Matrix Manager supports two types of user accounts, shown in the table bellow:

User Type	Role
Administrator	Access and management of the Matrix Manager, including configuration and setting up of devices. Manage Users and Groups. Configure personal working environments.
User	Access User Stations and connect to Targets they have been given permission for.

Adding Users

To add a user, do the following:

1. Select *Users* in the Sidebar.
2. Click **Add** at the bottom of the main page. The *User* tab opens:



Enter the required information in the fields provided. A description of each is given in the table below:

Field	Description
Username	From 1 to16 characters are allowed depending on the Account Policy settings.
Local User	Check the **Local User** box if the account is for logging in to the Matrix Manager or a User Station (Receiver). Uncheck the Local User box if the account is authenticated with a 3rd party external source, such as RADIUS, LDAP/ AD, or TACACS+. See *ANMS*, page 102 for details.

Field	Description
Password	From 0 to16 characters are allowed depending on the Account Policy settings.
Confirm Password	To be sure there is no mistake in the password, you are asked to enter it again. The two entries must match.
Description	Additional information about the user that you may wish to include.
Role	There are two categories: Administrator and User. ◆ The Administrators have full access to make changes within the Matrix Manager, which includes adding and removing Transmitters and Receivers, user accounts, preferences, and configuration settings. ◆ The Users can log in from User Stations to access Transmitters.
Status	Status allows you to control the user's account and access to the installation, as follows: ◆ *Disable Account* lets you suspend a user's account without actually deleting it, so that it can be easily reinstated in the future.

3. At this point you can assign the new user to a group by selecting the *Groups* tab – the Groups page is discussed on page 91. You can also assign the user's Targets and Groups access rights by selecting the *Devices* tab – the Devices page is discussed on page 95.

Note: Optionally, you can skip this step now to add more users and create groups, and come back to it later.

4. When your selections have been made click **Save**.
5. When the *Operation Succeeded* message appears, click **OK**.
6. Click **Users** in the Sidebar to return to the main screen. The new user appears in the Sidebar list and in the main panel, as well.
   - The Sidebar *Users* list can expand and collapse. If the list is expanded, click the minus symbol (–) next to the *Users* icon to collapse it; if it is collapsed there is a plus symbol (+) next to the icon. Click the plus symbol to expand it.
   - The icon for administrators is orange; the icon for users is green.
   - The large main panel shows the user's name; the description that was given when the account was created; and whether the account is currently active or has been disabled.

Modifying User Accounts

To modify a user account, do the following:

1. In the Sidebar *User* list, click the user's name

   – or –

   In the main panel, select the user's name

2. Click **Modify**.
3. In the *User* page that comes up, make your changes, then click **Save**.

Note: The *User* page is discussed on page 86; the *Groups* page is discussed on page 91, the *Devices* page is discussed on page 95.

Deleting User Accounts

To delete a user account do the following:

1. In the main panel, select the user's name.
2. Click **Delete**.
3. Click **OK**.

Groups

Groups allow administrators to easily and efficiently manage users and devices. Since device access rights apply to anyone who is a member of the group, administrators need only set them once for the group, instead of having to set them for each user individually. Multiple groups can be defined to allow some users access to specific devices, while restricting other users from accessing them.

Creating Groups

To create a group, do the following:

1. Select *Groups* on the menu bar.
2. Click **Add** at the bottom of the main panel. The Group notebook opens, with the *Group* tab selected:

3. Enter the required information in the appropriate fields. A description of each of the fields is given in the table below:

Field	Description
Group Name	A maximum of 16 characters is allowed.
Description	Additional information about the user that you may wish to include. A maximum of 63 characters is allowed.

4. At this point you can assign users to the group by selecting the *Members* tab – the Members page is discussed on page 93. You can also assign the group's Targets and Target Groups access rights by selecting the *Devices* tab – the Devices page is discussed on page 95.
5. When your selections have been made click **Save**.
6. When the *Operation Succeeded* message appears, click **OK**.
7. Click *Group* in the Sidebar to return to the main screen. The new group appears in the Sidebar Group list and in the main panel.

- The Sidebar *Group* list can expand and collapse. If the list is expanded, click the minus symbol (–) next to the *Users* icon to collapse it; if it is collapsed there is a plus symbol (+) next to the icon. Click the plus symbol to expand it.
- The large main panel shows the group's name, and the description that was given when the group was created

Repeat the above procedure to add additional groups.

Note: You must perform Step 7 before attempting to add a new group, or else the new group you are creating will replace the group you just finished creating.

Modifying Groups

To modify a group, do the following:

1. In the Sidebar *Group* list, click the group's name

   – or –

   In the main panel, select the group's name.
2. Click **Modify**.
3. In the *Group* notebook that comes up, make your changes, then click **Save**.

Note: The *Group* page is discussed on page 89; the *Members* page is discussed on page 93, The *Devices* page is discussed on page 95.

Deleting Groups

To delete a group do the following:

1. In the Sidebar, click the *Groups* icon.
2. In the main panel, select the group's name.
3. Click **Delete**.
4. Click **OK**.

Users and Groups

There are two ways to manage users and groups: from the Users notebook; and from the Group notebook.

Note: Before you can assign users to groups, you must first create them. See *Adding Users*, page 86 for details.

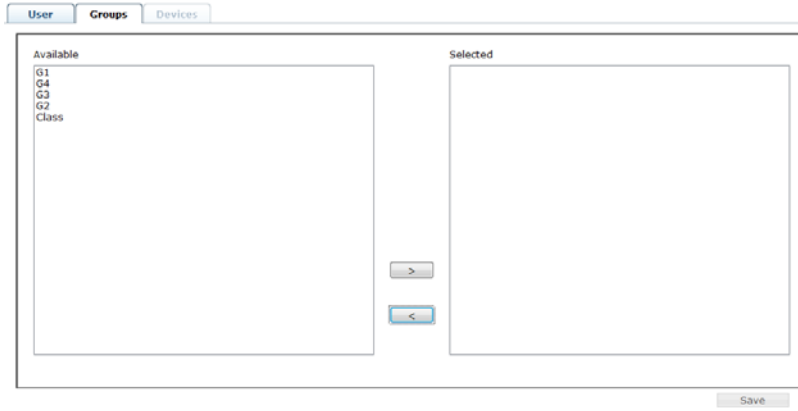
Assigning Users to a Group From the User's Notebook

To assign a user to a group from the User's notebook, do the following:

1. In the Sidebar *User* list, click the user's name

   – or –

   In the main panel, select the user's name
2. Click **Modify**.
3. In the *User* notebook that comes up, select the *Groups* tab. A screen, similar to the one below, appears:



4. In the *Available* column, select the group that you want the user to be in.
5. Click the **Right Arrow** to put the group's name into the *Selected* column.
6. Repeat the above for any other groups that you want the user to be in.
7. Click **Save** when you are done.

Note: If a user has permissions in addition to the ones assigned to the group, the user keeps those permissions in addition to the group ones.

Removing Users From a Group From the User's Notebook

To remove a user from a group from the User's notebook, do the following:

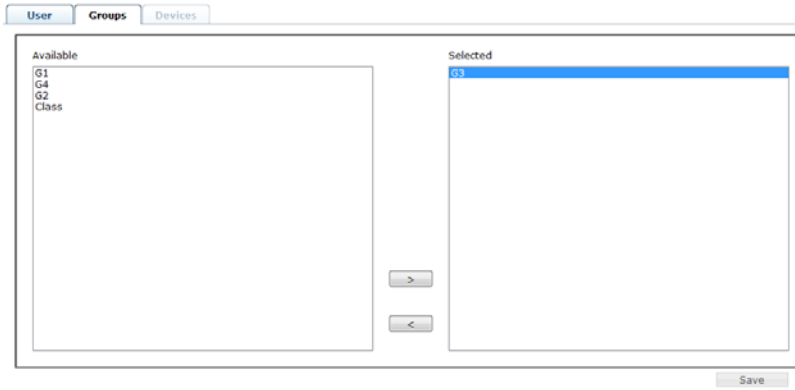
1. In the Sidebar *User* list, click the user's name

   – or –

   In the main panel, select the user's name.

2. Click **Modify**.

3. In the *User* notebook that comes up, select the *Groups* tab. A screen, similar to the one below, appears:



4. In the *Selected* column, select the group that you want to remove the user from.

5. Click the **Left Arrow** to remove the group's name from the *Selected* column. (It goes back into the *Available* column.)

6. Repeat the above for any other groups that you want to remove the user from.

7. Click **Save** when you are done.

Assigning Users to a Group From the Group's Notebook

To assign a user to a group from the Group notebook, do the following:

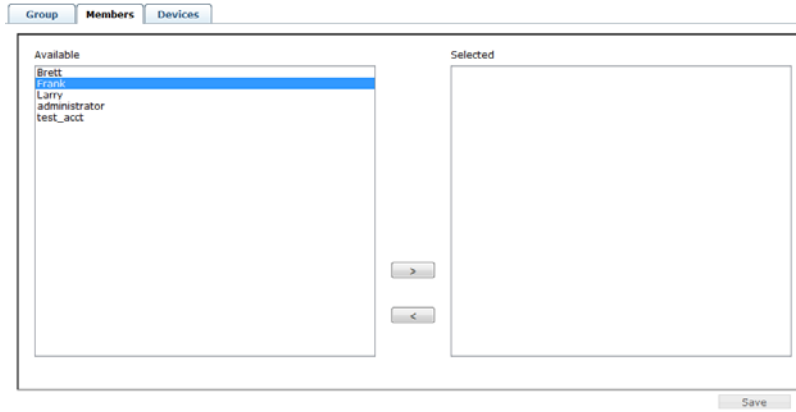
1. In the Sidebar *Group* list, click the group's name

   – or –

   In the main panel, select the group's name.

2. Click **Modify**.

3. In the *Group* notebook that comes up, select the *Members* tab. A screen, similar to the one below, appears:



4. In the *Available* column, select the user that you want to be a member of the group.

5. Click the **Right Arrow** to put the user's name into the *Selected* column.

6. Repeat the above for any other users that you want to be members of the group.

7. Click **Save** when you are done.

Note: If a user has permissions in addition to the ones assigned to the group, the user keeps those permissions in addition to the group ones.

Removing Users From a Group From the Group's Notebook

To remove a user from a group from the Group's notebook, do the following:

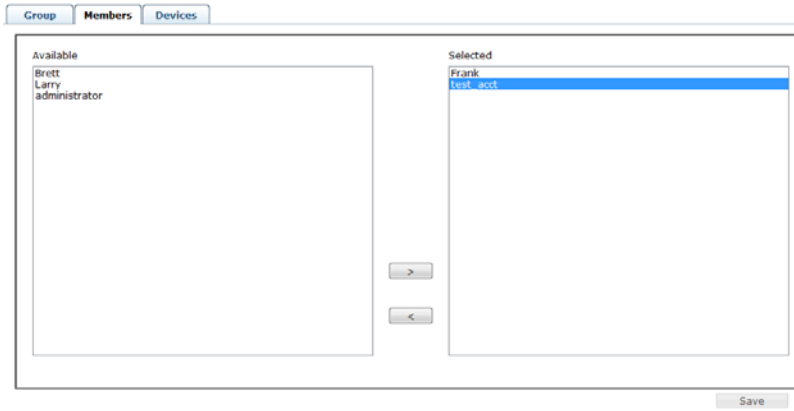
1. In the Sidebar *Group* list, click the group's name

   – or –

   In the main panel, select the group's name.

2. Click **Modify**.

3. In the *Group* notebook that comes up, select the *Members* tab. A screen, similar to the one below, appears:



4. In the *Selected* column, select the user that you want to remove from the group.

5. Click the **Left Arrow** to remove the user's name from the *Selected* column. (It goes back into the *Available* column.)

6. Repeat the above for any other users that you want to remove from the group.

7. Click **Save** when you are done.

Device

You can assign Target and Target Group permissions from the *Devices* tab. For information on Targets and Target Groups See *Targets*, page 75.

Assigning Device Permissions From the User's Notebook

To assign a device permissions to a user from the *User's* notebook, do the following:

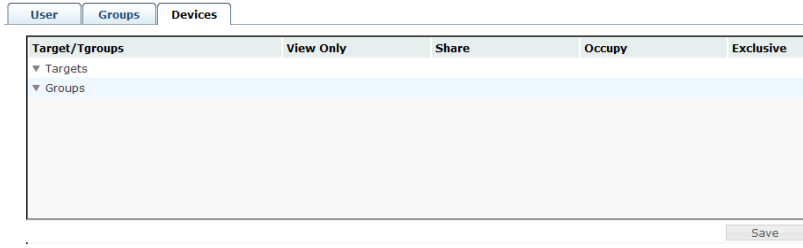
1. In the Sidebar *User* list, click the user's name

   – or –

   In the main panel, select the user's name.

2. Click **Modify**.

3. In the *User* notebook that comes up, select the *Devices* tab. A screen, similar to the one below, appears:



4. Make your permission settings for each device according to the information provided below:

Field	Description
Targets	Lists the Targets which you can assign access rights to for the user. (See *Targets*, page 75 for details)
Groups	Lists the Target Groups which you can assign access rights to for the user. (See *Target Groups*, page 79 for details)

Field	Description
Columns	Check the boxes to apply access rights on the device for the user. This defines how the Target can be accessed when multiple users access it. **View Only**: Users can only view the remote screen, and cannot perform operations on it. **Share**: Users simultaneously share control over the Target. Input from the users is placed in a queue and executed chronologically. **Occupy**: The first user to access the Target has control over the Target. However, additional users may view the Target's video display. If the user who controls the Target is inactive for longer than the time set in the Timeout box, Target control is transferred to the first user to move the mouse or strike the keyboard. **Exclusive**: The first user to access the Target has exclusive control over the Target. No other users can view the Target. The Timeout function does not apply to Targets which have this setting.

5. When you have finished making your choices, click **Save**.
6. In the confirmation popup that appears, click **OK**.

Assigning Device Permissions From the Groups' Notebook

To assign a device permissions to a Group of users, do the following:

1. In the Sidebar *Groups* list, click the group's name

   – or –

   In the main panel, select the group's name.

2. Click **Modify**.

3. In the *Groups* notebook that comes up, select the *Devices* tab.

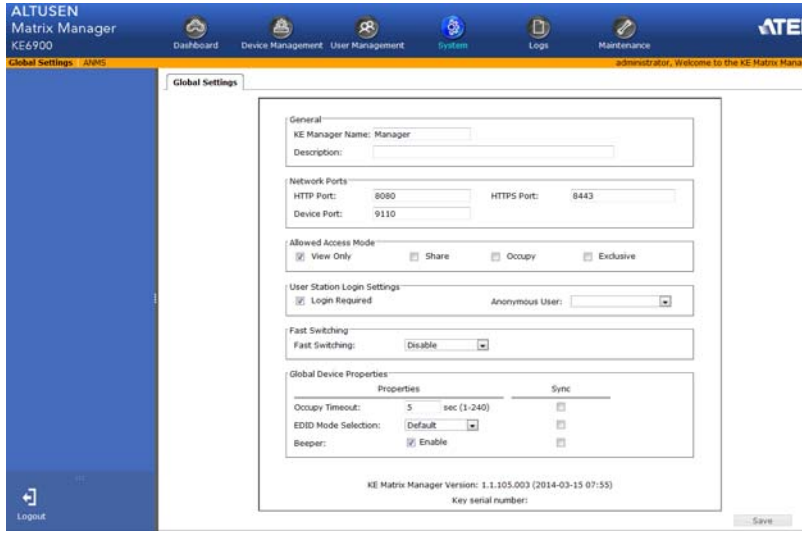
4. The screen that comes up is the same one that appears in the User's notebook. The only difference is that whatever settings you make apply to all members of the group instead of just one individual member.

   Make your device assignments according to the information described under *Assigning Device Permissions From the User's Notebook*, page 95.

Chapter 9
System

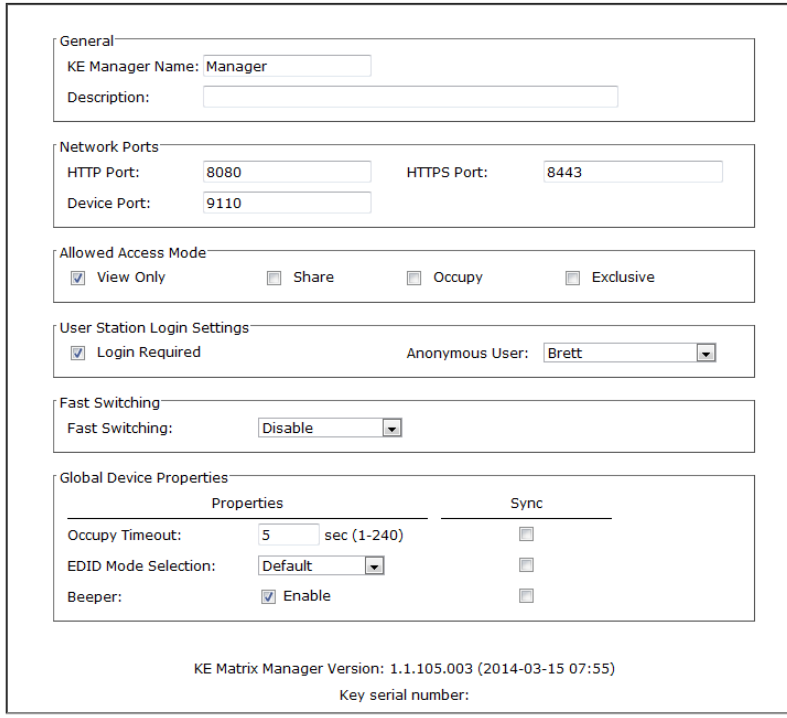
Overview

The *System* tab is used to configure the Matrix Manager's system settings and provides three menu bar items: **Global Settings**, **ANMS** and **Redundancy**. The System tab opens on the *Global Settings* page, as shown here:



Global Settings

The *Global Settings* page lets an administrator change the default settings used for the Matrix Manager:



Item	Description
General	Fill in a **Name** and **Description** for the Matrix Manager.
Network Ports	Use this setting to specify the service ports used to access the Matrix Manager: ◆ **Device Port:** This is the port number to configure on the Transmitter and User Station to access the Matrix Manager (see *Manager Address*, **page 34** and *Manager Address*, **page 30**). The default is 9110. ◆ **HTTP Port**: This is the port number to use for a browser login. The default is 8080. ◆ **HTTPS Port:** This is the port number to use for a secure browser login. The default is 8443. Example: To access the Matrix Manager on a computer with an IP address of 192.168.0.100, using a secure browser login (https), enter: **https://192.168.0.100:8443**

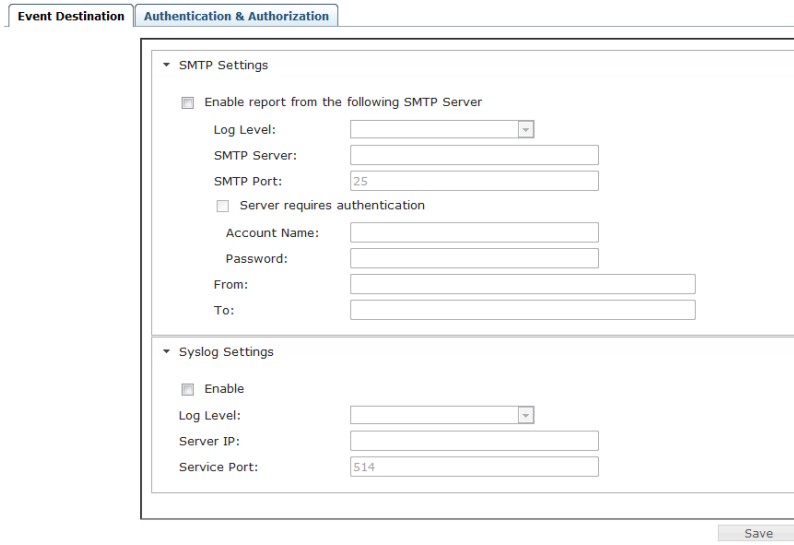
Item	Description
Allowed Access Mode	Select the default Access Mode for devices added to the Matrix Manager. This defines how the device can be accessed when multiple users logon. ◆ **View Only**: Users can access the computer and view the screen, but cannot perform any operations on it. ◆ **Exclusive**: The first user to connect to the Transmitter has exclusive control over the computer. No other users can view the computer. The Timeout function does not apply to devices that have this setting. ◆ **Occupy**: The first user to connect to the Transmitter has control over the computer. However, additional users may view the computers video display. If the user who controls the computer is inactive for longer than the time set in the Timeout box, computer control is transferred to the next user to move the mouse or strike the keyboard. ◆ **Share**: Users simultaneously share control over the computer. Input from the users is placed in a queue and executed chronologically.
User Station Login Settings	This will be the User Station's default setting when they are added to the Matrix Manager. You can change this setting from the User Station's *Properties*. ◆ Check **Login Required** to prompt users for a username and password at the User Station OSD before being able to access the Connections Page (see *Connections Page*, page 39). If you uncheck this, you must set the Anonymous User. ◆ **Anonymous User:** If the *Login Required* box is not checked, select a user from the drop-down menu to use as the default profile to anonymously login to the User Station, in the background. **Note:** WARNING! If Login Required isn't checked and an Anonymous User isn't selected, a system login error will occur at the User Station OSD.
Fast Switching	Allows you to select the default resolution to use that gives you the ability to switch faster between User Station and Transmitter connections.

Item	Description
Global Device Properties	These settings allow you to set the default properties used by all devices: ◆ **Occupy Timeout**: Set the number of seconds for a user's session to be inactive before the access is released for use by another user, when using the Occupy Access Mode. This will be the default setting for Transmitters. ◆ **EDID Mode Selection:** Extended Display Identification Data (EDID) contains a display's basic information and is used by the source device to utilize the best resolution across different monitors. This will be the default setting for Transmitters. Select how you want the source device to acquire the display's EDID: ◆ **Default**: EDID is set to the ATEN default configuration. ◆ **Auto**: Checks the EDID of all connected displays and uses the best resolution for all displays. ◆ **Manual**: Manually set the EDID configuration from the User Station's OSD (see *Manual EDID*, page 40). ◆ **Remix**: Checks the EDID of all connected displays and the source device uses the best common resolution for all displays. ◆ **Beeper**: Check this box for the device to alert you with a sound when its first being accessed or when a configuration change is made. Use the **Sync** check box for each option above to push the setting change to the devices after you click **Save**.

ANMS

The *ANMS* (Advanced Network Management Settings) page is used to set up login authentication and authorization management from external sources. It is organized as a notebook with two tabs – each with a series of related panels, as described below.

Event Destination



- *SMTP Settings*

  To have the Matrix Manager email reports from the SMTP server to you, do the following:

  1. Enable the *Enable report from the following SMTP Server*, select the the *Log Level* (Information, Warning, or Error), and key in the *SMTP Server* IP address and *SMTP Port*.
  2. If your server requires authentication, check the *Server requires authentication* checkbox, and key in the appropriate information for the *Account Name* and *Password* fields.
  3. Key in the email address of where the report is being sent from in the *From* field.

Note:
1. Only one email address is allowed in the *From* field, and it cannot exceed 64 Bytes.
2. 1 Byte = 1 English alphanumeric character.

4. Key in the email address (addresses) of where you want the SMTP reports sent to in the *To* field.

   Note: If you are sending the report to more than one email address, separate the addresses with a semicolon. The total cannot exceed 256 Bytes.

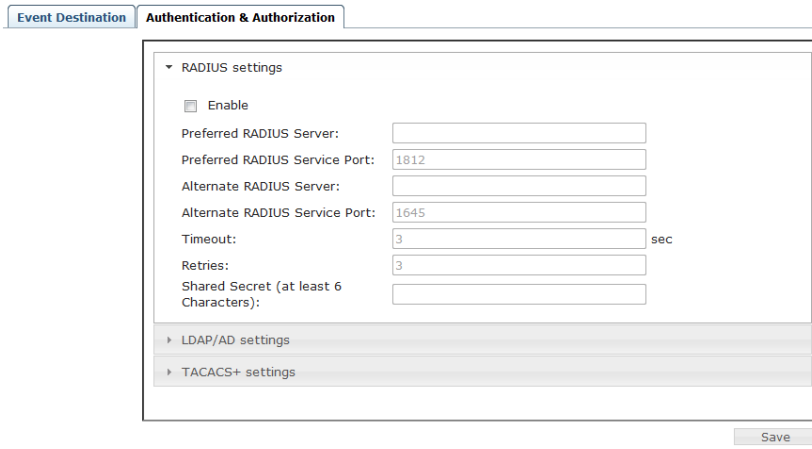
5. Click **Save**.

- *Syslog Settings*

  To record all the events that take place on the Matrix Manager and write them to a Syslog server, do the following:

  1. Check **Enable**.
  2. Use the drop-down menu to select the *Log Level* (Information, Warning, or Error).
  3. Key in the *Server IP* address of the Syslog server.
  4. Key in the *Service Port* number. The valid port range is 1-65535.
  5. Click **Save**.

Authentication & Authorization



- *RADIUS Settings*

  To allow authentication and authorization for the KE6900 / KE6940 through a RADIUS server, do the following:

  1. Check **Enable**.
  2. Fill in the IP addresses and service port of the *Preferred RADIUS Server* and *Alternate RADIUS Server.*
  3. In the *Timeout* field, set the time in seconds that the Matrix Manager waits for a RADIUS server reply before it times out.
  4. In the *Retries* field, set the number of allowed retries.
  5. In the *Shared Secret* field, key in the character string that you want to use for authentication between the Matrix Manager and the RADIUS Server. A minimum of 6 characters is required.
  6. On the RADIUS server, Users can be authenticated with any of the following methods:
     - Set the entry for the user as **su/xxxx**

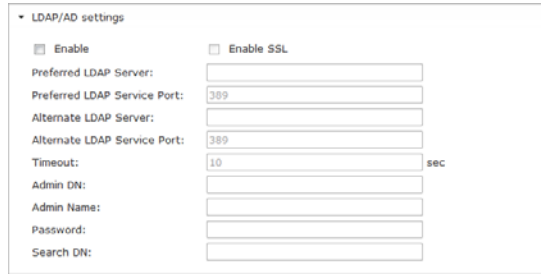
       Where *xxxx* represents the Username given to the user when the account was created on the Matrix Manager.

     - Use the same Username on both the RADIUS server and the Matrix Manager.
     - Use the same Group name on both the RADIUS server and the Matrix Manager.

- Use the same Username/Group name on both the RADIUS server and the Matrix Manager.

In each case, the user's access rights are the ones assigned that were assigned when the User of Group was created on the Matrix Manager.

- *LDAP / AD Authentication and Authorization Settings*:



To allow authentication and authorization for the Matrix Manager via LDAP / AD, refer to the information in the table, below:

Item	Action
Enable	Put a check in the Enable checkbox to allow LDAP / AD authentication and authorization.
Enable SSL	Put a check in the Enable checkbox to allow SSL connections.
LDAP Server IP and Port	Fill in the IP address and port number for the LDAP / AD server. ◆ You can use the IPv4 address, the IPv6 address or the domain name in the LDAP Server field. ◆ For LDAP, the default port number is 389.
Timeout	Set the time in seconds that the Matrix Manager waits for an LDAP / AD server reply before it times out.
Admin DN	Consult the LDAP / AD administrator to ascertain the appropriate entry for this field. For example, the entry might look like this: ou=kn4132,dc=aten,dc=com
Admin Name	Key in the LDAP administrator's username.
Password	Key in the LDAP administrator's password.
Search DN	Set the distinguished name of the search base. This is the domain name where the search starts for user names.

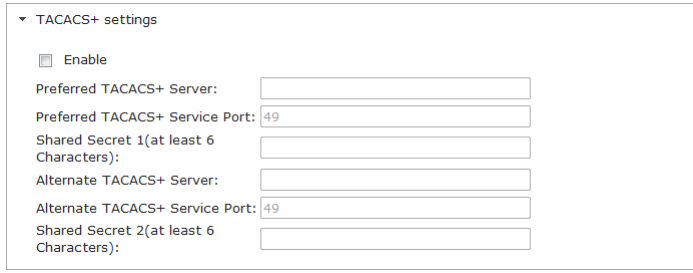
On the LDAP / AD server, Users can be authenticated with any of the following methods:

- With MS Active Directory schema.

Note: If this method is used, the LDAP schema for MS Active Directory must be extended. Without schema – Only the Usernames used on the Matrix Manager are matched to the names on the LDAP / AD server. User privileges are the same as the ones configured on the Serial Console Server.

- Without schema – Only the Usernames used on the Matrix Manager are matched to the names on the LDAP server. User privileges are the same as the ones configured on the switch.
- Without schema – Only Groups in AD are matched. User privileges are the ones configured for the groups he belongs to on the switch.
- Without schema – Usernames and Groups in AD are matched. User privileges are the ones configured for the User and the Groups on the switch.

- *TACACS+ Settings:*



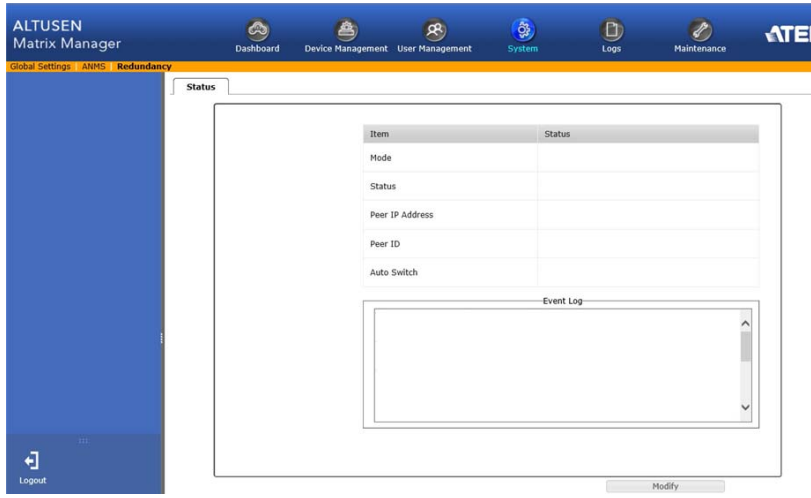
  - **Enable** TACACS+ and enter the following information:
    - Preferred TACACS+ Server
    - Preferred TACACS+ Service Port
    - Shared Secret 1
    - Alternate TACACS+ Server
    - Alternate TACACS+ Service Port
    - Shared Secret 2

Redundancy

The *Redundancy* page sets up a second computer as backup in case the computer hosting the Matrix Manager goes off-line. If the Matrix Manager is off-line, the secondary computer will automatically take over operations, allowing all connections to continue without disruption – with only a brief period (30 seconds) when new connections can't be started. When the primary computer comes back online it retrieves the database with any changes from the secondary computer and re-takes all Matrix Manager operations.

To setup Redundancy, do the following:

1. Install the Matrix Manager on a second computer with the USB License key (see page 43).
2. Open the Matrix Manager and go to the *System* → *Redundancy* page.

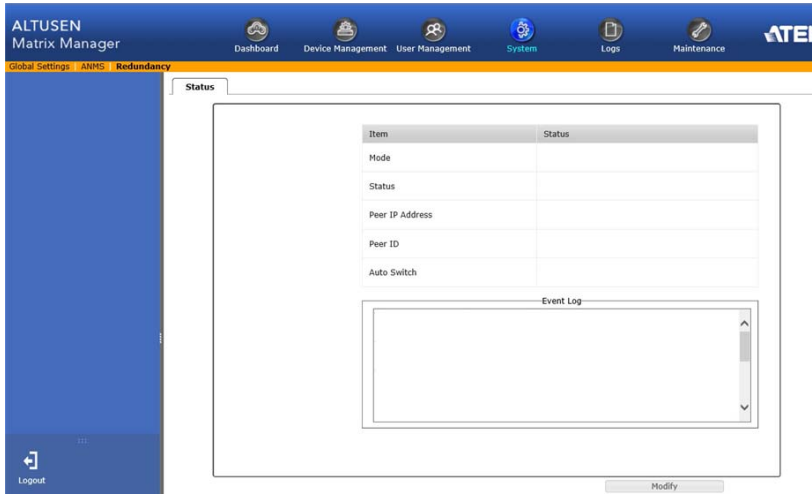


3. Click **Modify**. The *Status* window appears:

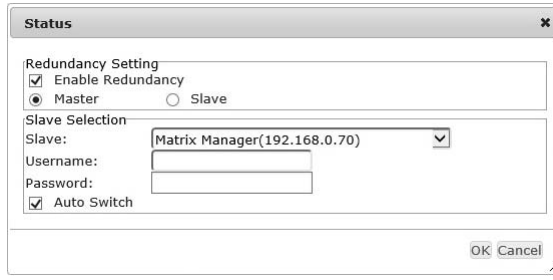
4. Check the **Enable Redundancy** box and select the **Slave** radio button.

5. Use the **Master** drop-down menu to select the primary computer's IP address.
6. Click **OK**.
7. This computer is now running in **Standby** mode, as identified in the orange status bar:

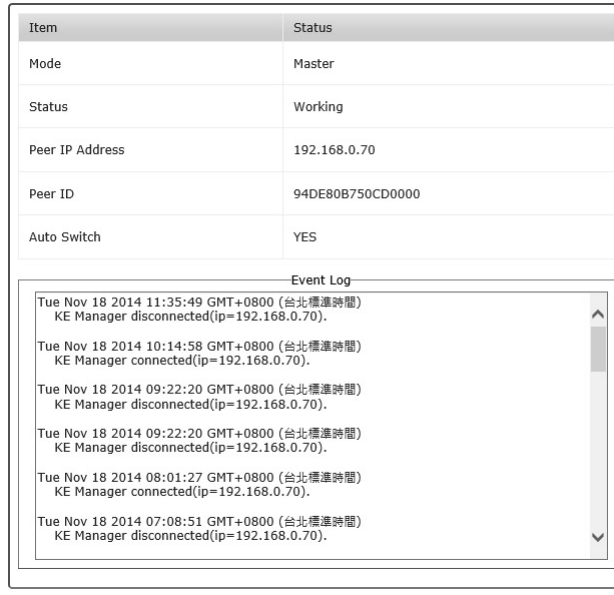
8. Remove the USB License key and plug it into the primary computer running the Matrix Manager software.
9. Open the Matrix Manager on the primary computer and go to the *System* → *Redundancy* page.



10. Click **Modify**. The *Status* window appears:



11. Check the **Enable Redundancy** box and select the **Master** radio button.
12. Use the **Slave** drop-down menu to select the secondary computer's IP address.
13. Enter the **Username** and **Password** of the secondary computer's local administrator account.
14. Check the **Auto Switch** box to automatically switch the Matrix Manager to the secondary computer when the primary computer is offline – and reverse the action when the primary computer is back online.
15. Click **OK**.
16. The **Redundancy** page provides information about the configuration.



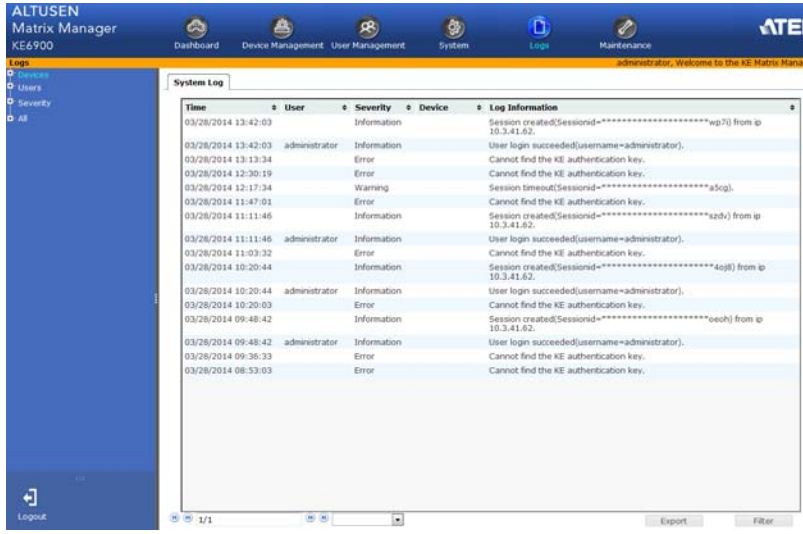
Item	Action
Mode	Displays the role of the computer running the Matrix Manager software: Master (primary) or Slave (secondary).
Status	Displays **Working** for the computer currently managing the Matrix Manager database. Displays **Standby** when the computer is waiting as a backup and getting database updates from the primary computer running the Matrix Manager.
Peer IP Address	Displays the IP address of the computer configured to send (primary) or receive (secondary) the database updates for redundancy.

Item	Action
Peer ID	Displays the MAC address of the computer configured to send (primary) or receive (secondary) the database updates for redundancy.
Auto Switch	Displays the Auto Switch (Yes/No) status. (Master only).
Event Log	Displays the logs that provide information about the Matrix Manager's redundancy status.

Chapter 10
Logs

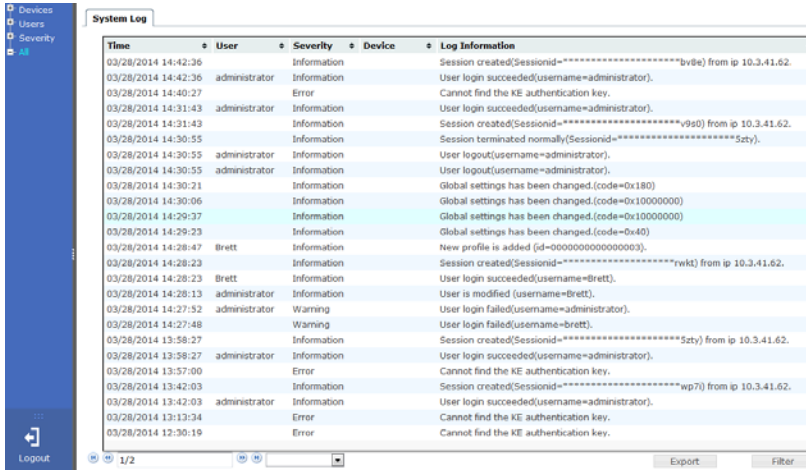
Overview

The Matrix Manager logs all the events that take place on it an stores them in a Log. The *Logs* tab opens on the **System Log** page, as shown here:



System Log

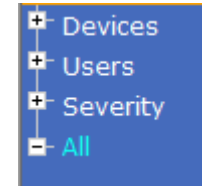
The *System Log* page displays events that take place on the Matrix Manager and provides a breakdown of the time, user, severity, device, and log information, for a description of each event. You can change the sort order of the display by clicking on the column headings.



- The first four buttons on the lower row navigate through the pages of the listed events. The left takes you to the first page; the right takes you to the last page; the middle buttons move you backward or forward one page.

Note: These buttons are only active when there is a relevant action they can perform. For example, when there is more than one page of information and you are on the first page, the “move forward” and “last page” buttons are active, but the “move backward” and “first page” buttons are not.

- Clicking the plus sign (+) beside a category in the sidebar menu expands the event headings into subcategories. Selecting a subcategory allows you to view only the logs that relate to that choice.
- Clicking **All** from the sidebar returns you to the default view to display all events.
- In general, a blank page, indicates that there were no log events recorded for that category.

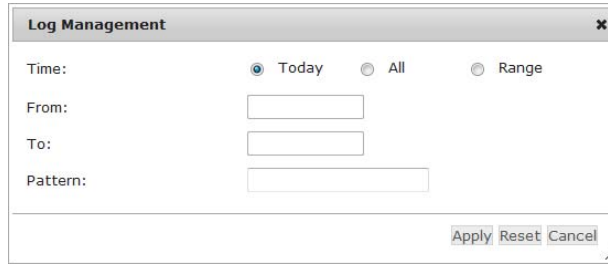


The log file tracks a maximum of 512 events. When the limit is reached, the oldest events get discarded as new events come in. The buttons at the bottom of the page are shown below and described in the table:

Button	Explanation
Navigation Buttons	The four buttons on the lower row (right side) navigate through the pages of the listed events. The left takes you to the first page; the right takes you to the last page; the middle buttons move you backward or forward one page.
Drop-Down Menu	Use this menu to select how many events you want to display per page. Available choices are 25, 50, and 100.
Export	Clicking *Export* lets you save the contents of the log to a file on your computer.
Filter	Clicking *Filter* allows you to search for particular events by date or by specific words or strings, as described in the next section.

Filter

Filter lets you narrow the log event display to ones that occurred at specific times; ones containing specific words or strings. When you access this function, the log filter dialog box appears at the bottom of the page:



(Continues on next page.)

(Continued from previous page.)

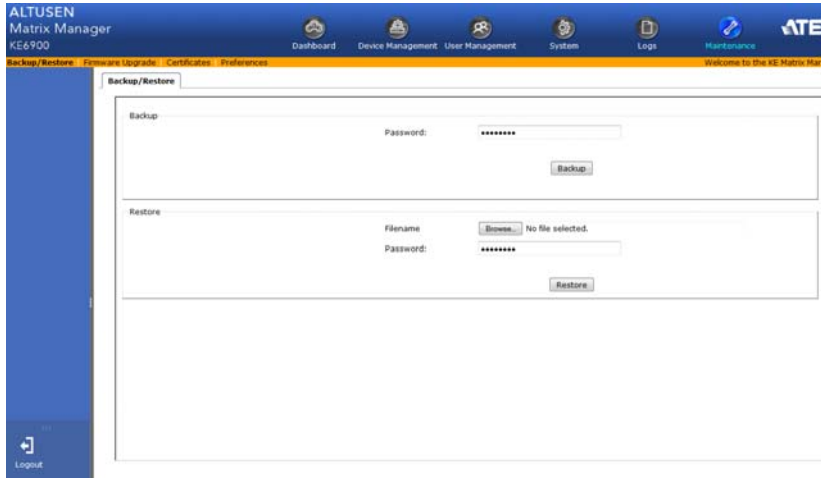
A description of the filter items is given in the table, below:

Item	Description
Time	This feature lets you filter for events that occurred at specific times, as follows: **Today**: Only the events for the current day are displayed. **All**: Displays all events. **Range:** Select a time frame of events. After selecting Range, click inside the **From/To** text box in order to bring up the calendar. ◆ **From**: Filters for events from a specific date and time to the present. Put a check in the checkbox to bring up a calendar. Set the date and time that you want the filtering to start from. All events from the Start date/time to the present are displayed. ◆ **To:** Filters for events from a specific date and time to a specific date and time. First select the **From** (described above). After checking **Range**, you have to click inside the text box in order to bring up the calendar.
Pattern	Filters for a particular word or string. Key the word or string into the *Information* text box. Only events containing that word or string are displayed. Wildcards (? for single characters; * for multiple characters) and the keyword **or** are supported. E.g., h*ds would return hands and hoods; h?nd would return hand and hind, but not hard; h*ds or h*ks would return hands and hooks.
Apply	Click to apply the filter choices.
Reset	Click this button to clear the entries in the dialog box and start with a clean slate.
Cancel	Click this button to exit the log filter function.

Chapter 11
Maintenance

Overview

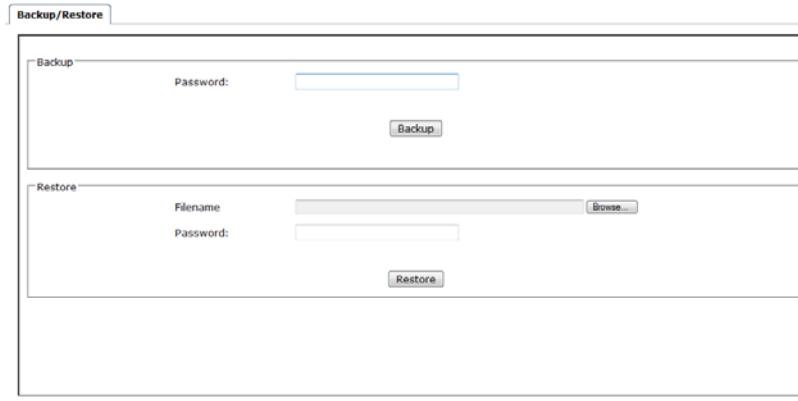
The *Maintenance* tab has four menu bar options: **Backup/Restore**, **Firmware Upgrade**, **Certificates**, and **Preferences**. When you click the Maintenance tab, it opens on the *Backup/Restore* page, as shown here:



- *Backup/Restore* allows administrators to backup system configuration settings to a file, and restore configuration settings from previously saved files.
- *Firmware Upgrade* allows administrators to upgrade firmware for network connected devices.
- *Certificates* allow for enhanced security, the *Private Certificate* section allows you to use your own private encryption key and signed certificate.
- *Preferences* allows the user that is logged in to set individual preferences for their browser sessions.

Backup / Restore

When you click the **Maintenance** tab Matrix Manager, the *Backup/Restore* page is displayed. The page is divided into two main sections: Backup, and Restore:



The operations to perform backup/restore procedures are described in the table below:

Procedure	Operation
Backup	Backs up the Matrix Manager configuration – including User Station, Transmitter, Target, and Profile configurations; user and group accounts, user profiles, logs, and system settings.
Restore	Deletes the current User Station, Transmitter, Target, and Profile configurations; user and group accounts, user profiles, logs, and system settings.; then restores those settings to the values that exist in the previously saved backup file.

Backup

To back up system configuration settings, do the following:

1. (Optional) In the *Backup* panel, provide a password for the backup file. Any combination of characters may be used for the password.

   Note: Providing a password is a security feature – if you provide a password, you will need to give the same password in order to restore the configuration settings from this file.

2. Click **Backup**.

3. In the dialog box that comes up, Click **Save** to save the configuration file (*System.conf*) to a location on your hard disk.
4. Navigate to the directory where you want to save the file and click **Save**.

Restore

To restore system configuration settings, do the following:

1. In the *Restore* panel, click **Browse**.
2. Navigate to the directory where the backup file is located and select it.
3. When you return to the Backup/Restore page enter the password you set when the backup file was created.

   Note: If you did not set a password for the file, leave the field blank.

4. Click **Restore**.
5. Click **OK** to confirm that you want to restore the configuration data.

   When the Restore procedure is in process, a message stating that the Matrix Manager will restart will appear. After a short while the Matrix Manager closes and refreshes at the log in screen. When it comes back up the configuration settings that were restored from the backup file are in effect.

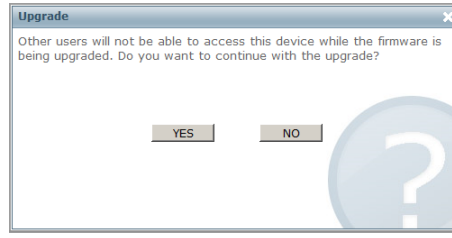
Firmware Upgrade

New firmware versions can be downloaded from our website as they become available. Check the website regularly, to find the latest upgrade packages.

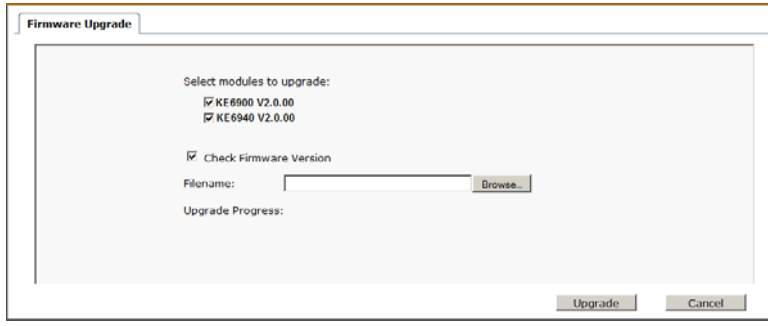
Under Firmware Upgrade all KE6900/KE6940 devices that are discovered online are provided in a list allowing you to select which devices get upgraded.

To upgrade the firmware do the following:

1. Go to our website and download the firmware upgrade package appropriate to your KE6900 / KE6940 device.
2. Open your browser and log in to the Matrix Manager with an administrator's account.
3. Click the **Maintenance** tab; select **Firmware Upgrade** on the menu bar. A confirmation dialog box may appear:



4. Click **Yes** to continue. After a short while, the *Firmware Upgrade* page comes up:



All the KE6900 / KE6940 devices that are capable of being upgraded are listed.

Note: Only online KE6900 / KE6940 devices show up in the list. Offline devices do not get upgraded.

5. Make sure there is a check in the checkbox in front of the modules you want to upgrade. Uncheck the modules that you do not want to upgrade.
6. Click **Browse**. Navigate to the directory where the firmware upgrade file is located and select it.
7. Enable or disable *Check Firmware Version*
   - If you enabled *Check Firmware Version* the current firmware level is compared with that of the upgrade file. If the current version is equal to or higher than the upgrade version, a popup message appears, to inform you of the situation and stops the upgrade procedure.
   - If you didn't enable *Check Main Firmware Version*, the upgrade file is installed without checking what its level is.
8. Click **Upgrade** to start the upgrade procedure. As the upgrade proceeds, progress information is shown on the screen. Once the upgrade completes successfully, the devices will reset.
9. Log in to the and check the firmware version to be sure it is the new one.

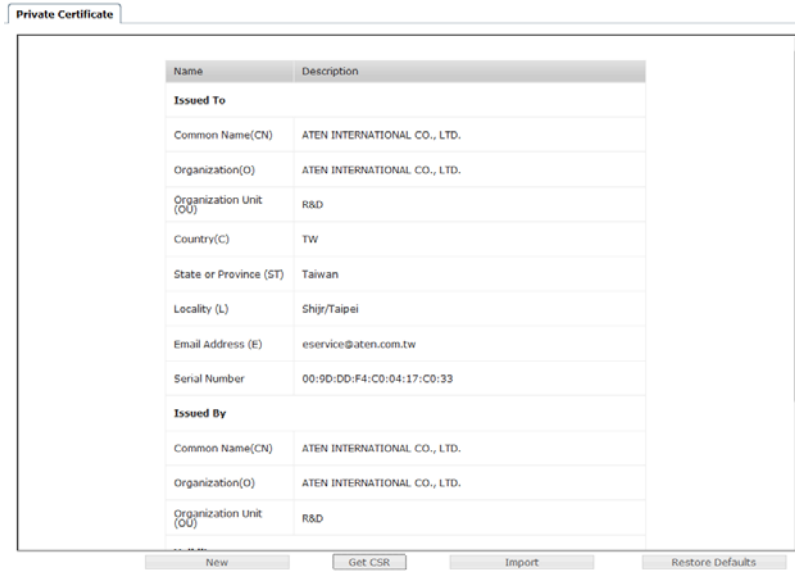
Firmware Upgrade Recovery

If the Upgrade Succeeded screen doesn't appear or the upgrade procedure is abnormally halted (due to computer crash, power failure, etc.), the device may become inoperable. If you find that the device does not work following a failed or interrupted upgrade, do the following

1. Power off the KE6900 / KE6940.
2. Press the **Reset** button, then power on the KE6900 / KE6940 while holding Reset.
3. Hold **Reset** for 5 seconds after the device is powered on.
4. The device will revert to a previous firmware version and recover from the failure.
5. Upgrade the firmware to the most current version available.

Certificates

This page provides information about the *Private Certificates*:



Private Certificate

When logging in over a secure (SSL) connection, a signed certificate is used to verify that the user is logging in to the intended site. For enhanced security, the *Private Certificate* section allows you to use your own private encryption key and signed certificate, rather than the default ATEN certificate.

There are two methods for establishing your private certificate: generating a self-signed certificate; and importing a third-party certificate authority (CA) signed certificate.

- Generating a Self-Signed Certificate

  If you wish to create your own self-signed certificate, a free utility – openssl.exe – is available for download over the web. See *Self-Signed Private Certificates*, page 139 for details about using OpenSSL to generate your own private key and SSL certificate.

- Obtaining a CA Signed SSL Server Certificate

  For the greatest security, we recommend using a third party certificate authority (CA) signed certificate. To obtain a third party signed certificate, go to a CA (Certificate Authority) website to apply for an SSL certificate.

After the CA sends you the certificate and private encryption key, save them to a convenient location on your computer.

- Importing the Private Certificate

  To import the private certificate, do the following:

1. Click **Import** from the bottom of the Private Certificate page, shown here:

2. Click **Browse** to the right of *Certificate Filename*; and browse to where your certificate file is located; and select it.
3. Click **Import** to complete the procedure.

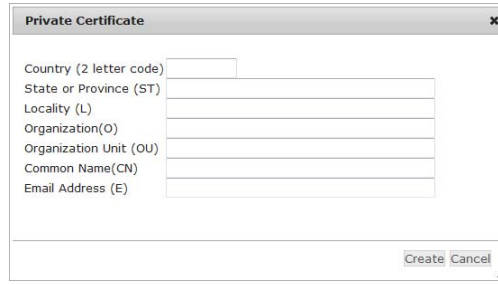
Note: Clicking **Restore Defaults** returns the device to using the default ATEN certificate.

Certificate Signing Request

The Certificate Signing Request (CSR) section provides an automated way of obtaining and installing a CA signed SSL server certificate.

To perform this operation do the following:

1. Click **New**. The following dialog box appears:



2. Fill in the form – with entries that are valid for your site – according to the example information in the following table:

Information	Example
Country (2 letter code)	TW

Information	Example
State or Province	Taiwan
Locality	Taipei
Organization	Your Company, Ltd.
Organization Unit	Tech Department
Common Name	mycompany.com **Note:** This must be the exact domain name of the site that you want the certificate to be valid for. If the site's domain name is *www.mycompany.com*, and you only specify *mycompany.com*, the certificate will not be valid.
Email Address	administrator@yourcompany.com

3. After filling in the form (all fields are required), click **Create**.

   A self-signed certificate based on the information you just provided is now stored on the Matrix Manager.

4. Click Get CSR, and save the certificate file (*csr.cer*) to a convenient location on your computer.

   This is the file that you give to the third party CA to apply for their signed SSL certificate.

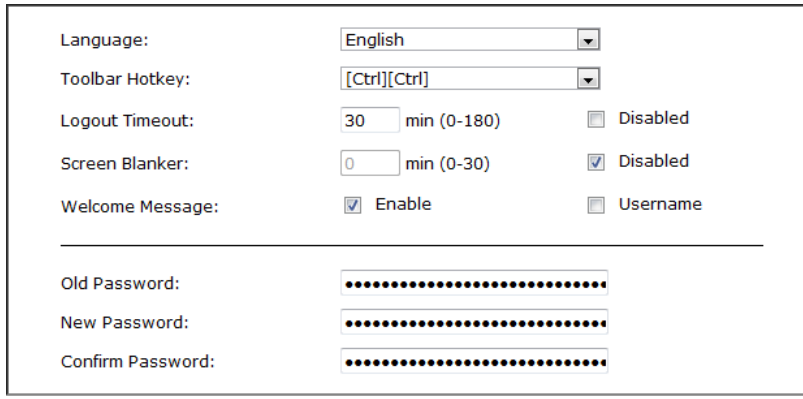
5. After the CA sends you the certificate, save it to a convenient location on your computer. Click **Import** to locate the file; then click **Import** to store it on the Matrix Manager.

Note: When you upload the file, the Matrix Manager checks the file to make sure the specified information still matches. If it does, the file is accepted; if not, it is rejected.

If you want to remove the certificate (to replace it with a new one because of a domain name change, for example), simply click **Restore Defaults**.

Preferences

Users can set individual preferences for their browser sessions on the *Preferences* page. The *Preferences* page allows you to select options for the user that is currently logged in.



Item	Description
Language	Click the drop-down menu to select the language you want to use during sessions for this user. Choices are: English, Chinese (Simplified), Chinese (Traditional), Japanese, Korean, Dutch, French, Spanish, Portuguese, and Russian.
Toolbar Hotkey	Select the hotkey combination to call the Tool Bar function for this user. The Tool Bar is used when accessing the computer from the Transmitter or Receiver side.
Logout Timeout	If there is no user input for the amount of time set with this function, the user is automatically logged out. A login is necessary before the Matrix Manager can be accessed again. The default is 30 minutes.
Screen Blanker	Set how many minutes the KE6900 / KE6940 waits when a session is idle before turning off the display.
Welcome Page	If you want the Welcome Message to appear on screen when the user logs in, select **Enable**. If you want the user's Screen Name to appear with the Welcome Message, check the **Username** check box.

Item	Description
Password	This section allows you to change the user's password: 1. Key in your old password in the Old password field. 2. Key in your new password in the New password field. 3. Key in your new password again in the Confirm password field.

When you have made your choices, Click **Save**.

To use the original system set preferences, click **Restore Defaults**.

Chapter 12
Firmware Upgrade Utility

The Windows-based Firmware Upgrade Utility (FWUpgrade.exe) provides a smooth, automated process for upgrading the KVM switch's firmware. The Utility comes as part of a Firmware Upgrade Package that is specific for each device. New firmware upgrade packages are posted on our web site as new firmware revisions become available. Check the web site regularly to find the latest packages and information relating to them:

`http://www.aten.com`

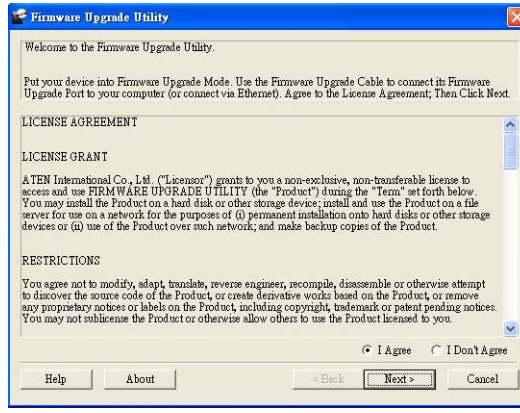
Preparation

1. From a computer that is not part of your KVM installation go to our Internet support site and choose the model name that relates to your device KE6900 / KE6940 to get a list of available Firmware Upgrade Packages.
2. Choose the Firmware Upgrade Package you want to install (usually the most recent), and download it to your computer.
3. Be sure that the computer is connected to the same LAN segment as the KE6900 / KE6940 devices.

Starting the Upgrade

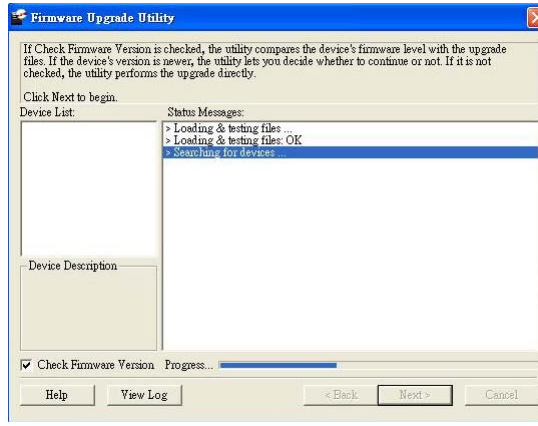
To upgrade your firmware:

1. Run the downloaded Firmware Upgrade Package file - either by double clicking the file icon, or by opening a command line and entering the full path to it. The Firmware Upgrade Utility Welcome screen appears:

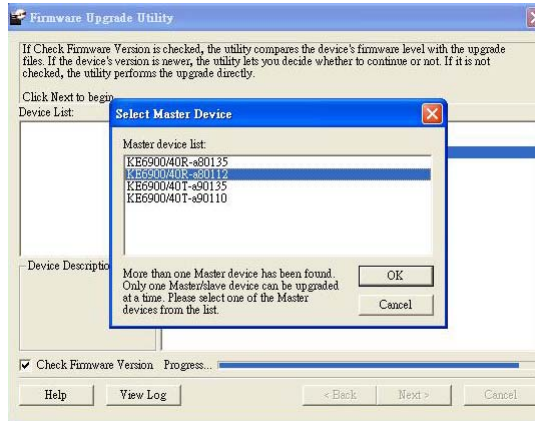


Note: The screens shown in this section are for reference only.

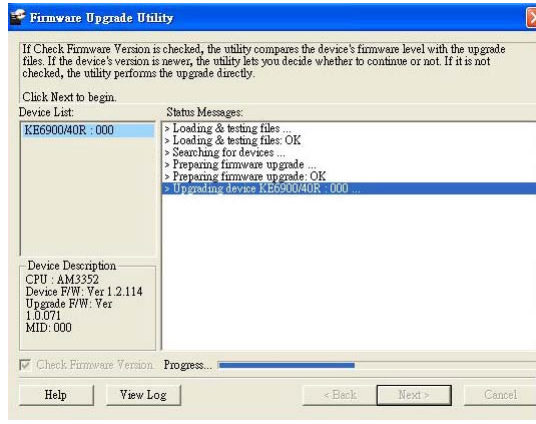
2. Read the License Agreement (enable the *I Agree* radio button).
3. Click **Next**. The Firmware Upgrade Utility main screen appears:



4. The Utility inspects your installation. All the devices capable of being upgraded by the package are listed in the *Select Master Device* list.



5. After you have made your device selection, Click **OK** and then **Next** to begin the upgrade.



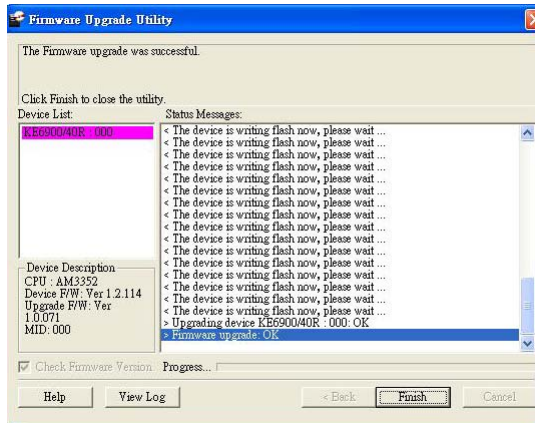
If you enabled Check Firmware Version, the Utility compares the device's firmware level with that of the upgrade files. If it finds that the device's version is higher than the upgrade version, it brings up a dialog box informing you of the situation and gives you the option to **Continue** or **Cancel**.

If you didn't enable *Check Firmware Version*, the Utility installs the upgrade files without checking whether they are a higher level, or not.

As the Upgrade proceeds status messages appear in the Status Messages panel, and the progress toward completion is shown on the *Progress* bar.

Upgrade Succeeded

After the upgrade has completed, a screen appears to inform you that the procedure was successful:



Firmware Upgrade Recovery

If the Upgrade Succeeded screen doesn't appear or the upgrade procedure is abnormally halted (due to computer crash, power failure, etc.), the device may become inoperable. If you find that the device does not work following a failed or interrupted upgrade, do the following

1. Power off the KE6900 / KE6940.
2. Press the **Reset** button, then power on the KE6900 / KE6940 while holding Reset.
3. Hold **Reset** for 5 seconds after the device is powered on.
4. The device will revert to a previous firmware version and recover from the failure.
5. Upgrade the firmware to the most current version available.

This Page Intentionally Left Blank

Appendix

Safety Instructions

General

- This product is for indoor use only.
- Read all of these instructions. Save them for future reference.
- Follow all warnings and instructions marked on the device.
- Do not place the device on any unstable surface (cart, stand, table, etc.). If the device falls, serious damage will result.
- Do not use the device near water.
- Do not place the device near, or over, radiators or heat registers.
- The device cabinet is provided with slots and openings to allow for adequate ventilation. To ensure reliable operation, and to protect against overheating, these openings must never be blocked or covered.
- The device should never be placed on a soft surface (bed, sofa, rug, etc.) as this will block its ventilation openings. Likewise, the device should not be placed in a built in enclosure unless adequate ventilation has been provided.
- Never spill liquid of any kind on the device.
- Unplug the device from the wall outlet before cleaning. Do not use liquid or aerosol cleaners. Use a damp cloth for cleaning.
- The device should be operated from the type of power source indicated on the marking label. If you are not sure of the type of power available, consult your dealer or local power company.
- The device is designed for IT power distribution systems with 230V phase-to-phase voltage.
- To prevent damage to your installation it is important that all devices are properly grounded.
- The device is equipped with a 3-wire grounding type plug. This is a safety feature. If you are unable to insert the plug into the outlet, contact your electrician to replace your obsolete outlet. Do not attempt to defeat the purpose of the grounding-type plug. Always follow your local/national wiring codes.
- Do not allow anything to rest on the power cord or cables. Route the power cord and cables so that they cannot be stepped on or tripped over.

- If an extension cord is used with this device make sure that the total of the ampere ratings of all products used on this cord does not exceed the extension cord ampere rating. Make sure that the total of all products plugged into the wall outlet does not exceed 15 amperes.
- To help protect your system from sudden, transient increases and decreases in electrical power, use a surge suppressor, line conditioner, or uninterruptible power supply (UPS).
- Position system cables and power cables carefully; Be sure that nothing rests on any cables.
- Never push objects of any kind into or through cabinet slots. They may touch dangerous voltage points or short out parts resulting in a risk of fire or electrical shock.
- Do not attempt to service the device yourself. Refer all servicing to qualified service personnel.
- If the following conditions occur, unplug the device from the wall outlet and bring it to qualified service personnel for repair.
  - The power cord or plug has become damaged or frayed.
  - Liquid has been spilled into the device.
  - The device has been exposed to rain or water.
  - The device has been dropped, or the cabinet has been damaged.
  - The device exhibits a distinct change in performance, indicating a need for service.
  - The device does not operate normally when the operating instructions are followed.
- Only adjust those controls that are covered in the operating instructions. Improper adjustment of other controls may result in damage that will require extensive work by a qualified technician to repair.
- Do not connect the RJ-11 connector marked “UPGRADE” to a public telecommunication network.

Rack Mounting

- Before working on the rack, make sure that the stabilizers are secured to the rack, extended to the floor, and that the full weight of the rack rests on the floor. Install front and side stabilizers on a single rack or front stabilizers for joined multiple racks before working on the rack.
- Always load the rack from the bottom up, and load the heaviest item in the rack first.
- Make sure that the rack is level and stable before extending a device from the rack.
- Use caution when pressing the device rail release latches and sliding a device into or out of a rack; the slide rails can pinch your fingers.
- After a device is inserted into the rack, carefully extend the rail into a locking position, and then slide the device into the rack.
- Do not overload the AC supply branch circuit that provides power to the rack. The total rack load should not exceed 80 percent of the branch circuit rating.
- Make sure that all equipment used on the rack – including power strips and other electrical connectors – is properly grounded.
- Ensure that proper airflow is provided to devices in the rack.
- Ensure that the operating ambient temperature of the rack environment does not exceed the maximum ambient temperature specified for the equipment by the manufacturer.
- Do not step on or stand on any device when servicing other devices in a rack.

Technical Support

International

- For online technical support – including troubleshooting, documentation, and software updates: **http://support.aten.com**
- For telephone support, See *Telephone Support*, page iii:

North America

Email Support		support@aten-usa.com
Online Technical Support	Troubleshooting Documentation Software Updates	http://www.aten-usa.com/support
Telephone Support		1-888-999-ATEN ext 4988

When you contact us, please have the following information ready beforehand:

- Product model number, serial number, and date of purchase.
- Your computer configuration, including operating system, revision level, expansion cards, and software.
- Any error messages displayed at the time the error occurred.
- The sequence of operations that led up to the error.
- Any other information you feel may be of help.

Specifications

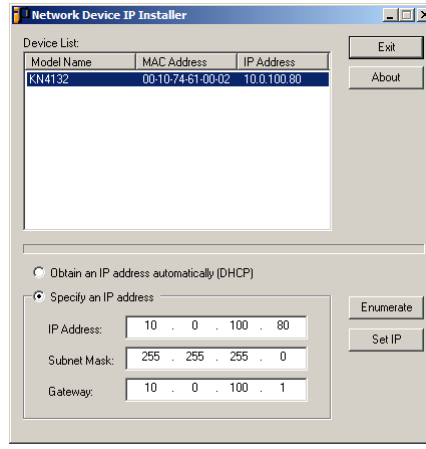
Function			KE6900T	KE6940T
Connectors	Console Ports	Keyboard	1 x USB Type A Female (White)	
		Video	1 x DVI-I Female (White)	2 x DVI-I Female (White)
		Mouse	1 x USB Type A Female (White)	
		Speaker	1 x Mini Stereo Jack Female (Green)	
		Mic.	1 x Mini Stereo Jack Female (Pink)	
		RS-232	1 x DB-9 Male (Black)	
	KVM Ports	KB / Mouse	USB Type B Female (White)	
		Speaker	1 x Mini Stereo Jack (Green)	
		Mic.	1 x Mini Stereo Jack (Pink)	
		Video	1 x DVI-I Female (White)	2 x DVI-I Female (White)
		RS-232	1 x DB-9 Female (Black)	
	Power		1 x DC Jack (Black)	
	LAN		1 x RJ-45 Female (Black)	
Switches	Console Selection / Config		1 x Slide switch (Black) (Auto, Local, Config)	
	Reset		1 x Semi-recessed Pushbutton	
LEDs	LAN		1 (Green / Orange)	
	Power		1 x Blue	
	Local		1 x Green	
	Remote		1 x Green	
Emulation	Keyboard / Mouse		USB	
Power Consumption			DC 5V	DC 5V
Video			Up to 1920 x 1200	
Environment	Operating Temp.		0–50ºC	
	Storage Temp		-20–60ºC	
	Humidity		0–95% RH, Non-condensing	
Physical Properties	Housing		Metal	
	Weight		1.13 kg	1.15 kg
	Dimensions (L x W x H)		21.50 x 16.30 x 4.60 cm	

Function			KE6900R	KE6940R
Connectors	USB Virtual Media		2 x USB Type A Female (White)	
	Console Ports	Keyboard	1 x USB Type A Female (White)	
		Video	1 x DVI-I Female (White)	2 x DVI-I Female (White)
		Mouse	1 x USB Type A Female (White)	
		Speaker	1 x Mini Stereo Jack Female (Green)	
		Mic.	1 x Mini Stereo Jack Female (Pink)	
	RS-232		1 x DB-9 Male (Black)	
	Power		1 x DC Jack (Black)	
	LAN		1 x RJ-45 Female (Black)	
Switches	OSD		1 x Pushbutton	
	Video		1 x Pushbutton	
	Graphics		1 x Pushbutton	
	Console Selection / Config		1 x Slide switch (Black) (Auto, Config)	
	Reset		1 x Semi-recessed Pushbutton	
LEDs	LAN		1 (Green / Orange)	
	Power		1 x Blue	
	Local		1 x Green	
	Remote		1 x Green	
Emulation	Keyboard / Mouse		USB	
Power Consumption			DC 5V	DC 5V
Video			Up to 1920 x 1200	
Environment	Operating Temp.		0–50ºC	
	Storage Temp		-20–60ºC	
	Humidity		0–95% RH, Non-condensing	
Physical Properties	Housing		Metal	
	Weight		1.25 kg	1.25 kg
	Dimensions (L x W x H)		22.80 x 17.10 x 55.00 cm	

IP Installer

From a client computer running Windows, an IP address for a transmitter or receiver can be assigned with the IP Installer utility. The utility can be obtained from the Download area of our website. Look under Driver/SW. After downloading the utility to your client computer, do the following:

1. Unzip the contents of IPInstaller.zip to a directory on your hard drive.
2. Go to the directory that you unzipped the IPInstaller program to and run IPInstaller.exe. A dialog box similar to the one below appears:



3. Select the Transmitter or Receiver in the Device List.

Note: 1. If the list is empty, or your device doesn't appear, click **Enumerate** to refresh the Device List.

2. If there is more than one device in the list, use the MAC address to pick the one you want. The MAC address is located on the devices bottom panel.

4. Select either *Obtain an IP address automatically (DHCP)*, or *Specify an IP address*. If you chose the latter, fill the IP Address, Subnet Mask, and Gateway fields with the information appropriate to your network.
5. Click **Set IP**.
6. After the IP address shows up in the Device List, click **Exit**. See *IP Installer*, page 152 for more information.

Trusted Certificates

Overview

When you try to log in to the device from your browser, a Security Alert message appears to inform you that the device's certificate is not trusted, and asks if you want to proceed.

The certificate can be trusted, but the alert is triggered because the certificate's name is not found on the Microsoft list of Trusted Authorities. You can ignore the warning and click **Yes** to go on.

Self-Signed Private Certificates

If you wish to create your own self-signed encryption key and certificate, a free utility – openssl.exe – is available for download over the web at **www.openssl.org**. To create your private key and certificate do the following:

1. Go to the directory where you downloaded and extracted *openssl.exe* to.
2. Run openssl.exe with the following parameters:

```
openssl req -new -newkey rsa:1024 -days 3653 -nodes -x509
-keyout CA.key  -out CA.cer -config openssl.cnf
```

Note: 1. The command should be entered all on one line (i.e., do not press [Enter] until all the parameters have been keyed in).

2. If there are spaces in the input, surround the entry in quotes (e.g., "ATEN International").

To avoid having to input information during key generation the following additional parameters can be used:

```
/C /ST /L /O /OU /CN /emailAddress.
```

Examples

```
openssl req -new -newkey rsa:1024 -days 3653 -nodes -x509
-keyout CA.key  -out CA.cer -config openssl.cnf -subj
/C=yourcountry/ST=yourstateorprovince/L=yourlocationor
city/O=yourorganiztion/OU=yourorganizationalunit/
CN=yourcommonname/emailAddress=name@yourcompany.com
```

```
openssl req -new -newkey rsa:1024 -days 3653 -nodes -x509
-keyout CA.key  -out CA.cer -config openssl.cnf -subj
/C=CA/ST=BC/L=Richmond/O="ATEN International"/OU=ATEN
/CN=ATEN/emailAddress=eservice@aten.com.tw
```

Importing the Files

After the openssl.exe program completes, two files – CA.key (the private key) and CA.cer (the self-signed SSL certificate) – are created in the directory that you ran the program from.

Limited Warranty

ALTUSEN warrants this product against defects in material or workmanship for a period of one (1) year from the date of purchase. If this product proves to be defective, contact ALTUSEN's support department for repair or replacement of your unit. ALTUSEN will not issue a refund. Return requests can not be processed without the original proof of purchase.

When returning the product, you must ship the product in its original packaging or packaging that gives an equal degree of protection. Include your proof of purchase in the packaging and the RMA number clearly marked on the outside of the package.

This warranty becomes invalid if the factory-supplied serial number has been removed or altered on the product.

This warranty does not cover cosmetic damage or damage due to acts of God, accident, misuse, abuse, negligence or modification of any part of the product. This warranty does not cover damage due to improper operation or maintenance, connection to improper equipment, or attempted repair by anyone other than ALTUSEN. This warranty does not cover products sold AS IS or WITH FAULTS.

IN NO EVENT SHALL ALTUSEN'S LIABILITY EXCEED THE PRICE PAID FOR THE PRODUCT. FURTHER, ALTUSEN SHALL NOT BE RESPONSIBLE FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES RESULTING FROM THE USE OF THE PRODUCT, ITS ACCOMPANYING SOFTWARE, OR ITS DOCUMENTATION. ALTUSEN SHALL NOT IN ANY WAY BE RESPONSIBLE FOR, WITHOUT LIMITATION, LOSS OF DATA, LOSS OF PROFITS, DOWNTIME, GOODWILL, DAMAGE OR REPLACEMENT OF EQUIPMENT OR PROPERTY, AND ANY EXPENSES FROM RECOVERY, PROGRAMMING, AND REPRODUCTION OF ANY PROGRAM OR DATA.

ALTUSEN makes no warranty or representation, expressed, implied, or statutory with respect to its products, contents or use of this documentation and all accompanying software, and specifically disclaims its quality, performance, merchantability, or fitness for any particular purpose.

ALTUSEN reserves the right to revise or update its product, software or documentation without obligation to notify any individual or entity of such revisions, or update.

For details about extended warranties, please contact one of our dedicated value added resellers.

Index

T

U