Simply Better Connections

RCMDVI00AT / RCMDVI40AT / RCMDVI00BT / RCMDVI40BT / RCMDVI50T

Secure Device Server

User Manual

Compliance Statements

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 of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

The device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

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.

Warning

Operation of this equipment in a residential environment could cause radio interference.

Suggestion

Shielded twisted pair (STP) cables must be used with the unit to ensure compliance with FCC & CE standards.

Achtung

Der Gebrauch dieses Geräts in Wohnumgebung kann Funkstörungen verursachen.

KCC Statement

유선 제품용 / A 급 기기 (업무용 방송 통신 기기)
이 기기는 업무용 (A 급) 전자파적합기기로서 판매자 또는 사용자는 이 점을 주의하시기 바라며 , 가정 외의 지역에서 사용하는 것을 목적으로 합니다 .

Industry Canada Statement
This Class A digital apparatus complies with Canadian ICES-003.

CAN ICES-003 (A) / NMB-003 (A)

RoHS
This product is RoHS compliant.

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	86-400-810-0-810
Japan	81-3-5615-5811
Korea	82-2-467-6789
North America	1-888-999-ATEN ext 4988 1-949-428-1111

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.

Product Information

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

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

Package Contents

Check to make sure that all components are in working order. If you encounter any problem, please contact your dealer.

RCMDVI00AT / RCMDVI40AT

Package content of RCMDVI00AT / RCMDVI40AT DVI Single/Dual Display KVM over IP Extender (Transmitter) with Remote Access:

1 Transmitter

1 KVM cable (DVI-D, USB Type-B, audio)

1 DVI-D cable (RCMDVI40AT only)

1 foot pad set (4 pcs)

1 power adapter

1 mounting kit

1 user instructions

RCMDVI00BT / RCMDVI40BT / RCMDVI50T

Package content of RCMDVI00BT / RCMDVI40BT / RCMDVI50T DVI Single/Dual Link Single/Dual Display KVM over IP Extender (Transmitter) with Remote Access:

1 Transmitter

1 KVM cable (DVI-D, USB Type-B, audio)

1 DVI-D cable (RCMDVI40BT only)

1 foot pad set (4 pcs)

1 power adapter

1 mounting kit

1 user instructions

Contents

About This Manual

This User Manual is provided to help you get the most from your RCM KVM over IP Transmitter. It covers all aspects of installation, configuration and operation. An overview of the information found in the manual is provided below.

The KVM over IP Extender models covered in this user manuals are:

Models	Product Names
RCMDVI00AT	DVI-I Single Display KVM over IP Extender (Transmitter) with Remote Access
RCMDVI40AT	DVI-I Dual Display KVM over IP Extender (Transmitter) with Remote Access
RCMDVI00BT	DVI-I Single Link Single Display KVM over IP Extender (Transmitter) with Remote Access
RCMDVI40BT	DVI-I Single Link Dual Display KVM over IP Extender (Transmitter) with Remote Access
RCMDVI50T	DVI-I Dual Link Single Display KVM over IP Extender (Transmitter) with Remote Access

Chapter 1, Introduction, introduces you to the RCM KVM over IP Transmitter. 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, API Functions, Provides useful API functions for users to access and configure the RCM KVM over IP Transmitter via Windows DLL as required by varying scenarios and applications.

Chapter 4, OSD Operation, explains the fundamental concepts involved in operating the RCMDVI00AT / RCMDVI40AT / RCMDVI00BT / RCMDVI40BT / RCMDVI50T, and provides a complete description of the On Screen Displays (OSDs) and how to work with them.

Chapter 5, Software Installation, explains the administrative procedures that are required to download and install the KVM over IP Matrix Manager on Windows and Linux computers.

Chapter 6, Browser / Telnet Operation, explains how to log in to the KVM over IP Matrix Manager with a web browser, and describes the features, functions, and how to work with the browser's main interface.

Chapter 7, System Status, explains how to use the KVM over IP Matrix Manager's System Status panel to manage Transmitters, Receivers, Users, Profiles and Logs.

Chapter 8, System Settings, explains the KVM over IP Matrix Manager's system settings, which include the General, ANMS, LDAP/AD, RADIUS, TACACS+ authentication, F/W Upgrade, Redundancy, Backup/Restore, Certificates, and Sessions tabs.

Chapter 9, Connections, describes how to use the KVM over IP Matrix Manager 's Connections panel to view and disconnect Transmitter and Receiver connections.

Chapter 10, Scheduled Profile, describes how to use the KVM over IP Matrix Manager's Scheduled Profile panel to view active profile schedules.

Chapter 11, Sessions, describes how to use the KVM over IP Matrix Manager's Sessions panel to view and disconnect user sessions.

Chapter 12, Remote Viewer, describes how to use the Remote Viewer to view and control video sources connected to AiT transmitters.

Chapter 13, Firmware Upgrade Utility, explains how to download and use the Firmware Upgrade Utility to install new firmware on the devices.

Chapter 14, CLI Commands, provides a complete list of the serial protocol and TCP/IP commands used when utilizing the RS-232 Serial Port or a network connection to configure the KE devices.

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

Note:

- Read this manual thoroughly and follow the installation and operation procedures carefully to prevent any damage to the unit or connected devices.
- The product may be updated, with features and functions added, improved or removed since the release of this manual. For an up-to-date user manual, visit http://www.aten.com/global/en/

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 (such as on a menu or dialog box), that comes next. For example, Start > Run means to open the *Start* menu, and then select *Run*.
	Indicates critical information.

Chapter 1
Introduction

Overview

The RCM series KVM over IP Extender (RCMDVI00AT / RCMDVI40AT / RCMDVI00BT / RCMDVI40BT / RCMDVI50T) is an ATEN KVM over IP matrix solution exclusively designed for production line applications. Combined with KE series Receivers and the KVM over IP Matrix Manager (CCKM), it extends and allows remote monitor and control access to PCs and/or workstations at a production line. The system lets operators set up a matrix of KVM consoles for managing the PCs and/or workstations via Ethernet connection, with the flexibility to control and configure each connection.

The high-performance IP-based RCM transmitters connects to a PC and/or workstation to deliver its data to the connected KE receivers, to collectively provide console access from a remote or separate locations. The PC / workstation can be 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, while keeping the PCs and/or workstations securely on the production line — away from the keyboard, mouse, and display.

The RCM transmitters are integrated with exclusive RCM API offering various functions for system integration and automation. The RCM transmitters sport a FPGA graphics processor that presents great image with video quality to enhance OCR accuracy. Moreover, the RCM transmitters further enhance theirs production line application capability by supporting access control box, USB/RS-232 touch panel, OSD title bar notification, multi-view, local console priority and RS-232 mouse.

The RCM transmitters offer exclusive, advanced RCM and OCR API integrated functions for easy management. Furthermore, for security, the RCM transmitters can pair with the optional 2XRT-0015G KVM over IP Access Control Box to locally enable or disable remote control privilege.

The RCM transmitters support flawless and lossless video compression quality with ultra low latency, with up to 1920 x 1200 resolution @ 60 Hz, 24-bit color depth.

For power redundancy, the RCM transmitters support dual power supplies with 2 DC jacks.

In addition, they support Fiber Channel over Ethernet via SFP fiber modules* which connect to a network switch at speeds up to 1.0 Gbps. The RCM transmitters can connect to KE receivers unit-to-unit or over a TCP/IP network via Gigabit Ethernet or the SFP ports. Connecting via both methods allows network failover.

The RCM transmitters support On Screen Display (OSD) configurations, from the connected KE receivers to configure both receivers and transmitters — for easy setup and operation.

RCM transmitters have RS-232 ports to connect to a serial terminal for configuration or serial devices such as touch screens and barcode scanners. They can connect to an Office LAN to support the Control Center Video Session Recorder (CCVSR) software and WinClient/ J avaClient. The CCVSR records all operations made on the PCs and/or workstations accessed through RCM transmitters. Every operation and change is recorded and saved to a secure video file for purposes such as security reference and troubleshooting. By using WinClient/JavaClient, you are provided with console access from a separate location over TCP/IP.

Refer to the table below for the variations in interfaces, functions and features:

Models	DVI	HDMI	DisplayPort	Power Redundancy via PoE*	Power Redundancy via Second Power Jack	Network Failover - SFP
RCMDVI00AT	1	-	-	-	1	1
RCMDVI40AT	2	-	-	-	1	1
RCMDVI00BT	1	-	-	-	1	1
RCMDVI40BT	2	-	-	-	1	1
RCMDVI50T	1	-	-	-	1	1

RCM KVM over IP Transmitters allow flexible setup as they can be integrated to PC-to-console connections 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 KVM over IP Matrix Manager (CCKM) allows you to define the aforementioned matrix connections and manage RCM/KE transmitters and KE receivers with features such as auto-detection, username/password authentication, switching and sharing of connections, scheduling, permissions and more. Whether you're extending computer access for Monitoring, Broadcasting, Editing or Workstation setup, the KVM over IP Matrix System gives you the flexibility and control to manage one or hundreds of extended connections. For more detailed feature list, refer to *Features* on page 4.

Note: The SFP module is sold separately. You can choose the 2A-136G, a multi-mode SFP module that provides 1 GbE connectivity up to 550 meters; or the 2A-137G, a single-mode SFP module that provides 1 GbE connectivity up to 10 kilometers. Visit ATEN's website or contact your ATEN dealer for more information.

Comparison Table

	DIO Control (Support Industrial Signal Light)	OSD Login (Local Console)	RFID Login (Local Console)	RCMMS	RCM API
RCMDVI00AT	X	X	X	O	O
RCMDVI40AT	X	X	X	O	O
RCMDVI00BT	O	O	O	O	O
RCMDVI40BT	O	O	O	O	O
RCMDVI50T	O	O	O	O	O

	Dual Link	VGA Support	Dual Display	ATEN Access Control Box
RCMDVI00AT	X	O	X	O
RCMDVI40AT	X	O	O	O
RCMDVI00BT	X	O	X	O
RCMDVI40BT	X	O	O	O
RCMDVI50T	O	O	X	O

Features

Exclusive RCM Functionalities

- Supports ATEN KVM over IP Access Control Box for on-site enabling / disabling of remote control privilege[1]
- Supports Legacy PS/2 Server with CV10KM USB to PS/2 Converter[2]
- Supports RCMMS for customizable Panel Array for operators to monitor all machines simultaneously
- OSD Title Bar Notification — instantly notifies users upon urgent events[3]
- Control terminal — supports DI / DO / Relay for the status detection of stack lights or any other external sensors[3]
- Supports an exclusive RCM API that enables more functions (e.g. OCR) to facilitate production line control for system integrators

Hardware

- Superior video quality — up to 1920 x 1200 @ 60 Hz; 24-bit color depth
- Supports recording of remotely-accessed computer operations using CCVSR
- Supports interlaced video format
- Supports stereo speakers and microphone
- Auto-MDIX — automatically detects cable type
- Built-in 8 kV /15 kV ESD protection and 2 kV surge protection
- Fan-less design for silent, energy-efficient operations
- Rack mountable — mounting options:

  1. 2X-021G Dual Rack Mount Kit[4]
  2. 2X-031G Single Rack Mount Kit[4]

- Supports 1 Gbps SFP fiber module expansions[5] for up to 10 km
- Supports power / network failover — dual DC jacks for power redundancy and 1 RJ-45 + 1 SFP fiber port for network failover to ensure constant availability for mission-critical applications
- Includes an industrial-grade power adapter — temperature tolerance of 0 ~ 50 ºC to ensure durability and adaptability under harsh environmental conditions.

- Supports digital (DVI) or analog (VGA) video output[6]
- Audio Enabled — supports stereo speakers and microphone
- High speed Virtual Media Support[7]
- Advance processor provides lossless and low latency video transmissions up to 1920 x 1200 @ 60 Hz; 2560 x 1600 @ 60 Hz (RCMDVI50T)

Management

- Integration with ATEN CCVSR Video Session Recording Software
- Local console — flexible local or over IP console access
- Supports Power Failover (2 DC Jacks) and Network Failover (SFP slot and RJ-45)
- Supports Tx OSD Login for Authentication Management[8]
- EDID Expert™ — selects optimum EDID settings for smooth power-up and highest quality display
- Four selectable access modes for multiple simultaneous access (Exclusive / Occupy / Share / View only mode) — administrators can select access modes of permissions on Tx devices to boost collaboration or to avoid interference among users
- On-screen preview — allows users to view and video of up to 36 displays on one screen
- Fast Switching — switches between different remote video resolutions on a local display within 0.3 seconds
- CLI — administrators can control all RCM transmitters via RS-232 or TCP/IP using a CLI or 3rd-party application
- Support Hotkey Commands
- Flashing LED and beeping features help locate and identify devices
- RCM devices can “Push” and “Pull” to share content

Security

- Dedicated LAN port for KE receiver direct connections — can be isolated from the corporate network
- Secure data transmission — 128-bit AES encryption to secure video / keyboard / mouse / data transmission
- Supports industry standard Transport Layer Security (TLS) protocol

Virtual Media

- Virtual media enables file transfers, OS patching, software installations and diagnostic testing
- Supports USB 2.0 DVD / CD drives, USB mass storage devices, PC hard drives and ISO images
- Supports Smart Card / CAC Reader
- Works with USB-enabled servers at OS and BIOS level

Advanced Features[9]

- Video Walls — create multiple video walls with up to 64 (8 x 8) displays per layout
- Advanced Scheduling — improves efficiency and saves costs by allowing connections to be set based on time and date
- Virtual Transmitter — to stream video, audio, USB, and serial sources independently
- Supports both internal and external authentication — external authentication supports LDAP (Active Directory), RADIUS, and TACACS+
- Four selectable access modes for multiple simultaneous access (Exclusive / Occupy / Share / View only mode) — administrators can select access modes of permissions on transmitter devices to boost collaboration or to avoid interference among users
- Configurable user and group permissions for access and control of RCM transmitters
- Transmitter grouping of up to 4 sets of RCM series transmitters to support Multi-Display applications
- Receiver privilege control — users at the transmitter local console can enable / disable receiver control privilege by simply pressing a button from the connected Access Control Box[1]
- Authentication Lock — automatically logs in upon reconnection after temporary power off or network disconnection
- Connection Redundancy — automatically connects to another transmitter (Tx) after disconnection with the original Tx, ensuring constant access to servers and/or workstations

- Disconnection Alert — Pop-up warning message and looping alarm beeping to notify users of disconnection status
- RCM API support through dedicated remote port: for system integration and automation
- Boundless Switching — simply moves the mouse cursor across screen boundaries to switch between different receivers (Rx)
- Supports recording of remotely-accessed computer operations using CCVSR
- RFID login without typing username and password[10]
- "Push" and "Pull" — shares content instantly to / from a single Rx or video wall by just one click

---

Note: 1. The KVM over IP Access Control Box (2XRT-0015G) is sold separately. Contact your ATEN dealer for product information.

2. The CV10KM USB to PS/2 Converter is sold separately. Contact your ATEN dealer for product information.

3. These exclusive RCM functionalities are only available on RCMDVI00BT / RCMDVI40BT / RCMDVI50T.

4. Please refer to the *Compatible Products* section on the product web page for the various compatible accessories.

5. SFP modules are required for fiber network connection. The SFP module (2A-136G / 2A-137G) is sold separately. Contact your ATEN dealer for product information.

6. To convert a DVI to VGA signal, a DVI-I to VGA converter is required.

7. Some of the RCMDVI00AT / RCMDVI40AT / RCMDVI00BT / RCMDVI40BT / RCMDVI50T's features may not be supported, depending on the functionality of the cascaded KVM switch. (For example, some switches do not support virtual media.)

8. This functionality is only available on RCMDVI00BT / RCMDVI40BT / RCMDVI50T.

9. Advanced functions are supported when the RCM transmitters are managed by KVM over IP Matrix Manager (CCKM).

10. This functionality is only available on RCMDVI00BT / RCMDVI40BT / RCMDVI50T and compatible with RFID Reader (Soyal AR-725-U) only.

Supported Video Resolutions

Resolutions	RCMDVI00AT / RCMDVI40AT / RCMDVI00BT / RCMDVI40BT / RCMDVI50T
3840 x 2160 @ 24/25/30 Hz	
3440 x 1440 @ 50 Hz	
2560 x 2048 @ 50 Hz	
2560 x 1600 @ 60 Hz	● (**RCMDVI50T only**)
2560 x 1440 @ 60 Hz	
2560 x 1080 @ 24/25/30/50/60/100/120 Hz	
2048 x 2048 @ 30/60 Hz	
2048 x 1536 @ 60 Hz	
2048 x 1536 @ 30 Hz	
2048 x 1152 @ 60 Hz	
1600 x 1600 @ 60 Hz	
1920 x 2160 @ 60 Hz	
1920 x 2160 @ 30 Hz	
1920 x 1440 @ 60 Hz	
1920 x 1200 @ 60 Hz	●
1920 x 1080 @ 60 Hz	●
1600 x 1200 @ 60 Hz	●
1680 x 1050 @ 60 Hz	●
1400 x 1050 @ 60 Hz	●
1280 x 1024 @ 60/75 Hz	●
1280 x 960 @ 60 Hz	●
1280 x 720 @ 60 Hz	●
1600 x 900 @ 60 Hz	●
1440 x 900 @ 60 Hz	●
1152 x 864 @ 75 Hz	●
1366 x 768 @ 60 Hz	●
1280 x 720 @ 60 Hz	●
1024 x 768 @ 60/70/75/85 Hz	●
848 x 480 @ 60 Hz	
800 x 600 @ 56/60/72/75/85 Hz	●
720 x 400 @ 70/85 Hz	●
640 x 480 @ 60/72/75/85 Hz	●

Requirements

Console

- 1 or 2 DVI-D compatible monitors (respectively for RCMDVI00AT / RCMDVI00BT / RCMDVI50T or RCMDVI40AT / RCMDVI40BT) capable of the highest possible resolution
- 1 USB mouse
- 1 USB keyboard
- 1 microphone
- 1 set of speakers

Computers

The following components must be available on each PC / workstation that is to be connected to the device:

- 1 or 2 DVI ports (respectively for RCMDVI00AT / RCMDVI00BT / RCMDVI50T or RCMDVI40AT / RCMDVI40BT)
- 2 USB Type-A ports
- 1 audio in port
- 1 audio out port

Cables

- For optimal signal integrity and to simplify the setup, we strongly recommend that you only use the high-quality KVM cable, and the DVI-D cable (RCMDVI40AT / RCMDVI40BT only), that is provided with this package.

Minimum Hardware/Software Requirements

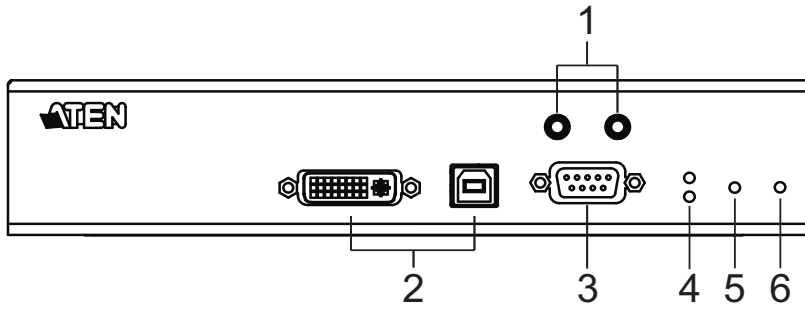
The minimum hardware and software requirements for the computer running the KVM over IP Matrix Manager are:

- Processor: Pentium 4, 2.60 GHz or above
- Memory: 1 GB or above
- HDD: 500 MB or above
- Web browser: Internet Explorer 10 or later, Chrome 70 or later, Firefox 62 or later
- Operating System Requirements:
  - Windows 7, 8.1, 10, server 2016, or Server 2019
  - Linux Ubuntu 16.04 or later, CentOS 7 or later
  - MacOS 10 or later

Note: Only Java Runtime Environment (JRE) 8 is supported.

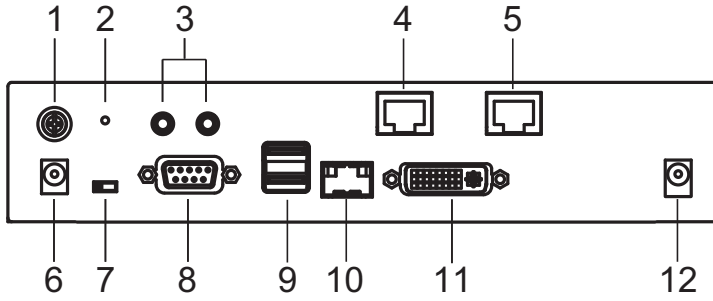
Components

RCMDVI00AT Front View



No.	Component	Description
1	audio ports	These mini stereo ports are for connecting to the speakers (green) and microphone (pink) ports of the PC / workstation.
2	KVM ports	The USB Type-B, DVI-D KVM cable supplied can link the transmitter to the PC / workstation to be controlled.
3	RS-232 port	This RS-232 serial port is for connecting to the PC / workstation for serial control or for connecting to a KVM over IP Access Control Box (2XRT-0015G).
4	remote / local LED	Lights green to indicate which side of the installation (local or remote) currently has KVM control of the PC / workstation.
5	LAN LED	This LED indicates the network status. ◆ Lights when connected to the LAN and blinks when the Ethernet connection is active: ◆ Orange: 10 Mbps ◆ Orange + Green: 100 Mbps ◆ Green: 1000 Mbps ◆ Off when not connected to the LAN.
6	power LED	Lights blue to indicate the unit is turned on.

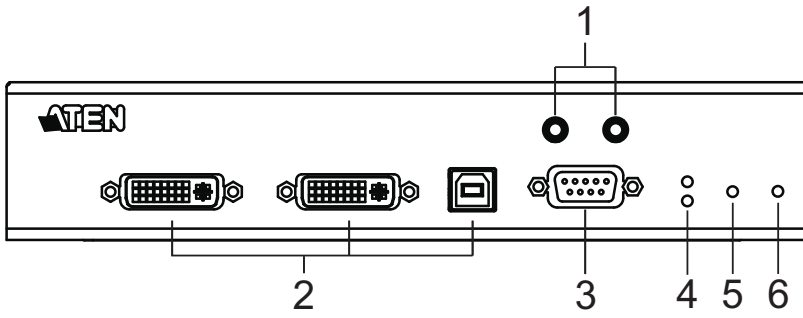
RCMDVI00AT Rear View



No.	Component	Description
1	grounding terminal	The wire used to ground the unit connects here.
2	reset button	This reset button 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 than three seconds resets the unit back to its factory default settings*. **Note:** The Reset to Factory Default function resets everything but the login information (username/password) to the factory default settings. To reset the login information, refer to *Reset All Information* on page 266.
3	audio ports	These mini stereo ports can connect to speakers (green) and a microphone (pink).
4	LAN port	The cable that connects the unit to the LAN plugs in here.
5	remote port	Connects an Ethernet cable to allow access to the web interface of the unit or for CCVSR recording.
6	power jack	The cable from the DC power adapter connects here.

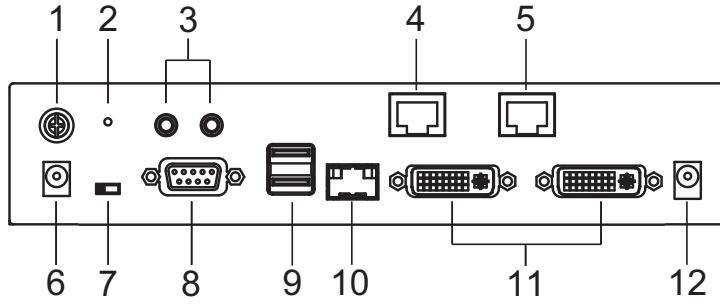
No.	Component	Description
7	function switch	Use this switch to set the unit's mode to: ◆ **Auto**: Shared (simultaneous) KVM control of the PC / workstation at the transmitter and receiver console.* ◆ **RS-232 Config**: The device is ready to be configured via serial commands through the RS-232 port. When connected to a KVM over IP Access Control Box (2XRT-0015G), users can enable / disable control privileges of the connected receivers. ◆ **Local**: Only the local transmitter has KVM control of the PC / workstation. The receiver's KVM access to the PC / workstation is locked. **Note:** In Auto mode, RS-232 and audio functions will work on the receiver but not on the transmitter.
8	RS-232 port	This RS-232 serial port is for connecting to a serial terminal.
9	USB ports (console)	The unit's USB keyboard and USB mouse plug into these ports.
10	SFP slot	The Gigabit Ethernet (GbE) optical fiber cable that connects the unit to the LAN plugs in here.
11	DVI-I out	The cable from the local DVI monitor plugs in here.
12	power jack	Connects a second power source for power redundancy.

RCMDVI40AT Front View



No.	Component	Description
1	audio ports	These mini stereo ports are for connecting to the speakers (green) and microphone (pink) ports of the PC / workstation.
2	KVM ports	The USB Type-B, DVI-D KVM cable supplied can link the transmitter to the PC / workstation to be controlled.
3	RS-232 port	This RS-232 serial port is for connecting to the PC / workstation for serial control or for connecting to a KVM over IP Access Control Box (2XRT-0015G).
4	remote / local LED	Lights green to indicate which side of the installation (local or remote) currently has KVM control of the PC / workstation.
5	LAN LED	This LED indicates the network status. ◆ Lights when connected to the LAN and blinks when the Ethernet connection is active: ◆ Orange: 10 Mbps ◆ Orange + Green: 100 Mbps ◆ Green: 1000 Mbps ◆ Off when not connected to the LAN.
6	power LED	Lights blue to indicate the unit is turned on.

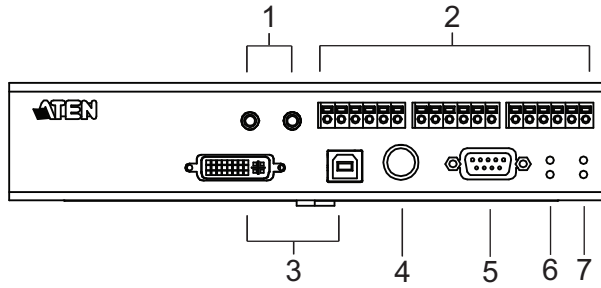
RCMDVI40AT Rear View



No.	Component	Description
1	grounding terminal	The wire used to ground the unit connects here.
2	reset button	This reset button 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 than three seconds resets the unit back to its factory default settings*. **Note:** The Reset to Factory Default function resets everything but the login information (username/password) to the factory default settings. To reset the login information, refer to *Reset All Information* on page 266.
3	audio ports	These mini stereo ports can connect to speakers (green) and a microphone (pink).
4	LAN port	The cable that connects the unit to the LAN plugs in here.
5	remote port	Connects an Ethernet cable to allow access to the web interface of the unit or for CCVSR recording.
6	power jack	The cable from the DC power adapter connects here.

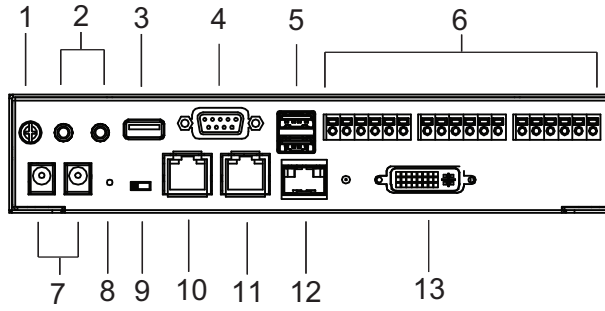
No.	Component	Description
7	function switch	Use this switch to set the unit's mode to: ◆ **Auto**: Shared (simultaneous) KVM control of the PC / workstation at the transmitter and receiver console.* ◆ **RS-232 Config**: The device is ready to be configured via serial commands through the RS-232 port. When connected to a KVM over IP Access Control Box (2XRT-0015G), users can enable / disable control privileges of the connected receivers. ◆ **Local**: Only the local transmitter has KVM control of the PC / workstation. The receiver's KVM access to the PC / workstation is locked. **Note:** In Auto mode, RS-232 and audio functions will work on the receiver but not on the transmitter.
8	RS-232 port	This RS-232 serial port is for connecting to a serial terminal.
9	USB ports (console)	The unit's USB keyboard and USB mouse plug into these ports.
10	SFP slot	The Gigabit Ethernet (GbE) optical fiber cable that connects the unit to the LAN plugs in here.
11	DVI-I out	The cable from the local DVI monitor plugs in here.
12	power jack	Connects a second power source for power redundancy.

RCMDVI00BT Front View



No.	Component	Description
1	audio ports	These mini stereo ports are for connecting to the speakers (green) and microphone (pink) ports of the PC / workstation.
2	DI / relay	Connects to stack light or temperature sensor.
3	KVM ports	The USB Type-B, DVI-D KVM cable supplied can link the transmitter to the PC / workstation to be controlled.
4	access control port	Connects to the KVM over IP Access Control Box (2XRT-0015G).
5	RS-232 port	This RS-232 serial port is for connecting to the PC / workstation for serial control or for connecting to a KVM over IP Access Control Box (2XRT-0015G).
6	remote / local LED	Lights green to indicate which side of the installation (local or remote) currently has KVM control of the PC / workstation.
7	power LEDs	Lights blue to indicate the unit is turned on.

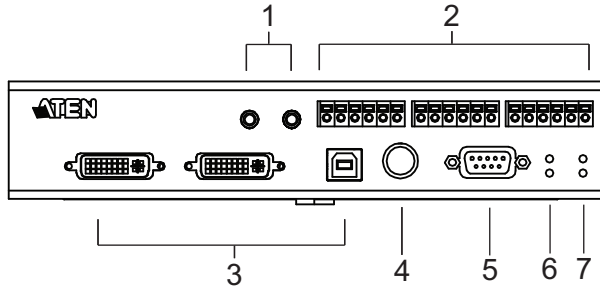
RCMDVI00BT Rear View



No.	Component	Description
1	grounding terminal	The wire used to ground the unit connects here.
2	audio ports	These mini stereo ports can connect to speakers (green) and a microphone (pink).
3	USB Type-A port	Connects to USB peripherals.
4	RS-232 port	This RS-232 serial port is for connecting to a serial terminal.
5	USB ports (console)	The unit's USB keyboard and USB mouse plug into these ports.
6	DO / relay	Connects to electric door lock or alarm.
7	power jacks	The cable from the DC power adapter connects here. Connect both power jacks to a power source for power redundancy.
8	reset button	This reset button 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 than three seconds resets the unit back to its factory default settings*. **Note:** The Reset to Factory Default function resets everything but the login information (username/password) to the factory default settings. To reset the login information, refer to *Reset All Information* on page 266.

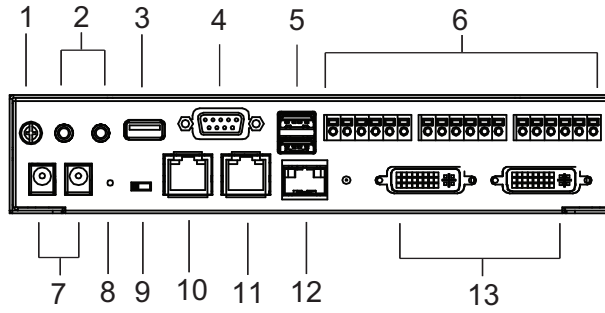
No.	Component	Description
9	function switch	Use this switch to set the unit's mode to: ◆ **Auto**: Shared (simultaneous) KVM control of the PC / workstation at the transmitter and receiver console.* ◆ **RS-232 Config**: The device is ready to be configured via serial commands through the RS-232 port. When connected to a KVM over IP Access Control Box (2XRT-0015G), users can enable / disable control privileges of the connected receivers. ◆ **Local**: Only the local transmitter has KVM control of the PC / workstation. The receiver's KVM access to the PC / workstation is locked. **Note:** In Auto mode, RS-232 and audio functions will work on the receiver but not on the transmitter.
10	remote port	Connects an Ethernet cable to allow access to the web interface of the unit or for CCVSR recording.
11	LAN port	The cable that connects the unit to the LAN plugs in here.
12	SFP slot	The Gigabit Ethernet (GbE) optical fiber cable that connects the unit to the LAN plugs in here.
13	DVI-I out	The cable from the local DVI monitor plugs in here.

RCMDVI40BT Front View



No.	Component	Description
1	audio ports	These mini stereo ports are for connecting to the speakers (green) and microphone (pink) ports of the PC / workstation.
2	DI / relay	Connects to stack light or temperature sensor.
3	KVM ports	The USB Type-B, DVI-D KVM cable supplied can link the transmitter to the PC / workstation to be controlled.
4	access control port	Connects to the KVM over IP Access Control Box (2XRT-0015G).
5	RS-232 port	This RS-232 serial port is for connecting to the PC / workstation for serial control or for connecting to a KVM over IP Access Control Box (2XRT-0015G).
6	remote / local LED	Lights green to indicate which side of the installation (local or remote) currently has KVM control of the PC / workstation.
7	power LEDs	Lights blue to indicate the unit is turned on.

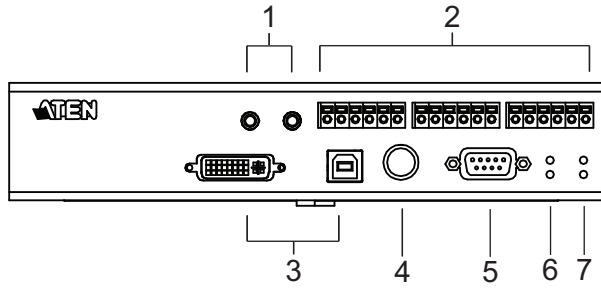
RCMDVI40BT Rear View



No.	Component	Description
1	grounding terminal	The wire used to ground the unit connects here.
2	audio ports	These mini stereo ports can connect to speakers (green) and a microphone (pink).
3	USB Type-A port	Connects to USB peripherals.
4	RS-232 port	This RS-232 serial port is for connecting to a serial terminal.
5	USB ports (console)	The unit's USB keyboard and USB mouse plug into these ports.
6	DO / relay	Connects to electric door lock or alarm.
7	power jacks	The cable from the DC power adapter connects here. Connect both power jacks to a power source for power redundancy.
8	reset button	This reset button 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 than three seconds resets the unit back to its factory default settings*. **Note:** The Reset to Factory Default function resets everything but the login information (username/password) to the factory default settings. To reset the login information, refer to *Reset All Information* on page 266.

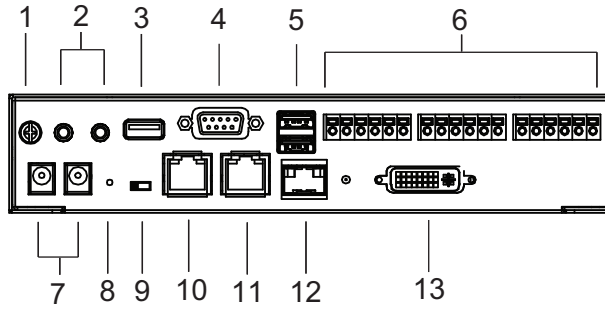
No.	Component	Description
9	function switch	Use this switch to set the unit's mode to: ◆ **Auto**: Shared (simultaneous) KVM control of the PC / workstation at the transmitter and receiver console.* ◆ **RS-232 Config**: The device is ready to be configured via serial commands through the RS-232 port. When connected to a KVM over IP Access Control Box (2XRT-0015G), users can enable / disable control privileges of the connected receivers. ◆ **Local**: Only the local transmitter has KVM control of the PC / workstation. The receiver's KVM access to the PC / workstation is locked. **Note:** In Auto mode, RS-232 and audio functions will work on the receiver but not on the transmitter.
10	remote port	Connects an Ethernet cable to allow access to the web interface of the unit or for CCVSR recording.
11	LAN port	The cable that connects the unit to the LAN plugs in here.
12	SFP slot	The Gigabit Ethernet (GbE) optical fiber cable that connects the unit to the LAN plugs in here.
13	DVI-I out	The cable from the local DVI monitor plugs in here.

RCMDVI50T Front View



No.	Component	Description
1	audio ports	These mini stereo ports are for connecting to the speakers (green) and microphone (pink) ports of the PC / workstation.
2	DI / relay	Connects to stack light or temperature sensor.
3	KVM ports	The USB Type-B, DVI-D KVM cable supplied can link the transmitter to the PC / workstation to be controlled.
4	access control port	Connects to the KVM over IP Access Control Box (2XRT-0015G).
5	RS-232 port	This RS-232 serial port is for connecting to the PC / workstation for serial control or for connecting to a KVM over IP Access Control Box (2XRT-0015G).
6	remote / local LED	Lights green to indicate which side of the installation (local or remote) currently has KVM control of the PC / workstation.
7	power LEDs	Lights blue to indicate the unit is turned on.

RCMDVI50T Rear View



No.	Component	Description
1	grounding terminal	The wire used to ground the unit connects here.
2	audio ports	These mini stereo ports can connect to speakers (green) and a microphone (pink).
3	USB Type-A port	Connects to USB peripherals.
4	RS-232 port	This RS-232 serial port is for connecting to a serial terminal.
5	USB ports (console)	The unit's USB keyboard and USB mouse plug into these ports.
6	DO / relay	Connects to electric door lock or alarm.
7	power jacks	The cable from the DC power adapter connects here. Connect both power jacks to a power source for power redundancy.
8	reset button	This reset button 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 than three seconds resets the unit back to its factory default settings*. **Note:** The Reset to Factory Default function resets everything but the login information (username/password) to the factory default settings. To reset the login information, refer to *Reset All Information* on page 266.

No.	Component	Description
9	function switch	Use this switch to set the unit's mode to: ◆ **Auto**: Shared (simultaneous) KVM control of the PC / workstation at the transmitter and receiver console.* ◆ **RS-232 Config**: The device is ready to be configured via serial commands through the RS-232 port. When connected to a KVM over IP Access Control Box (2XRT-0015G), users can enable / disable control privileges of the connected receivers. ◆ **Local**: Only the local transmitter has KVM control of the PC / workstation. The receiver's KVM access to the PC / workstation is locked. **Note:** In Auto mode, RS-232 and audio functions will work on the receiver but not on the transmitter.
10	remote port	Connects an Ethernet cable to allow access to the web interface of the unit or for CCVSR recording.
11	LAN port	The cable that connects the unit to the LAN plugs in here.
12	SFP slot	The Gigabit Ethernet (GbE) optical fiber cable that connects the unit to the LAN plugs in here.
13	DVI-I out	The cable from the local DVI monitor plugs in here.

This Page Intentionally Left Blank

Chapter 2
Hardware Setup

1. Important safety information regarding the placement of this device is found on page 247. 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.

Mounting

For convenience and flexibility, the transmitters can be mounted on system racks or on a wall.

Note: 1. Optional mounting options are available, refer to *Optional Rack Mount* on page 257 for more information.

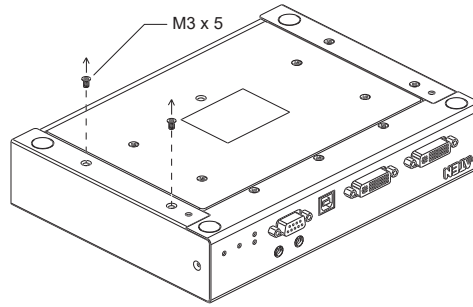
2. It is highly recommended to mount the RCMDVI00AT / RCMDVI40AT / RCMDVI00BT / RCMDVI40BT / RCMDVI50T on a system rack or on a wall and avoid stacked setup to ensure proper ventilation

The following sections will demonstrate how to mount the transmitters with the included mounting kit.

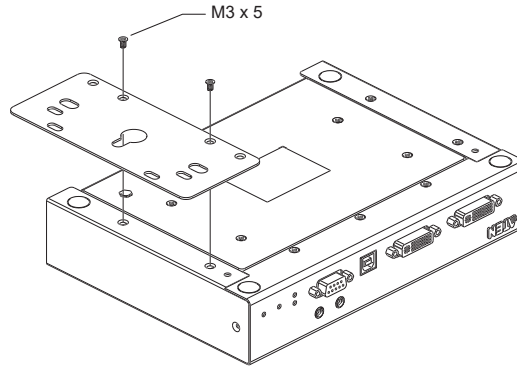
Attaching the Bracket

Follow the steps below to attach the mounting bracket to the unit, exemplified using KE6940T:

1. Unscrew the screws from the side shown in the diagram below:



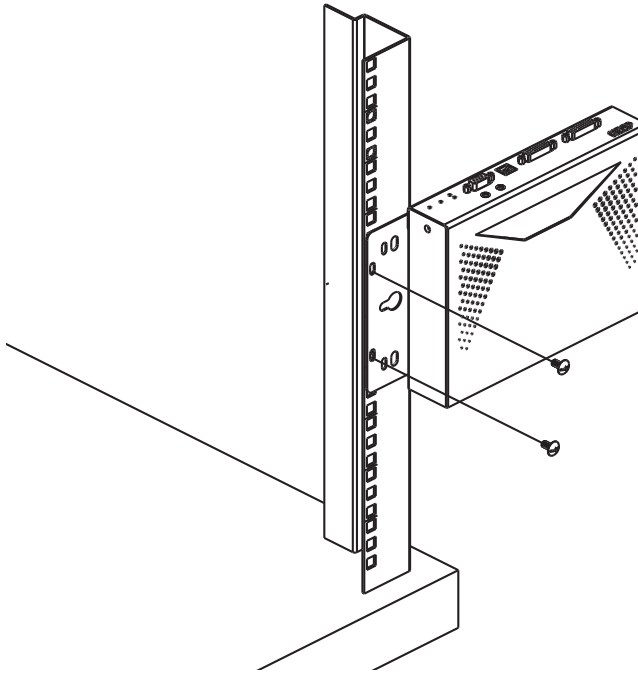
2. Use the screws from step 1 to screw the mounting bracket to the bottom of the Transmitter as shown below:



Rack Mount

Note: The diagram below is exemplified using KE6940T.

Screw the bracket into a convenient location on the rack.

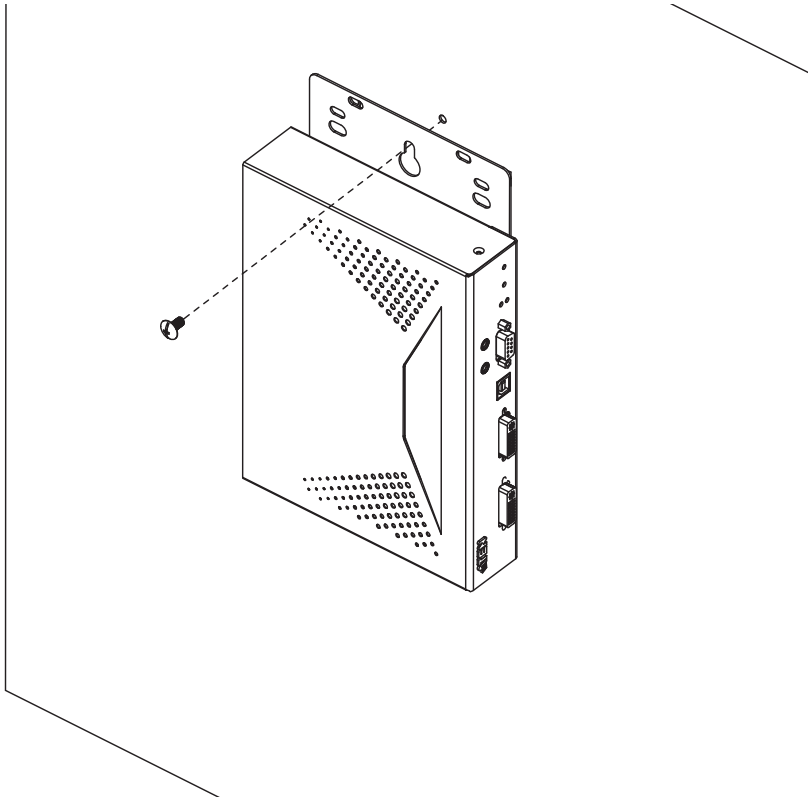


Note: Rack screws are not provided. We recommend that you use M5 x 12 Phillips Type I cross recessed screws.

Wall Mount

Note: The diagram below is exemplified using KE6940T.

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



RCMDVI00AT / RCMDVI40AT Point-to-Point Installation

Setting up the RCMDVI00AT / RCMDVI40AT system in a point-to-point configuration is simply a matter of plugging in the cables. Since this is a transmitter-receiver setup, we will demonstrate using RCMDVI40AT-KE6940AR.

Note: 1. In a point-to-point configuration, no administrator setup is necessary.

2. It is highly recommended to mount RCMDVI00AT / RCMDVI40AT on a rack or wall and avoid stacked setup to ensure proper ventilation.

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

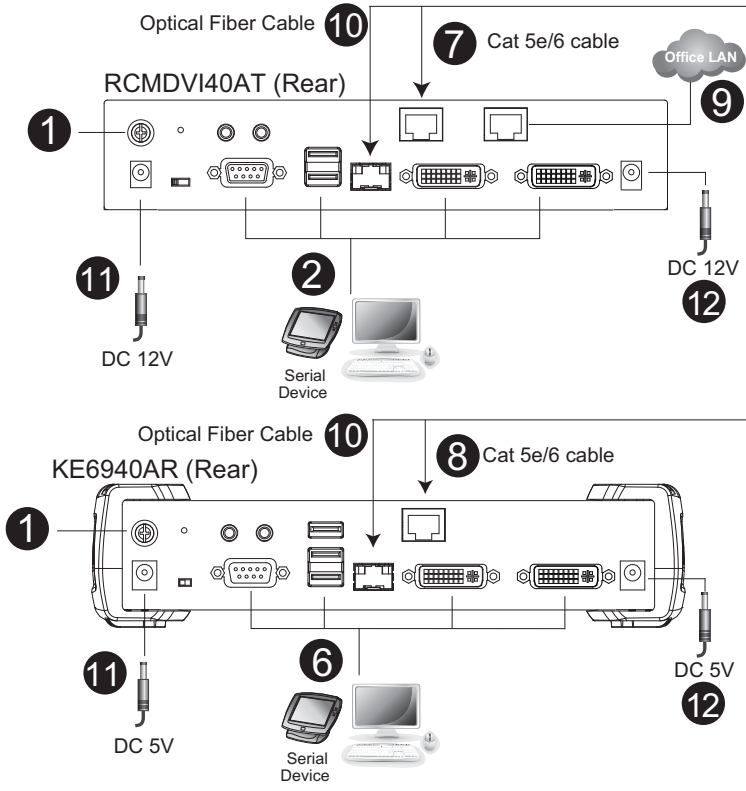
1. Use a grounding wire to connect the unit's grounding terminal to a suitable grounded object.
2. Plug the mouse, keyboard, DVI monitor(s), and serial devices into the unit's console ports.
3. Connect the KVM cable (DVI-D, USB, audio) and the DVI-D cable (RCMDVI40AT only) provided into the KVM ports on the front of the unit.
4. Connect the other end of the KVM cable (DVI-D, USB, audio) and the DVI-D cable (RCMDVI40AT only) into the keyboard, video, mouse, speaker and microphone ports on the PC / workstation.
5. For control of serial devices, connect the RS-232 port on the front of the transmitter to a serial port on the computer.
6. Plug the mouse, keyboard, DVI monitor(s), and serial devices into the console ports of the receiver (KE6940AR is used as the example here)[1].
7. Connect a Cat 5e/6 cable to the transmitter's LAN port.
8. Connect the other end of the Cat 5e/6 cable to the receiver's LAN port.
9. To allow remote access to the web interface of the transmitter or for CCVSR recording, use an Ethernet cable to connect its remote port to a network.

10. (Optional) Instead of connecting through the LAN ports, you can choose to connect the extenders through the SFP slots. To do so, plug SFP modules into the transmitter and receiver's SFP slots, then connect each end of the Gigabit Ethernet (GbE) optical fiber between the SFP modules[2].
11. Connect the transmitter and receiver to power, thereby turning them on, by plugging the power adapters into AC power sources and plug the other ends into the transmitter and receiver's power jacks.
12. (Optional) For power redundancy, connect another power adapter (available for purchase separately), connected to an AC power source, to the power jack of each transmitter / receiver.
13. Power on the PC / workstation.

Note: 1. For advanced features when connecting a keyboard or mouse with special functions, see *USB Mode*, page 133.

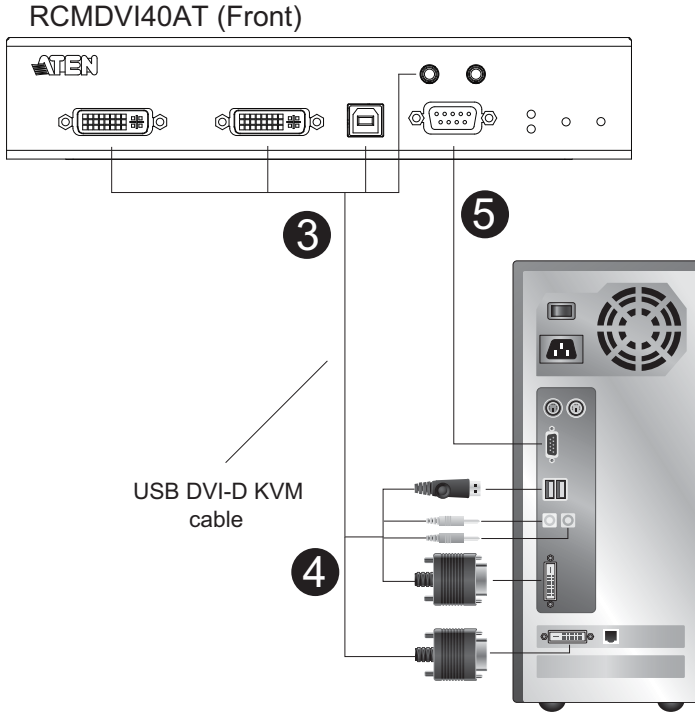
2. The SFP module 2A-136G / 2A-137G is sold separately. Contact your ATEN dealer for product information.

RCMDVI40AT Point-to-Point Installation 1 of 2



Note: The diagram above shows the RCMDVI40AT setup with a KE6940AR. The RCMDVI00AT-KE6900AR installation is the same except with one less DVI monitor.

RCMDVI40AT 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).

RCMDVI00AT / RCMDVI40AT LAN Installation

Setting up the units on a network allows point-to-point, point-to-multipoint, and multipoint-to-multipoint computer (PC and/or workstation) to console operation by connecting multiple extender devices on the same TCP/IP LAN. Prior to setup, we recommend laying out the plans for your RCM/KE installation using our performance guide (see *Keys to Network Performance*, page 271).

A few points to note during your setup:

- The units are preconfigured with factory-default network settings. If you install only one set of RCM/KE series units, you do not need to change these default network settings. See *Default IP Addresses*, page 47, for further details.
- In a network setup with multiple units, each transmitter and receiver must be configured with a unique IP address. See *Network Configuration*, page 46, for further details.
- We recommend using 1000-Mbps Gigabit Ethernet switches (wire speeds, non-blocking with 1 Gbps / 1.5 Mpps performance per port) between RCM/KE series devices installed on different LAN segments. 10/100 Mbps switches might cause poor performance.
- 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.
- If your network uses cascaded switches, please check to ensure the data throughput is sufficient.
- To get the best performance, we suggest that you create a private network for RCM/RCM/KE devicess, as they are bandwidth-intensive devices.
- The unit supports network redundancy. Where both LAN and SFP ports are connected, a network redundancy is established. Please note that if you use copper SFP modules, the module has to be removed for the unit to switch to the LAN port's network.
- For USB keyboards / mouses with special designs and/or advanced functions, see *USB Mode*, page 133.
- Make sure that all the equipment is powered off before the installation.

The installation is similar to that of *RCMDVI00AT / RCMDVI40AT Point-to-Point Installation* on page 31, with the difference in connecting the transmitter

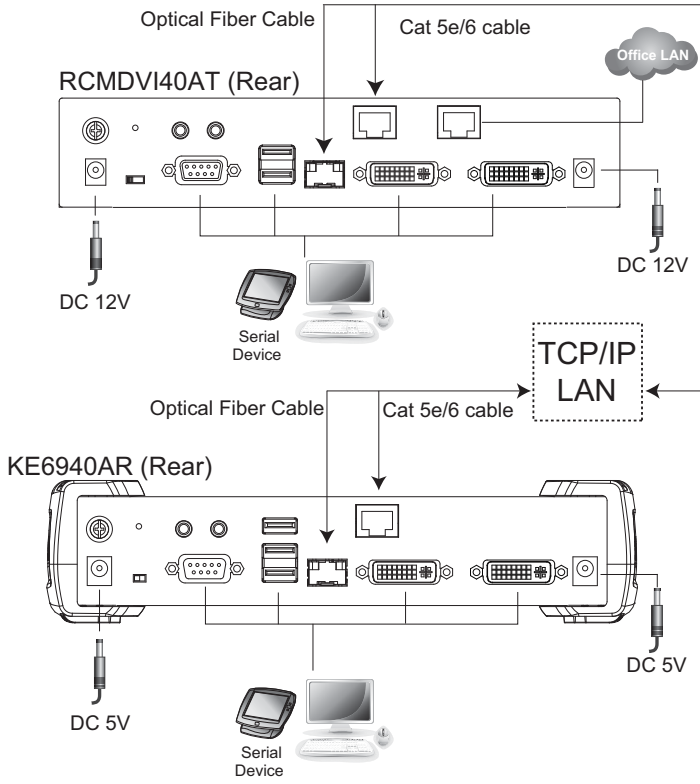
and the receiver to a local area TCP/IP network. Refer to the diagrams on the following page and connect accordingly.

Repeat these steps for each transmitter and receiver you wish to install on the network then power on the computer(s).

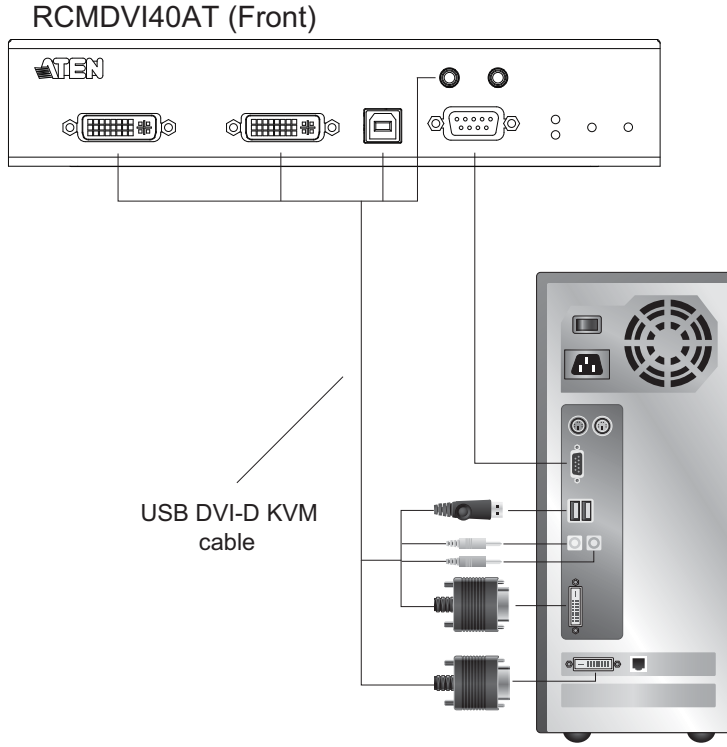
Note: 1. If you wish to use CCVSR and/or remote access with WinClient / JavaClient, you will still need to connect the remote port of the RCMDVI00AT / RCMDVI40AT to an Office LAN.

2. It is highly recommended that the units are mounted on a system rack or on a wall and avoid stacked setup to ensure proper ventilation

RCMDVI00AT / RCMDVI40AT Network Installation Diagram 1 of 2



RCMDVI00AT / RCMDVI40AT Network Installation Diagram 2 of 2



RCMDVI00BT / RCMDVI40BT / RCMDVI50T Point-to-Point Installation

Setting up the RCMDVI00BT / RCMDVI40BT / RCMDVI50T system in a point-to-point configuration is simply a matter of plugging in the cables. Since this is a transmitter-receiver setup, we will demonstrate using RCMDVI40BT-KE6910R.

Note: 1. In a point-to-point configuration, no administrator setup is necessary.

2. It is highly recommended to mount RCMDVI00BT / RCMDVI40BT / RCMDVI50T on a rack or wall and avoid stacked setup to ensure proper ventilation.

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

1. Use a grounding wire to connect the unit's grounding terminal to a suitable grounded object.
2. Plug the mouse, keyboard, DVI monitor(s), and serial devices into the unit's console ports.
3. Connect the KVM cable (DVI-D, USB, audio) and the DVI-D cable (RCMDVI40AT only) provided into the KVM ports on the front of the unit.
4. Connect the other end of the KVM cable (DVI-D, USB, audio) and the DVI-D cable (RCMDVI40BT only) into the keyboard, video, mouse, speaker and microphone ports on the PC / workstation.
5. For control of serial devices, connect the RS-232 port on the front of the transmitter to a serial port on the computer.
6. Connect the KVM over IP Access Control Box (2XRT-0015G) for access control.
7. Connect the stack light or temperature sensor for safety purposes.
8. Plug the mouse, keyboard, DVI monitor(s), and serial devices into the console ports of the receiver (KE6910R is used as the example here)[1].
9. Connect a Cat 5e/6 cable to the transmitter's LAN port.
10. Connect the other end of the Cat 5e/6 cable to the receiver's LAN port.

11. To allow remote access to the web interface of the transmitter or for CCVSR recording, use an Ethernet cable to connect its remote port to a network.

12. (Optional) Instead of connecting through the LAN ports, you can choose to connect the extenders through the SFP slots. To do so, plug SFP modules into the transmitter and receiver's SFP slots, then connect each end of the Gigabit Ethernet (GbE) optical fiber between the SFP modules[2].

13. Connect the electric door lock or alarm security purposes.

14. Connect the transmitter and receiver to power, thereby turning them on, by plugging the power adapters into AC power sources and plug the other ends into the transmitter and receiver's power jacks.

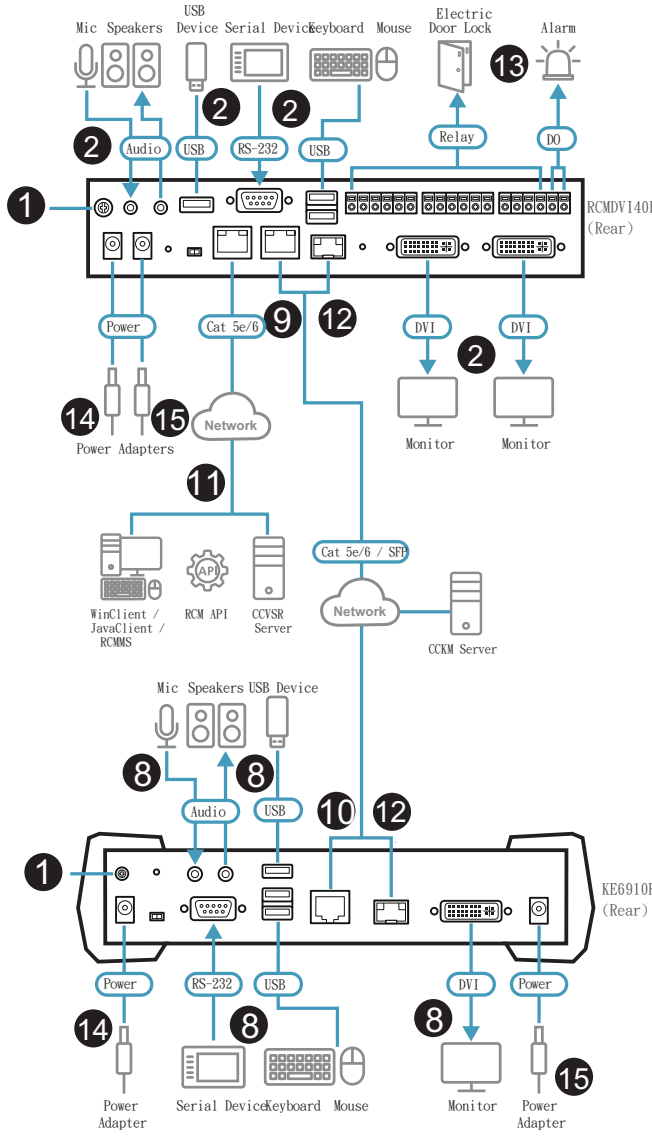
15. (Optional) For power redundancy, connect another power adapter (available for purchase separately), connected to an AC power source, to the power jack of each transmitter / receiver.

16. Power on the PC / workstation.

Note: 1. For advanced features when connecting a keyboard or mouse with special functions, see *USB Mode*, page 133.

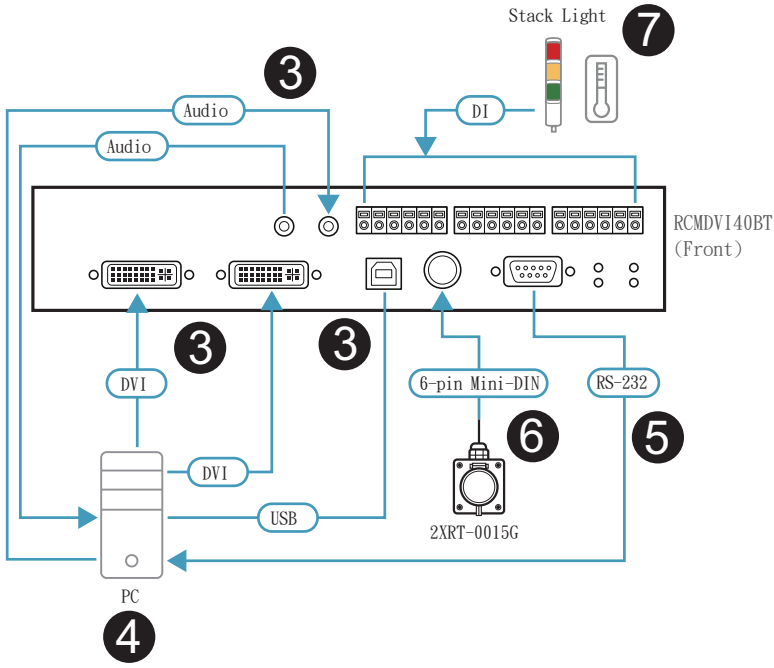
2. The SFP module 2A-136G / 2A-137G is sold separately. Contact your ATEN dealer for product information.

RCMDVI40BT Point-to-Point Installation 1 of 2



Note: The diagram above shows the RCMDVI40BT setup with a KE6910R. The RCMDVI00AT-KE6900AR installation is the same except with one less DVI monitor.

RCMDVI40BT 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).

RCMDVI00BT / RCMDVI40BT / RCMDVI50T LAN Installation

Setting up the units on a network allows point-to-point, point-to-multipoint, and multipoint-to-multipoint computer (PC and/or workstation) to console operation by connecting multiple extender devices on the same TCP/IP LAN. Prior to setup, we recommend laying out the plans for your RCM/KE installation using our performance guide (see *Keys to Network Performance*, page 271).

A few points to note during your setup:

- The units are preconfigured with factory-default network settings. If you install only one set of RCM/KE series units, you do not need to change these default network settings. See *Default IP Addresses*, page 47, for further details.
- In a network setup with multiple units, each transmitter and receiver must be configured with a unique IP address. See *Network Configuration*, page 46, for further details.
- We recommend using 1000-Mbps Gigabit Ethernet switches (wire speeds, non-blocking with 1 Gbps / 1.5 Mpps performance per port) between RCM/KE series devices installed on different LAN segments. 10/100 Mbps switches might cause poor performance.
- 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.
- If your network uses cascaded switches, please check to ensure the data throughput is sufficient.
- To get the best performance, we suggest that you create a private network for RCM/RCM/KE devicess, as they are bandwidth-intensive devices.
- The unit supports network redundancy. Where both LAN and SFP ports are connected, a network redundancy is established. Please note that if you use copper SFP modules, the module has to be removed for the unit to switch to the LAN port’s network.
- For USB keyboards / mouses with special designs and/or advanced functions, see *USB Mode*, page 133.
- Make sure that all the equipment is powered off before the installation.

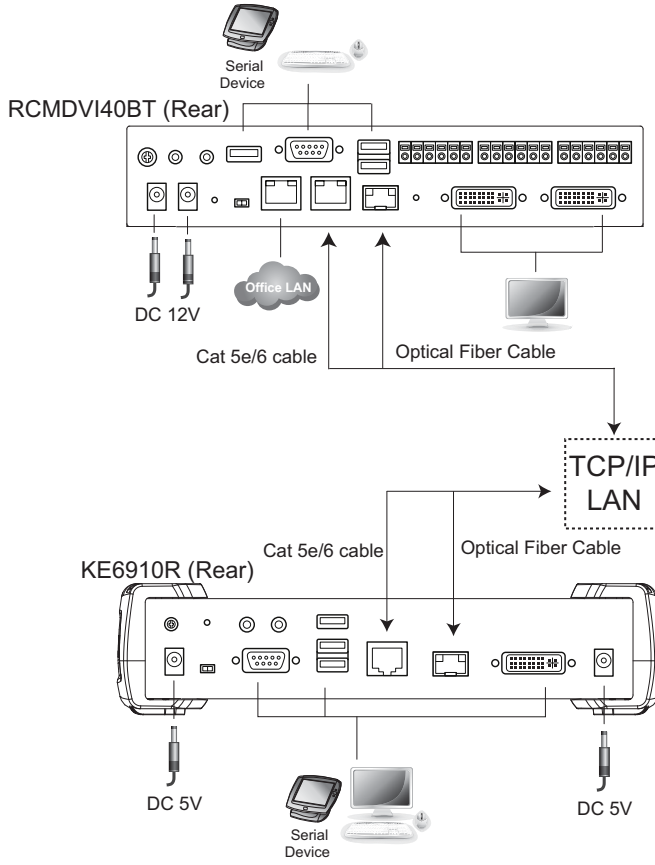
The installation is similar to that of *RCMDVI00BT / RCMDVI40BT / RCMDVI50T Point-to-Point Installation* on page 38, with the difference in connecting the transmitter and the receiver to a local area TCP/IP network. Refer to the diagrams on the following page and connect accordingly.

Repeat these steps for each transmitter and receiver you wish to install on the network then power on the computer(s).

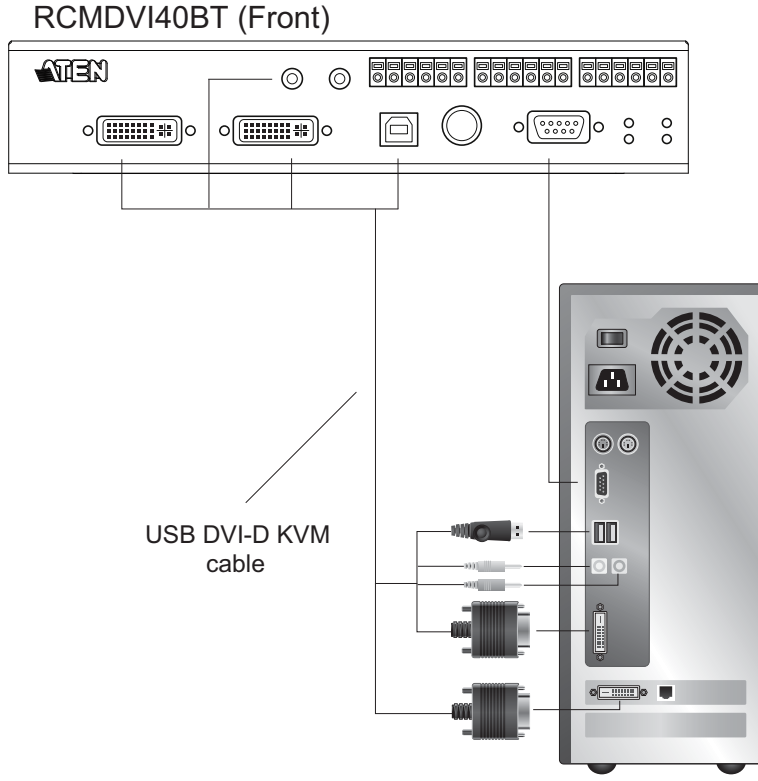
Note: 1. If you wish to use CCVSR and/or remote access with WinClient / JavaClient, you will still need to connect the remote port of the RCMDVI00BT / RCMDVI40BT / RCMDVI50T to an Office LAN.

2. It is highly recommended that the units are mounted on a system rack or on a wall and avoid stacked setup to ensure proper ventilation

RCMDVI00BT / RCMDVI40BT / RCMDVI50T Network Installation Diagram 1 of 2



RCMDVI00BT / RCMDVI40BT / RCMDVI50T Network Installation Diagram 2 of 2



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 263.

Note: 1. Both devices are preconfigured with factory-default network settings. If you install only one set of RCM/KE series units, you do not need to change these default network settings. See *Default IP Addresses*, page 47, 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 46, for further details.

3. We recommend using 1000 Mbps Gigabit Ethernet switches (wire speeds, non-blocking with 1 Gbps / 1.5 Mpps performance per port) between devices installed on different LAN segments. 10/100 Mbps 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 that you create a private network for the RCM/KE 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 *RCMDVI00AT / RCMDVI40AT LAN Installation*, page 35 and see *RCMDVI00BT / RCMDVI40BT / RCMDVI50T LAN Installation*, page 42).

2. From the KE receiver, press the **[Scroll Lock]** key twice to invoke the OSD.

3. Select the *receiver* 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 RCM/KE devices. Key in a valid unique IP address.

     Note: See *Default IP Addresses*, page 47, for the preconfigured factory-default settings.

   - *Subnet Mask* — sets the subnet mask for the RCM/KE devices. Key in a valid subnet mask value.

     Note: The default setting is 255.255.255.0

   - *Default Gateway* — sets the default gateway for the RCM/KE devices. Key in a valid default gateway.
6. Click **Save**.

Exit OSD

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 receiver can connect to the transmitter to access the PC / workstation remotely (see *OSD Matrix Mode*, page 73 for instructions).

Default IP Addresses

The preconfigured factory-default IP addresses for the RCM/KE series devices are as follows:

transmitters – `192.168.0.61`

receivers – `192.168.0.60`

RCM I/O Ports

The following table provides the port values used by RCM/KE series devices.

Device	Port	Number
KVM over IP Matrix Manager (TCP)	HTTP	8080
	HTTPS	8443
	Device TCP	9110
	CLI	9111
	Redundancy	9120
	Database Service	1527
KVM over IP Matrix Manager (UDP)	Port	9110
	Broadcast	9000
RCM/KE TX/RX Device (TCP)	Manager	9110
	Service	9000
	Telnet	23
	SSH	22
RCM/KE TX Device (TCP)	VM	9001
	vUSB	9002
	Serial	9003
	USB Access Mode	9009
KE RX Device (TCP)	CLI	9130
RCM/KE KE TX/RX Device (UDP)	Manager	9110
	Service	9000
	Array Mode	9120
	Video	0xFE00(65024) - 0xFE03(65027)
	Audio	0xFE04(65028) - 0xFE05(65029)

Chapter 3
API Functions

Overview

This chapter takes users through some of the most commonly-used API functions that can be used to access and configure the RCM KVM over IP Transmitters based on 32-bit/64-bit Windows Dynamic-link Library (DLL).

Note: For a complete list of the RCM API functions and/or the DLL-related materials available, please contact your local dealer.

Starting an API Session

Before implementing an API function to the RCM device, the user must first start an API session by entering the following:

`StartSession(<IP address>,1,<username>,<password>)`

Example:
`StartSession(192.168.0.60,1,administrator,password)`

Then press [Enter].

The ID of the API session — *SID* — is returned, which is needed for implementing any API function to the device via the session:

Example: *4*

Note: A return value < 0 indicates an error. Please refer to the *Error Code Specification* document for the details of the errors represented, or look up its related description by using the error description search function, see *Error Description Search*, page 53.

To end the API session, type the following then press [Enter]:

`EndSession(<SID>)`

Example: `EndSession(4)`

0 is returned, representing the successful termination of the API session.

Access Management

Local Console Access

Function	Description	Example
DisableLocalConsole(<SID>)	Disables local console access.	DisableLocalConsole(*4*)
EnableLocalConsole(<SID>)	Enables local console access.	EnableLocalConsole(*4*)

Remote Port Access

Function	Description	Example
LockClientLogin(<SID>)	Prohibits remote access to the remote port. Returned value of '0' = Success	LockClientLogin(*4*)
UnlockClientLogin(<SID>)	Allows remote access to the remote port. Returned value of '0' = Success	UnlockClientLogin(*4*)
SetPortAccessMode(1,<access mode>)	Sets the access mode for the remote port. *0* = full access *1* = view only *2* = denied access	SetPortAccessMode(1,*0)*

Checking Access Control Box Pushbutton

Function	Description	Example
GetLocalPushButtonStatus(<SID>)	Shall be used in conjunction with the ATEN Access Control Box, checks the current pushbutton status. *0* = released *1* = pressed	GetLocalPushButtonStatus(*4*)

Remote Monitoring

The following sequence of functions are used for capturing the image of the RCM device for remote monitoring:

1. Type the following to set the parameters for capturing images from the RCM device, including its quality, width, height, and time interval:

   ```
   SetCaptureParams(<SID>,1,<image quality, 20-95>,<image
   width, in pixels>,<image height, in pixels>,1,<interval,
   0-1000 ms>)
   ```

Function Example	Returned Value
SetCaptureParams(*4*,1,*95*,*1920*,*1080*,1,*1000*)	*0* = success

2. Type the following to check if there are any new updates/changes to the image since the last time interval:

   ```
   GetCaptureStatus(<SID>,1)
   ```

Function Example	Returned Value
GetCaptureStatus(*4*,1)	*1* = new updates/changes *0* = no updates/changes

3. Type the following to get the buffer size of the image captured:

   ```
   GetCaptureBufferSize(<SID>,1)
   ```

Function Example	Returned Value
GetCaptureBufferSize(*4*,1)	> *0* = the buffer size *0* = pending

4. Type the following to get the data of the image captured:

   ```
   GetCaptureDat(<SID>,1,<pointer to a buffer of
   image>,<buffer size>,dw,dh)
   ```

Function Example	Returned Value
GetCaptureDat(*4*,1,*00*,*2073600*,dw,dh)	> *0* = success

Remote Access

Function	Description	Example
StartViewer(<SID>,1)	Opens an internal viewer for remote access.	StartViewer(*4*,1)
CloseViewer(<SID>,1)	Closes the internal viewer for remote access.	CloseViewer(*4*,1)

OCR Functions

■ Sample Image Compare

Function	Description	Example
OCR_FastFindSamplePicture(<SID>,1,<horizontal position *x*>,<vertical position *y*>,<width>,<height>,<lpSampleFileName.*bmp*>)	Compares a specified region of the device's image with a sample image. *0* = success	*1*OCR_FastFindSamplePicture(*4*,1,*0*,*0*,*1920*,*1080*,*sample.bmp*)

■ Read Text

Function	Description	Example
ReadTextFromZoneMemEx(<SID>,1,<horizontal position *x*>,<vertical position *y*>,<width>,<height>,<pointer to *memory buffer of text*>,<size of *memory buffer*>,<font type, based on *ocrsetting.ini*>,<allowed ambiguity threshold; -1 = automatic detection>)	Gets texts from a specified region of the device's image.	*1*OCR_ReadTextFromZoneMemEx(*4*,1,*0*,*0*,*1920*,*1080*,*pointer*,sizeof(*pointer*),*-1*)

Other API Functions

■ Set Mouse Mode

Function	Description	Example
SetMouseMode(<SID>,1,<mouse mode, 0/1 = manual/automatic)	Sets the mouse mode to manual or automatic.	SetMosueMode(*4*,1,*1*)

■ Get Remote Session Info

Function	Description	Example
GetSessionByPort(<SID>,1,lpBuf,<lpBuf size>)	Gets the session list information currently accessing the RCM device.	GetSessionByPort(*4*, 1,lpBuf,*1024*64*)

■ Kill Sessions by User Account

Function	Description	Example
KillSessionByName(<SID>,<username>,<username size>)	Terminates sessions currently accessed by the specified user.	KillSessionByName(*4*,*nicholas*,*8*2*)

■ Kill Remote Port Sessions

Function	Description	Example
KillSessionByPort(<SID>,1,<port list>,<port list length>)	Terminates all sessions currently accessing the remote port.	KillSessionByPort(*4*,1,*"\x01"*,*1*)

■ Sets Denied Access Prompt Message

Function	Description	Example
SetMessageByPort(<SID>,1,<prompt message, max. 30 characters>,<message length>)	Sets a prompt message for notifying users without access rights to the remote port.	SetMessageByPort(*4*, 1,*access denied*,*13*2)

■ Error Description Search

Function	Description	Example
GetErrorDescription(<error code>)	Searches for error description by a specified returned error value.	GetErrorDescription(*-9*)

For a complete list of the RCM API functions, please contact your local dealer.

This Page Intentionally Left Blank

Chapter 4
OSD Operation

Overview

This chapter provides instructions to configure and operate KE Series devices using the local On Screen Display (OSD). To configure the network settings with the OSD, see *Network Configuration*, page 46.

Invoking the OSD

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

To invoke the OSD, press the OSD pushbutton on the front of the receiver, or tap the **[Scroll Lock**] key on the keyboard twice. The *OSD* main appears.

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. To change the OSD hotkeys, see page 72.

3. If the keyboard/mouse doesn't work when the OSD is invoked, see *USB Mode*, page 133.

Touch Screen Calibration

If you're using a touch screen monitor and the OSD appears off center, you can use the blinking + at the corners to adjust the position of the OSD.

OSD Hotkeys

The OSD hotkeys navigate the receiver's OSD screens. The hotkeys work after logging in from the *System Login* screen (see page 73) but not the *OSD Configuration* screen. Pressing a hotkey will immediately take you to the corresponding OSD screen.

Hotkey	OSD Screen	Page
[F1]	Connections Page 1 in List Mode	74
[F2]	Connections Page 1 in Array Mode	77
[F3]	Profile Page 1	78
[F5]	Push Content Page 1	79
[F6]	Pull Content Page 1	81
[F7]	Receiver > Properties	60
[F8]	User Preferences	72
[F9]	OSD Login Screen (logs user off)	73

Users can also use the [Page Up] and [Page Down] keys to jump to the previous and next configuration pages.

Non-OSD Hotkeys

The following are the hotkeys that can be used without entering the OSD screen:

Reverting to Previous

Users can use the [Alt] + [K] hotkey to switch back to the transmitter channel previously accessed.

Hotkey Mode

The Hotkey Mode allows users to quickly switch from one transmitter to another. Either press [Num Lock] + [-] or [Ctrl] + [F12] to enter Hotkey Mode.

Once in Hotkey Mode, you can use the [Next Arrow] and [Previous Arrow] keys to quickly switch between different transmitters. You can also press a [Number Key] + [S] / [O] / [E] / [V] to access a transmitter based on its order number in Favorites (see page 75) by Share / Occupy / Exclusive / View Only mode.

Microphone Hotkey

You can switch microphone access between receivers with a hotkey:

1. Press and hold down **[Num Lock]**.
2. Press and release **[-]**.
3. Release **[Num Lock]**.
4. Press **1**.

Press the **Esc** key to cancel.

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, the system will prompt you to change the password.

The OSD components are described in the table below:

No.	Item	Description
1	Receiver	Select this radio button, enter a password, and click Configure to enter the *Receiver Configuration* screen.

No.	Item	Description
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	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 Connection	Clicking this button exits the OSD and returns you to the computer's video display.

First-time Login

If you are the administrator, and are logging in for the first time (Receiver or User Preference radio button), use the default password: *password*).

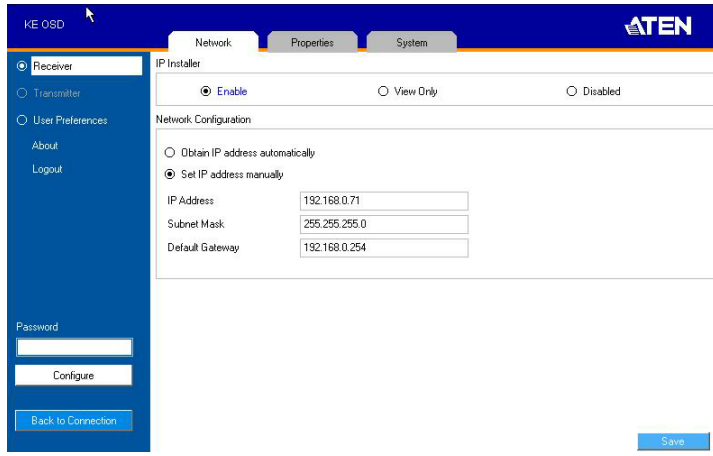
For security purposes, the system will prompt you to change the login password immediately as shown below:

Click **OK** and change the password in the dialog box shown below:

Enter the password and confirm it in the next field. The password must be different from your original password.

Receiver Configuration

Select the *Receiver* radio button and click **Configure** to login, the Network tab appears:



Network

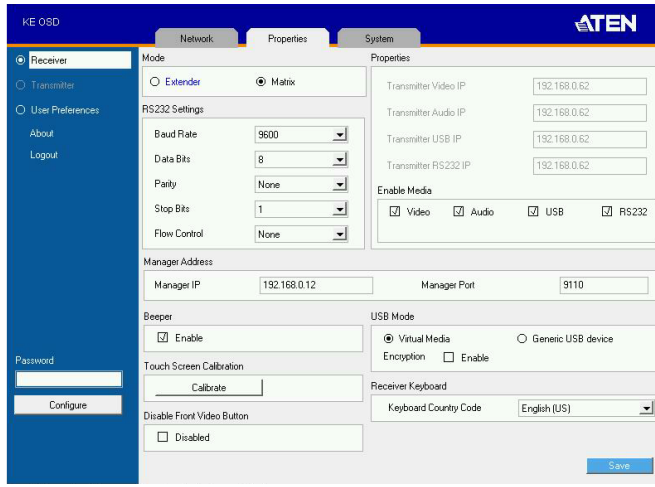
The Network tab allows you to configure the receiver's IP address settings:

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 263 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 46.

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

Properties

The *Properties* tab allows you to configure the receiver's settings.



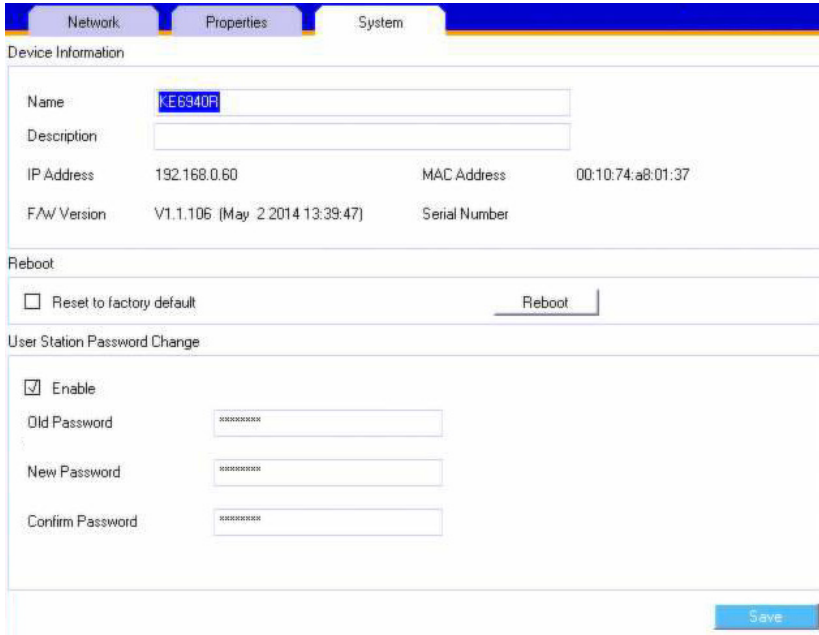
Item	Description
Mode	Select **Extender** mode for simple one-to-one (transmitter to receiver) setups that are managed with the receiver's OSD menu. Select **Matrix** mode to manage devices and connections from the KVM over IP Matrix Manager web GUI. This mode is for advanced administration of Transmitter to receiver connections (see *Browser / Telnet Operation*, page 93).
Properties	If you selected **Extender** mode (above) set the RCM transmitter's IP address as the source of video, audio, USB, and RS-232 source signals, to be sent to the receiver. If you selected **Matrix** mode (above) the *Properties* will be grayed out. Use Channels to configure the transmitter connections (see *Browser / Telnet Operation*, page 93).
RS-232 Settings	Configure the serial device settings for the receiver. The default settings are: Baud Rate: 9600 Parity: None Data Bits: 8 bits Stop bits: 1 bit Flow Control: None

Item	Description
Enable Media	Select which type of media the receiver can stream from transmitters: video, audio, USB, and RS-232.
Manager Address	Set the **IP** address and **Port** number of the PC running the KVM over IP Matrix Manager. The default port number is 9110.
Beeper	Check this box to allow the receiver to sound a beep when configuration changes are made to it.
Touch Screen Calibration	Use this button to calibrate the surface of a USB touch screen connected to the unit. When the calibration screen appears, touch the flashing + symbol at the corners until the process is complete.
USB Mode	Select the type of USB device connected to the USB ports: **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. When receivers connected to the same transmitter mount or unmount USB disk drives, the keyboard and mouse operations will experience a brief delay. Transmitters can support up to 12 virtual media connections at the same time (keyboard/mouse included). **vUSB (Generic USB device)**: 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. In this mode, RCMDVI00AT / RCMDVI40AT / RCMDVI00BT / RCMDVI40BT / RCMDVI50T transmitters supports up to 5 USB connections. **Encryption**: Check this box to encrypt USB drives plugged into the USB ports.
Receiver Keyboard	Use the Keyboard Country Code drop-down menu to select the receiver's language keyboard for use in the OSD.
Disable front video button	You can enable or disable the function (select video mode or graphic mode) of the video pushbutton on the front of the receiver. Check **Disable** to disable. Uncheck **Disable** to enable.

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

System

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

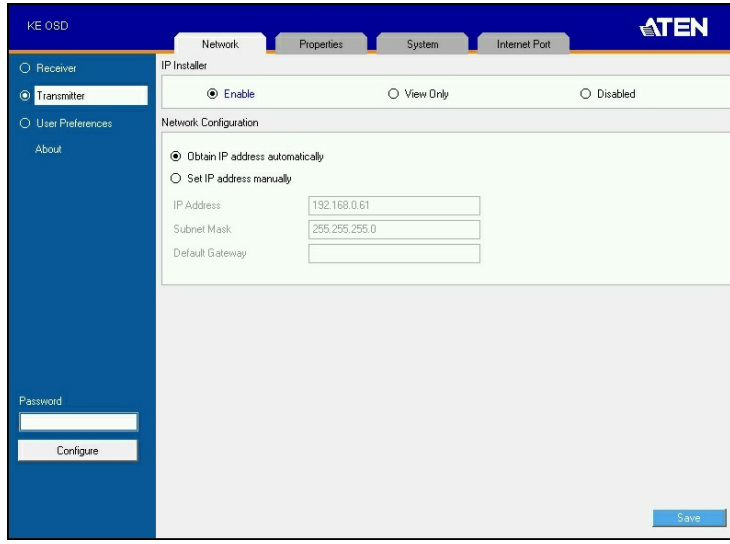


Item	Description
Device Information	Enter the **Name**, and **Description** of the receiver. It also displays the *IP Address*, *MAC Address*, *F/W Version*, *and Serial Number* of the receiver.
Reboot	Check the box and click **Reboot** to reset the receiver's settings back to the factory default. All custom settings (except for login account settings) will be lost.
Receiver Password Change	Check **Enable** to require a password for access to the receiver'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

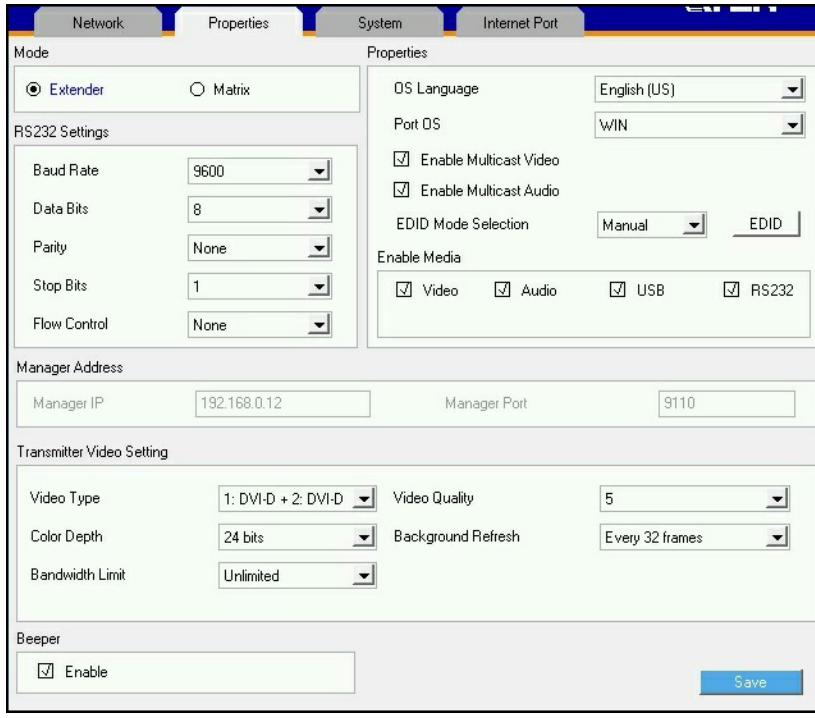
The *Network* tab allows you to configure the Transmitter's IP address settings:

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 263 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 46.

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 receiver) setups that are managed with the receiver's OSD menu. Select **Matrix** mode to manage devices and connections from the KVM over IP Matrix Manager web GUI. This mode is for advanced administration of transmitter to receiver connections (see *Browser / Telnet Operation*, page 93).

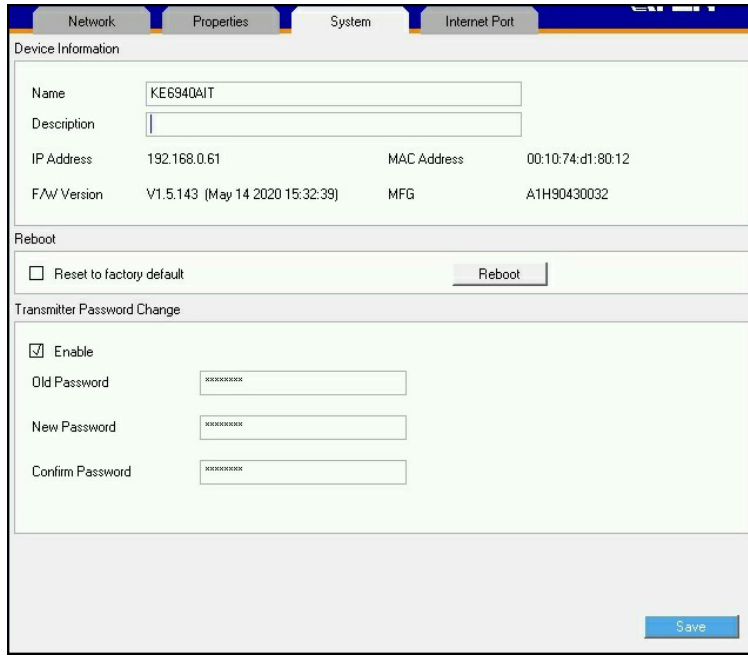
Item	Description
Properties	**Port OS:** Use the drop-down menu to select the operating system of the computer connected to the transmitter. **OS Language:** Use the drop-down menu to select the operating system language of the computer connected to the transmitter. **Enable Multicast Video:** Check this box to allow a broadcast of the transmitter's video signal to be sent out to multiple receivers. **Enable Multicast Audio:** Check this box to allow a broadcast of the transmitter's audio signal to be sent out to multiple receivers. **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. When *Manual* or *Remix* is selected, the receiver's OSD will have a button allowing the local EDID setting to be configured for the connection. 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 the ATEN default EDID to use the best common resolution for all displays. ◆ **Manual**: Manually set the EDID configuration from the Connections Page (see page 74). ◆ **Remix**: Manually checks the EDID of all connected displays and the ATEN default EDID to use the best common resolution for all displays (see page 74).
Enable Media	Select which type of media the transmitter can stream to receivers: video, audio, USB, and RS-232.
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 KVM over IP Matrix Manager. 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). This option is available for KE6900, KE6940, KE6900A, KE6940A units and will be grayed out for other models. **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 *Access Type*, page 128). If there is no activity from the receiver occupying the port for the amount of time set here, the Receiver is timed out and the port is released. The first Receiver 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:

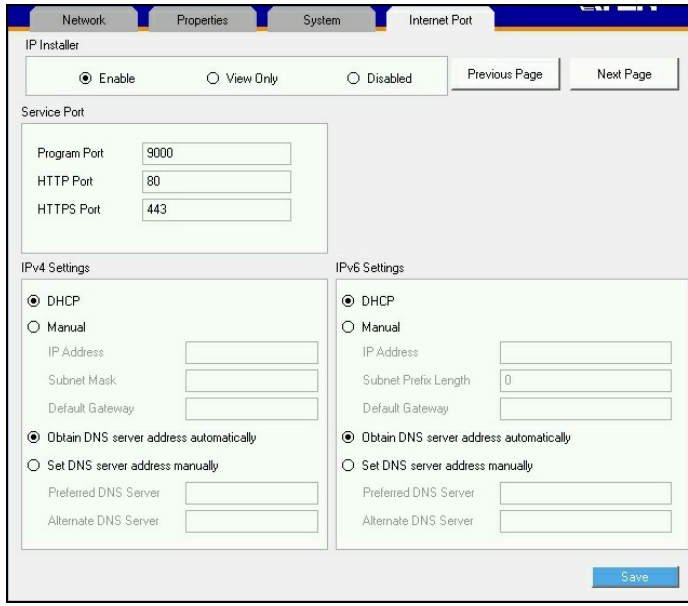


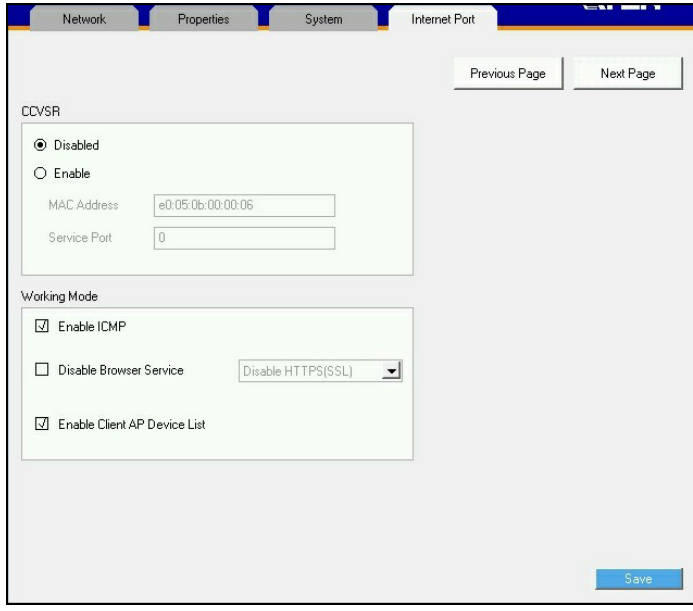
Item	Description
Device Information	Enter the **Name** and **Description** of the transmitter. It also displays the *IP Address*, *MAC Address*, *F/W version*, and *Serial Number* of the Transmitter.
Reboot	Check the box and click **Reboot** to reset the transmitter's settings back to the factory default. All custom settings (except for login account 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**.

Internet Port

The *Internet Port* tab allows you to configure the transmitter's remote port settings:





IP Installer

The IP Installer is an external Windows-based utility for assigning IP addresses to the transmitter. Click one of the radio buttons to select *Enabled, Disabled, or View Only* for the IP Installer utility. See p. 263 for IP Installer details.

Note: 1. If you select *View Only*, you will be able to see the transmitter in the IP Installer's Device List, but you will not be able to change the IP address.

2. For security purposes, we strongly recommend that you set this to *View Only* or *Disabled* after using it.

Service Ports

Specify the ports that the transmitter uses for various network services.

- **Program**: This is the port number for connecting to the transmitter from the Windows Client and Java Viewers, and from the Windows and Java Client AP programs. The default is 9000.
- **HTTP**: The port number for a browser login. The default is 80.
- **HTTPS**: The port number for a secure browser login. The default is 443.

Note: 1. Valid entries for all of the service ports are from 1–65535.

2. The service ports cannot have the same value. You must set a different value for each one.

3. If there is no firewall (on an intranet, for example), it does not matter what these numbers are set to, since they have no effect.

If a firewall is being used, the Administrator can specify the port numbers that the firewall will allow (and set the firewall accordingly). If a port other than the default is set, users must specify the port number as part of the IP address when they log in. If an invalid port number (or no port number) is specified, the transmitter will not be found.

IPv4 Settings

The transmitter can either have its IP address assigned dynamically at boot-up (DHCP), or it can be given a fixed IP address.

- For dynamic IP address assignment, select the **DHCP** radio button. (This is the default setting.)

- To specify a fixed IP address, select the **Manual** radio button and fill in the IP address.

Note: 1. If you choose *DHCP*, when the transmitter starts up it waits to get its IP address from the DHCP server. If it has not obtained the address after one minute, it automatically reverts to its factory default IP address, 192.168.0.61.

2. If the transmitter is on a network that uses DHCP to assign network addresses, and you need to ascertain its IP address, you can use the IP installer. See *IP Installer*, page 263 for information.

The transmitter can either have its DNS server address assigned automatically, or a fixed address can be specified.

- For automatic DNS Server address assignment, select the **Obtain DNS server address automatically** radio button.
- To specify a fixed address, select the **Set DNS server address manually** radio button and fill in the required information.

Note: Alternate DNS Server address is optional.

IPv6 Settings

The transmitter can either have its IPv6 address assigned dynamically at boot-up (DHCP), or it can be given a fixed IPv6 address.

- For dynamic IP address assignment, select the **DHCP** radio button. (This is the default setting.)
- To specify a fixed IP address, select the **Manual** radio button and fill in the IP address.

The transmitter can either have its DNS server address assigned automatically, or a fixed address can be specified.

- For automatic DNS Server address assignment, select the **Obtain DNS server address automatically** radio button.
- To specify a fixed address, select the **Set DNS server address manually** radio button and fill in the required information.

Note: Alternate DNS Server address is optional.

CCVSR

Important operations occur on the transmitter can be recorded using the CCVSR program.

Check **Enable** to enable the CCVSR function and specify the **MAC address** and the **Service Port** of the computer the CCVSR runs on.

Note: The valid port range is 1–65535. The port number must different than the one used for the *Program* port (see *Service Ports*, page 69).

Working Mode

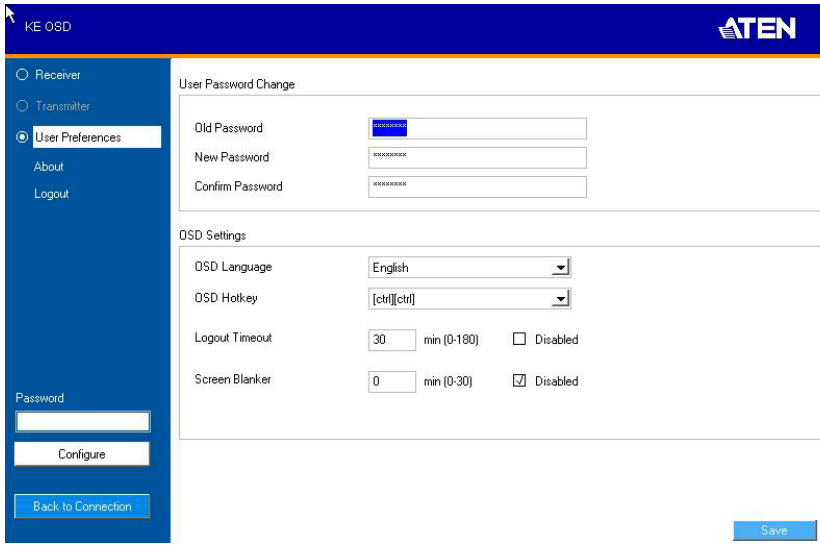
Use this section to set the working mode parameters.

- **Enable ICMP**: Check to enable ICMP service.
- **Disable Browser Service**: Check to disable a particular access. Available options are: browser, http or https.
- **Enable Client AP Device List**: Check to enable this function. When enabled, the unit will be discoverable in the Server List when using the WinClient or Java Client AP (see *Starting Up* on page 191). Disabling this function will render the unit undiscoverable in the Server List but can still be connected to.

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:

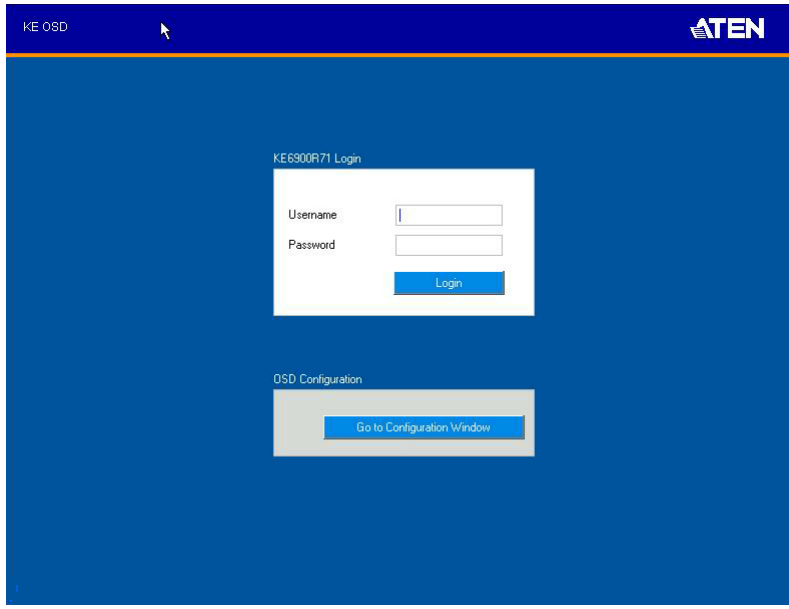


Item	Description
User Password Change	This section allows you to change the OSD password: 1. Key in the old password in the Old password field. 2. Key in the new password in the New password field. 3. Key in the new password again in the Confirm password field.
OSD Language	Click the drop-down menu to select the language you want to use for OSD sessions.
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**.

OSD Matrix Mode

If you set the system to Matrix mode (in Properties), you will see the *System Login* screen when you invoke the OSD, which provides access to the *Connection Page* by entering a username and password:

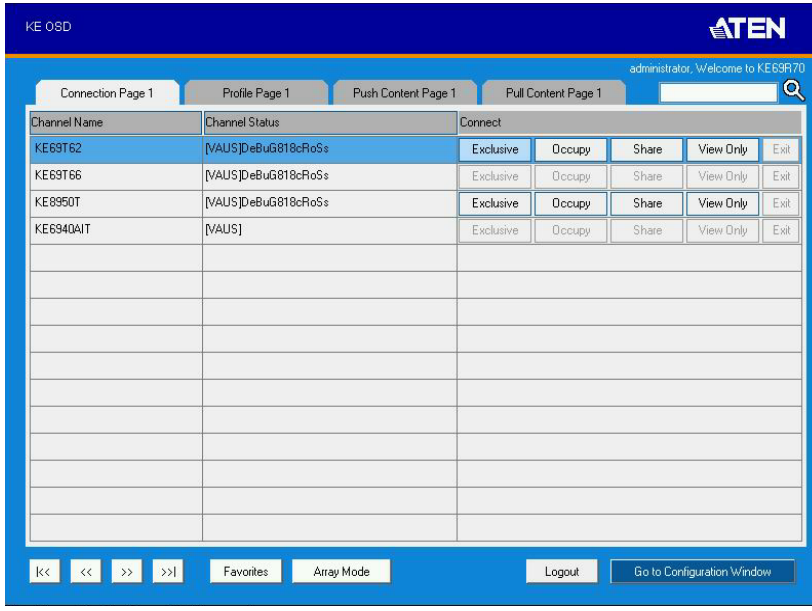


Note: 4. If the receiver does not require a login, click *Login to system*. For information about Extender and Desktop/Matrix modes, see *Mode*, page 60.

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

Connections Page

List Mode



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

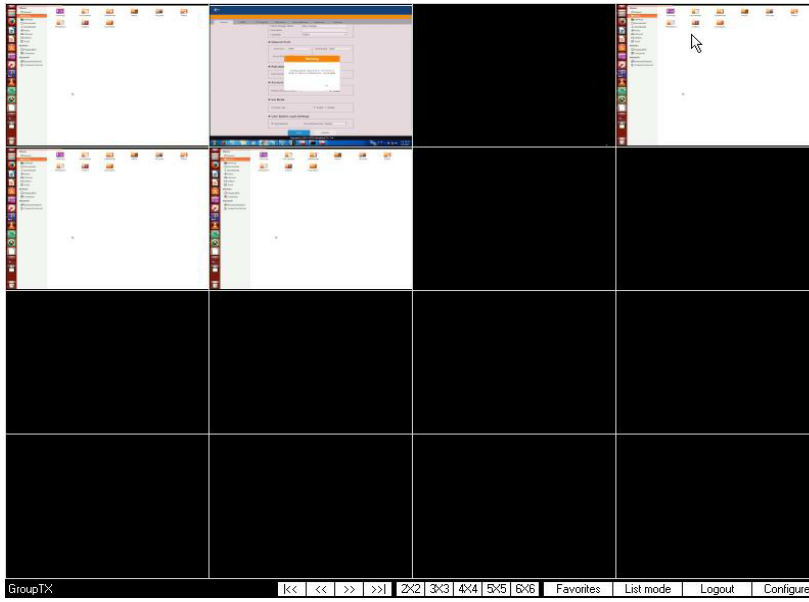
No.	Item	Description
1	Channel Name	Lists the channel connections available for the receiver. A channel is a defined connection to transmitters, created in the Device Management tab of the KVM over IP Matrix Manager (see *Browser / Telnet Operation*, page 93).
2	Channel Status	This field provides the status information of the channel, including the device name of the receiver(s) currently accessing and its operation mode. Operation modes are abbreviated as S, O, E and E for Share, Occupy, Exclusive and View Only, respectively.
3	Search	Search for transmitters based on the keyword(s) entered.

No.	Item	Description
4	Connect	To connect the receiver to a channel, click the access type: **Exclusive**: The first receiver to access the channel has exclusive control over the channel. No other receivers can view the channel. The Timeout function does not apply to this setting. **Occupy**: The first receiver to access the channel has control over the channel. However, additional receivers may view the channel's video display. If the receiver controlling the channel is inactive for longer than the time set in the Timeout box, control is transferred to the first receiver to move the mouse or strike the keyboard. **Share**: Simultaneously shares control over the channel. Input from the receivers is placed in a queue and executed chronologically. **View Only**: Receivers can only view the video display of the connected PC / workstation.
5	Next Arrow	Use these two buttons to navigate to the next page or to the end of the list if there are more channels available than can be seen on the page.
6	Previous Arrow	Use these two buttons to navigate to the previous page or to the beginning of the list if there are more channels available than can be seen on the page.
7	Favorites	Click **Favorites** to list only the channels marked as favorites. Channels marked as favorites appear with a heart icon. To add/remove a Favorite, select a channel and then right-click with the mouse to select **Add to Favorite** or **Remove from Favorite**. **Note:** Up to 50 channels can be marked as *Favorites*.
8	Array Mode	Click to view the channel connections with a preview image of each source. The list will be shown in groups of six at a time. The Array Mode is discussed on page 77.
9	List Mode	This option appears after selecting *Array* mode. Click to view the channel connections in a list that can be sorted by name or with favorites listed first. Click the Channel Name heading to change the sort.

No.	Item	Description
10	EDID Mode	When a transmitter's EDID is configured, depending on its setting, different buttons will or won't appear to configure the receiver's EDID for the connection. The following rules apply to the receiver's OSD according to the transmitter's EDID setting: ◆ Under **Default** or **Auto** EDID mode, no EDID button appears as there is nothing to configure. ◆ Under **Manual** or **Remix** EDID mode, the EDID button appears allowing you to select *Manual EDID* or *Remix EDID*. Click **Manual** or **Remix** to adjust the EDID setting locally. To set the transmitter's EDID Mode, see *Properties*, page 65.
11	Logout	Click this button to log out of the Connection Page.
12	Go to Configuration Window	Click this button to return to the main OSD screen.

Array Mode

In *Array* Mode, the screen is divided into a grid of panels, with each panel showing the video display of a particular channel. Right-click a panel and select a mode to connect: **E**: Exclusive, **O**: Occupy, **S**: Share, **V**: View Only, **X**: Exit. While video is displayed when the mouse cursor hovers over it, any audio sent from the transmitter will be heard by the receiver.

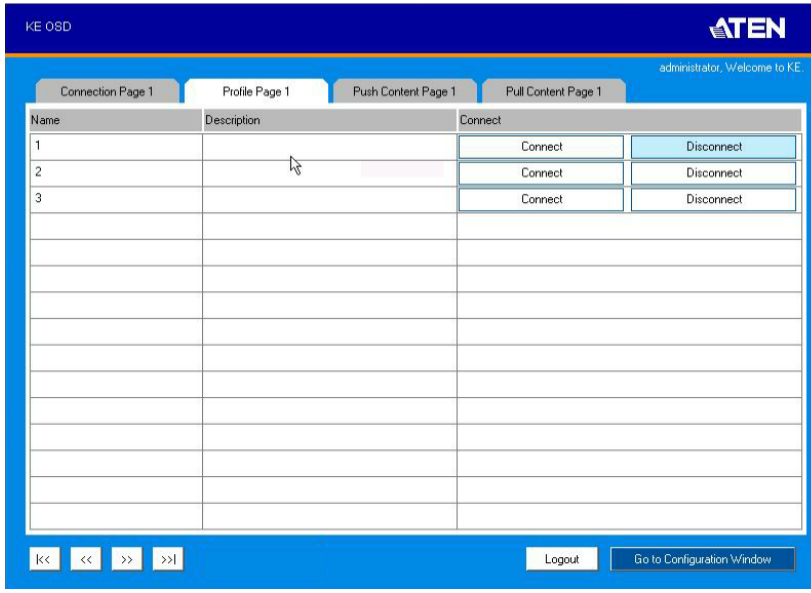


No.	Item	Description
1	Next Arrow	Use these two buttons to navigate to the next page or to the end of the list if there are more channels available than can be seen on the page.
2	Previous Arrow	Use these two buttons to navigate to the previous page or to the beginning of the list if there are more channels available than can be seen on the page.
3	Grid Selection	Select a range for how many channels you want to display. Options are: 2x2, 3x3, 4x4, 5x5, and 6x6.
4	Favorites	Click **Favorites** to list only the channels marked as favorites. Click **All** to list all channels. To add/remove a Favorite, go to List Mode, select a channel and then right-click with the mouse to select **Add to Favorite** or **Remove from Favorite**. **Note:** Up to 50 channels can be marked as *Favorites*.

No.	Item	Description
5	List Mode	Click to view the channel connections in a list that can be sorted by name or with favorites listed first. Click the Channel Name heading to change the sort. *List Mode* is discussed on page 75.
6	Logout	Click this button to log out of the Connection Page.
10	Configure	Click this button to return to the main OSD screen.

Profile Page

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



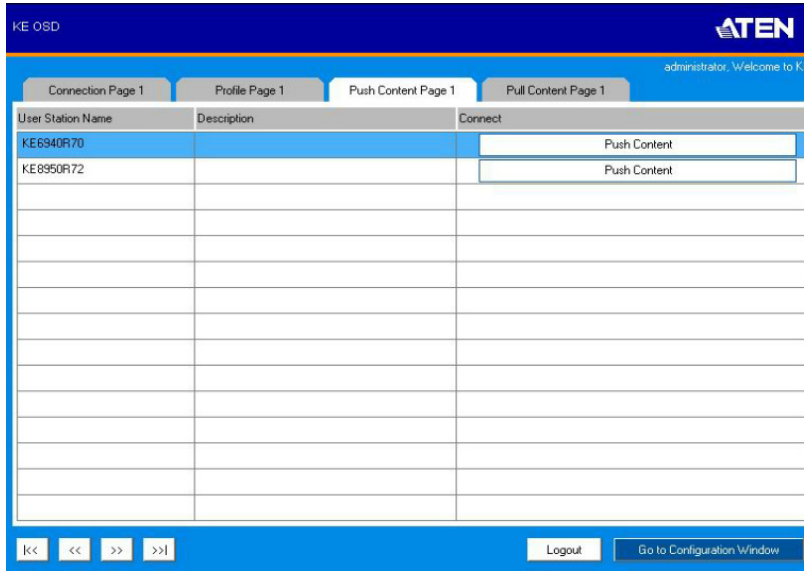
The *Profile Page* components are described in the table below:

No.	Item	Description
1	Name	Lists the Profiles available. Profiles give receivers access to channels 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 receiver will connect with the settings of that Profile (see *Adding a Profile*, page 149).
4	Disconnect	Click Disconnect to end the current Profile connection.

No.	Item	Description
5	Next Arrow	Use these two buttons to navigate to the next page or to the end of the list if there are more Profiles available than can be seen on the page.
6	Previous Arrow	Use these two buttons to navigate to the previous page or to the beginning of the list if there are more Profiles available than can be seen on the page.
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.

Push Content

Push Content allows you to push the receiver's channel connection to another receiver's console, allowing both to access the computer. Select the *Push Content* tab and the following screen appears:



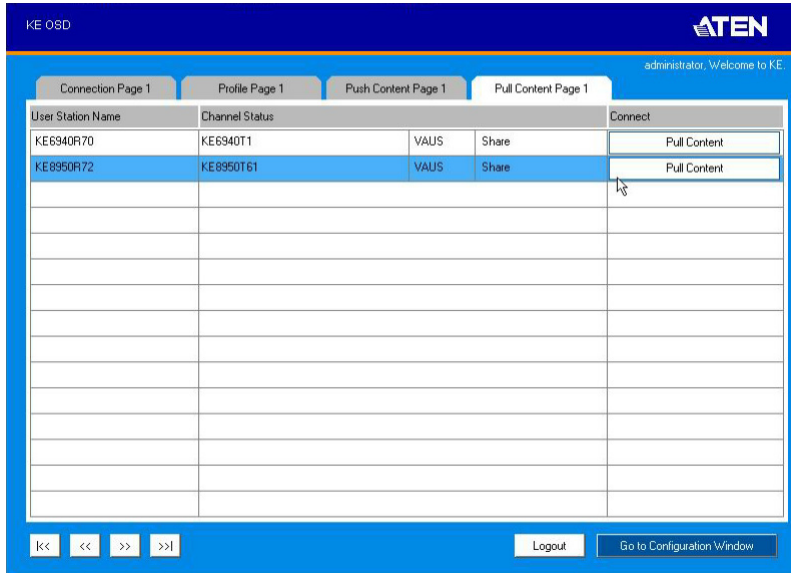
The *Push Content Page* components are described in the table, below:

No.	Item	Description
1	Receiver Name	Lists the receivers that can be selected to push the local receiver's channel connection to.

No.	Item	Description
2	Description	The field provides a description of the receiver that was entered when it was created.
3	Connect	Click **Push Content** to push the local receiver's channel connection to the selected receiver's console. The local receiver's channel connection will appear on the receiver that it was pushed to and both will share access to the computer. The access mode selected at the local receiver will determine how access is shared (see *Transmitter Permissions*, page 127 for details).
5	Next Arrow	Use these two buttons to navigate to the next page or to the end of the list if there are more choices available than can be seen on the page.
6	Previous Arrow	Use these two buttons to navigate to the previous page or to the beginning of the list if there are more choices available than can be seen on the page.
9	Logout	Click this button to log out of the Connection Page.
10	Go to Configuration Window	Click this button to return to the main OSD screen.

Pull Content

Pull Content allows you to pull a receiver's computer connection to the local receiver's console, allowing both to access to the computer. Click the *Pull Content* tab and the following screen appears:



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

No.	Item	Description
1	Receiver Name	Lists the receiver names currently connected to the channel listed under *Channel Status*.
2	Channel Status	Lists the name, description and access type of each available channel connection.
3	Connect	Click **Pull Content** and the receiver will pull the channel connection to the local console using the access mode displayed under Channel Status.
5	Next Arrow	Use these two buttons to navigate to the next page or to the end of the list if there are more choices available than can be seen on the page.
6	Previous Arrow	Use these two buttons to navigate to the previous page or to the beginning of the list if there are more choices available than can be seen on the page.
9	Logout	Click this button to log out of the Connection Page.
10	Go to Configuration Window	Click this button to return to the main OSD screen.

This Page Intentionally Left Blank

Chapter 5
Software Installation

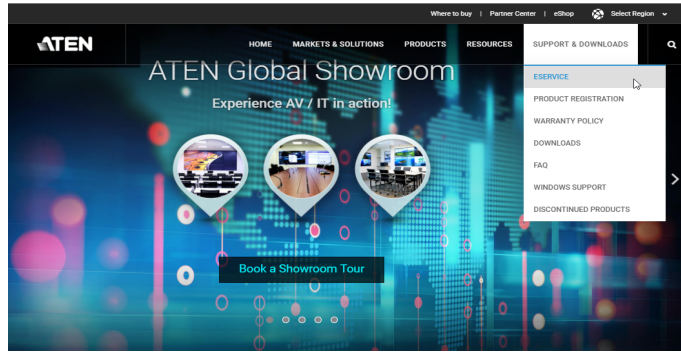
Overview

The *CCKM KVM over IP Matrix Manager* is a browser-based GUI that provides management of RCM/KE series devices over a network. You can download the KVM over IP Matrix Manager and manage up to 8 RCM/KE devices for free, or purchase a license for the KVM over IP Matrix Manager. To purchase a license, contact your local authorized ATEN dealer.

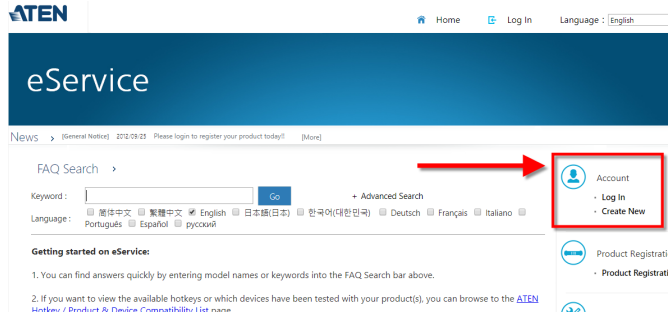
Download

To download the KVM over IP Matrix Manager, do the following:

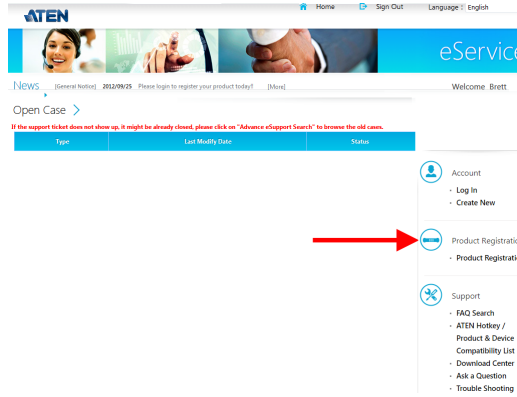
1. Visit our website and click **Support & Downloads** → **ESERVICE**.



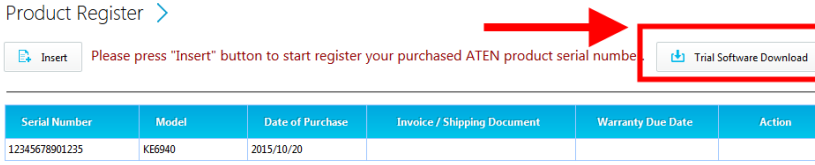
2. Under *Account*, click **Create New** or **Log In**.



3. After logging in, click **Product Registration** to register the KE device(s) you have purchased.

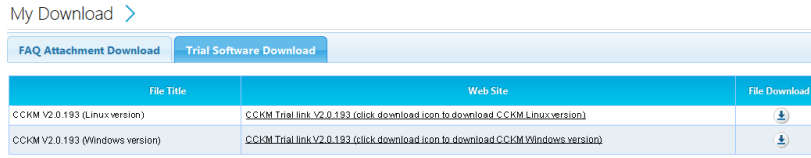


4. After you have registered the KE device(s), click **Trial Software Download**.



Note: The downloaded version of the KVM over IP Matrix Manager includes full functions and can configure up to 8 KE Series devices. If you would like to configure more KE Series devices, please contact your ATEN reseller to purchase a license and upgrade the license of your software, see page 88.

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



6. Unzip the *cckm_win_Vx.x.xxx.zip* or *cckm_linux_Vx.x.xxx.zip* file and double click the *.exe file to start the installation.

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

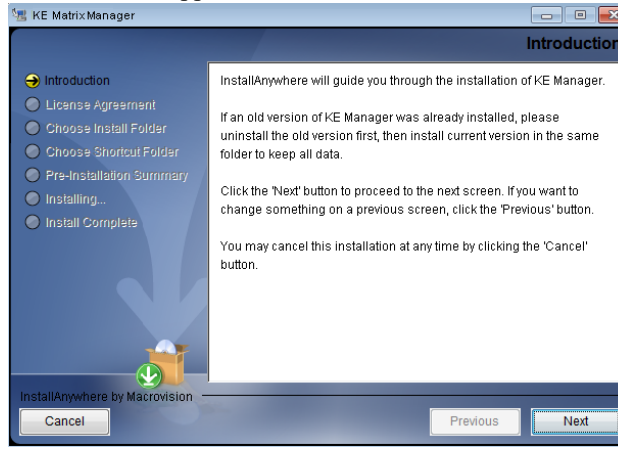
Installing the KVM over IP Matrix Manager

The following are instructions to install the KVM over IP Matrix Manager on a primary or secondary computer. For software requirements, see *Minimum Hardware/Software Requirements*, page 10.

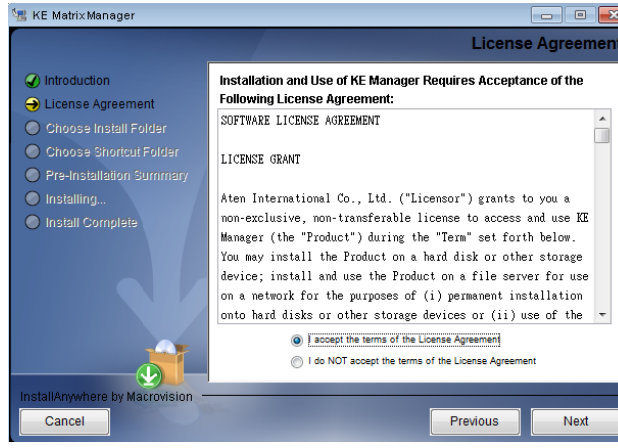
1. Insert the USB license key into a USB port on your computer.

   Note: If you have more than 8 KE Series devices in your setup, a USB license key is required to install the KVM over IP Matrix Manager.

2. Double-click the *KEMatrixManagerSetup* file to start the setup. When the *Introduction* screen appears, click **Next**.

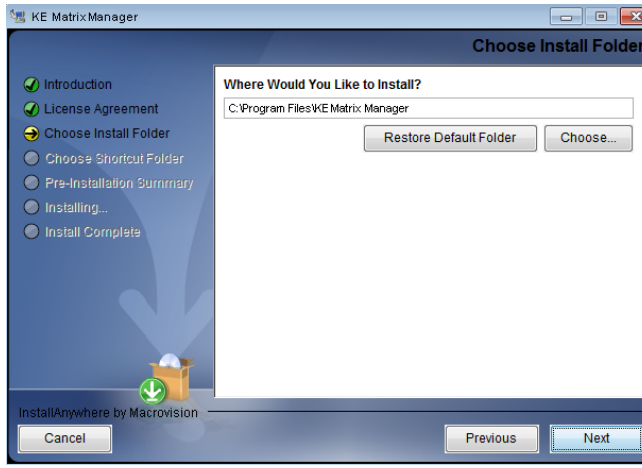


3. The *License Agreement* appears:



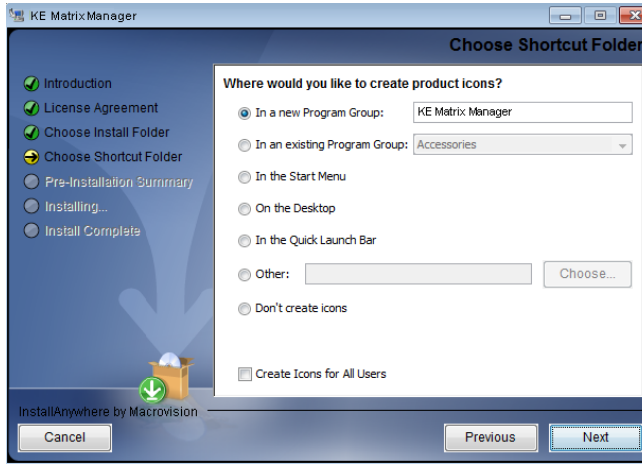
If you agree with the License Agreement, select *I accept the terms of the license agreement,* and click **Next**.

4. The *Choose Install Folder* screen appears:



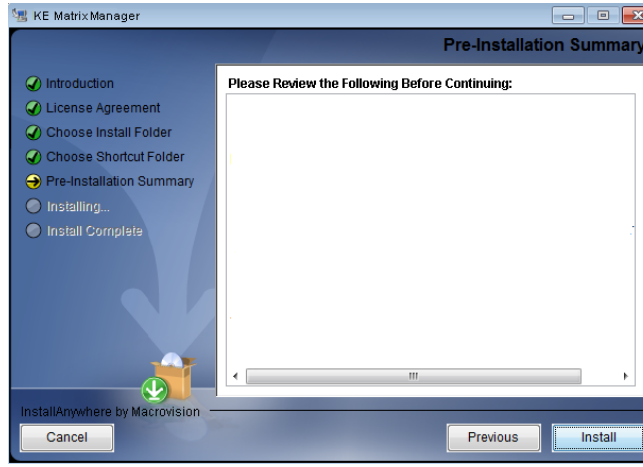
Select where you would like to install the program, and click **Next**.

5. The *Choose Shortcut Folder* screen appears:



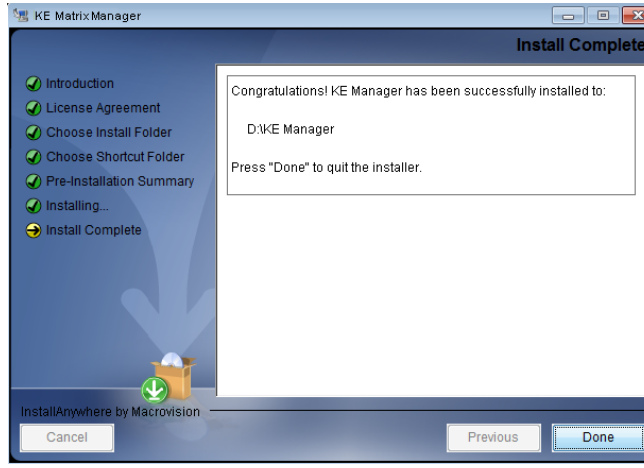
Select where to create shortcuts for the program by selecting the options provided, and click **Next**.

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.

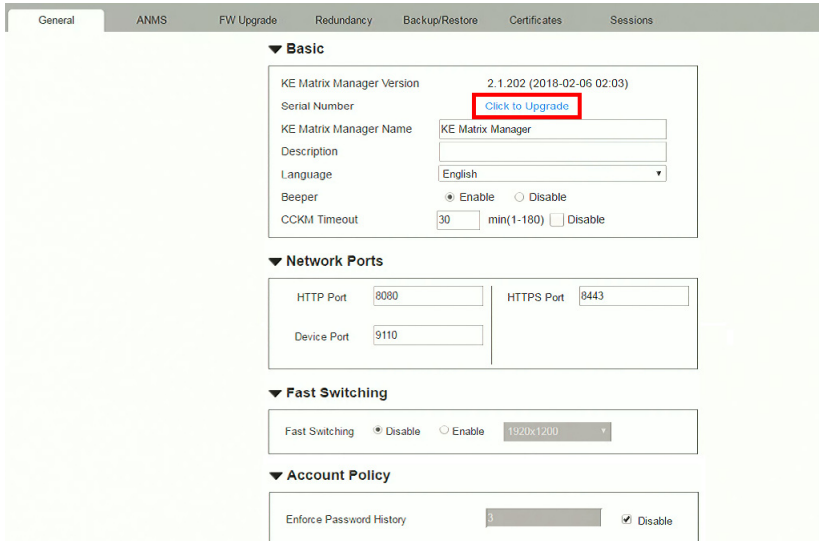
7. When the process is done, the *Install Complete* screen appears:



Click **Done**.

Upgrading License

After you purchase a license to upgrade the KVM over IP Matrix Manager, go to the *Settings* - *General* tab (see page 155), and at the top page, select **Click to Upgrade**:



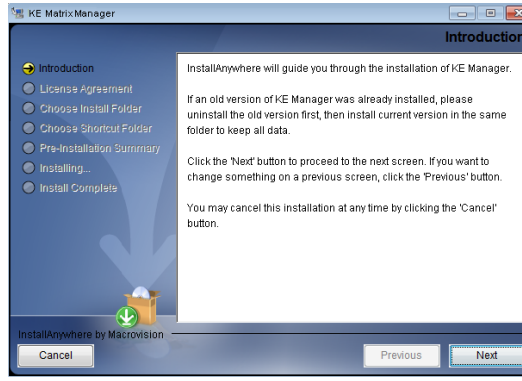
Linux Installation

The following are instructions to install the full version of the KVM over IP Matrix Manager on a Linux server. For software requirements, see *Minimum Hardware/Software Requirements*, page 10.

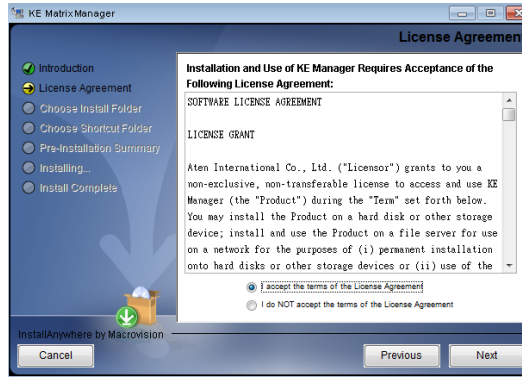
1. Download the KVM over IP Matrix Manager installation file to the Linux server.
2. Change the properties of the installation file so that its executable by running the command: `chmod a+x filename`

   Example: `chmod a+x kemanager_setup.bin`
3. Start the installation with the command:

   `sudo sh ./kemanager_setup.bin`
4. When the *Introduction* screen appears, click **Next**.:

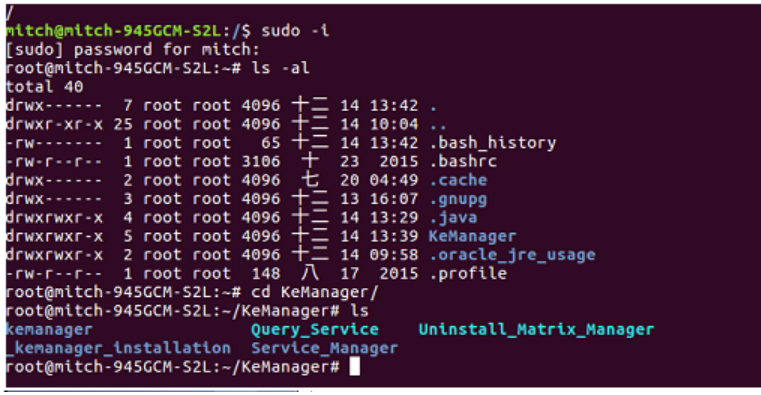


5. The *License Agreement* appears:

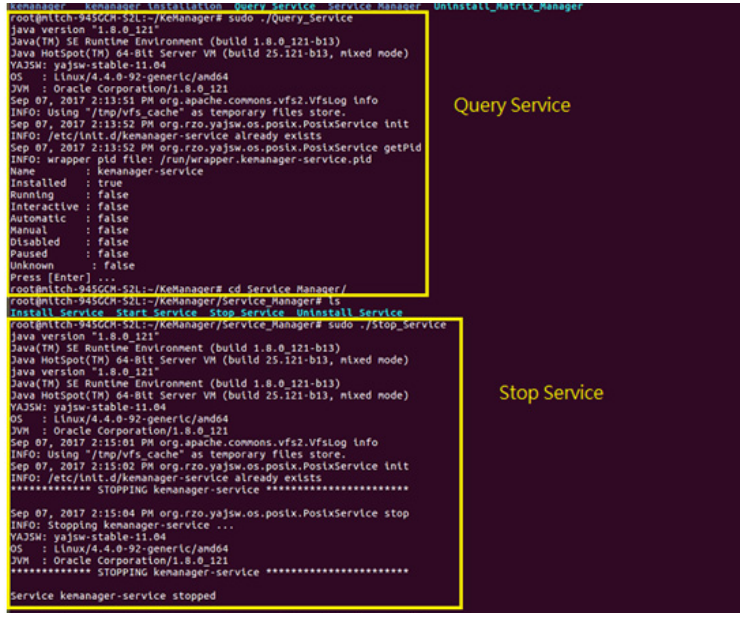


If you agree with the License Agreement, select *I accept the terms of the license agreement,* and click **Next**.

6. When the *Choose Install Folder* screen appears, select the location and continue through the installation by clicking **Next**.
7. After the software installs successfully, a directory provides useful links:

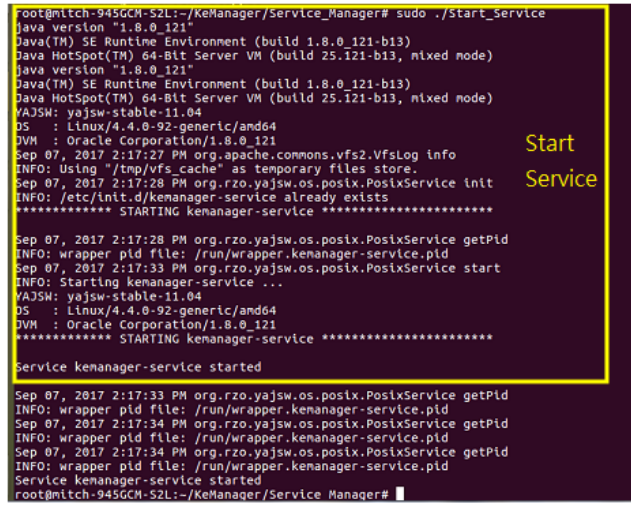


8. The "Uninstall_Matrix_Manager" can be used to uninstall the software. By default the root folder can be accessed as shown below:
   `sudo -i  cd /root  cd KeManager  sudo ./Uninstall_Matrix_Manager`
9. To check and stop the KVM over IP Matrix Manager service, use the following commands:
   `cd KeManager  sudo ./Query_Service` Stop service: `sudo ./Stop_Service`



10. To check and start the KVM over IP Matrix Manager service, use the following commands:

`cd KeManager` `sudo ./Query_Service` Stop service: `sudo ./Start_service`



This Page Intentionally Left Blank

Chapter 6
Browser / Telnet Operation

Overview

The *CCKM KVM over IP Matrix Manager* can be accessed through most standard web browsers and via Telnet. Once users log in and are authenticated, the browser GUI comes up. The first section explains the login procedure and web browser components. The last section provides details for connecting via Telnet.

Logging In

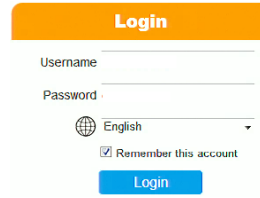
1. Open the browser and specify the IP address of the computer installed with the KVM over IP Matrix Manager, in the browser's URL location bar.

   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, or *8080* is the http port number, and a colon is inserted between it and the IP address.

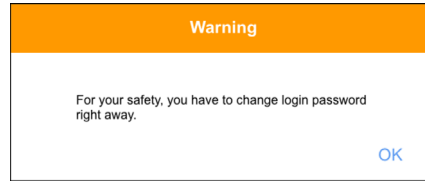
2. If a Security Alert box appears, accept the certificate — it can be trusted (See *Trusted Certificates*, page 264 for details). The Login page appears:



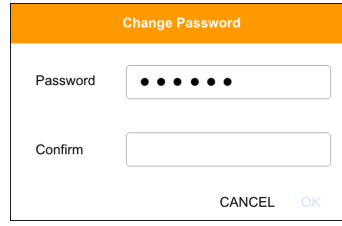
3. Enter the *Username* and *Password*, and click **Login**.

Note: Only administrator accounts can be used for login. By default, the username and password are *administrator* and *password*, respectively.

4. For security purposes, the system will prompt you to change the password immediately.



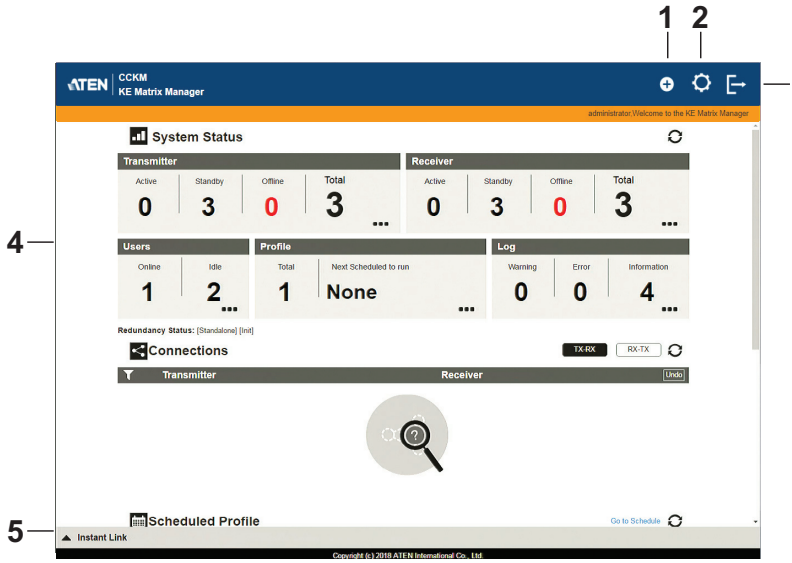
Click **OK** for the password change dialog box.



5. Enter the new password and confirm it by entering the password again.
6. Click **OK** to complete the change and the KVM over IP Matrix Manager main page appears. Refer to the next page for more details.

The KVM over IP 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	Install Wizard	This icon helps you locate transmitters / receivers on the LAN to add them to the KVM over IP Matrix Manager (see *Installation Wizard*, page 97). If a device can't be found, check the Network settings in the device's OSD menu (see page 59 & 63).
2	System Settings	Click this icon to enter the *System Setting* section where you can configure the KVM over IP Matrix Manager. The Settings are discussed on page 155.
3	Logout	Click this button to log out of your KVM over IP Matrix Manager web session.
4	Interactive Display Panel	This is your main work area. Scroll the page up or down to view the various selections. Some items can be clicked to open a settings page, while others provide status information.
5	Instant Link	Clicking this icon opens the lower bar which allows you to instantly connect RCM/KE devices. Instant Link is discussed on page 100.

Interactive Display Panel

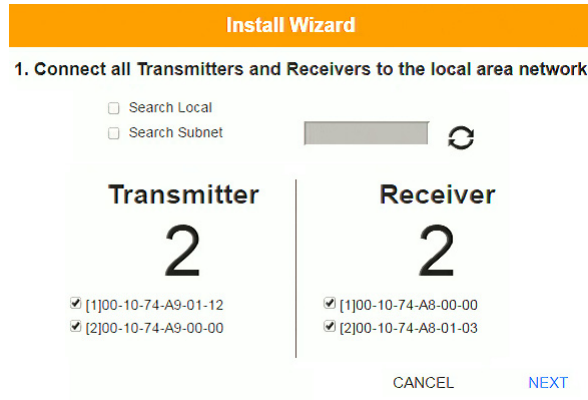
The functions associated with each of the icons on the main Interactive Display Panel are explained in the table below:

Icon	Function
	**System Status:** System Status provides an overview of the transmitter, receiver, user, profile, and log status. Each heading can be clicked to open the respective settings page. System Status is discussed on page 107.
	**Connections:** Connections provides a visual display of current transmitter and receiver connections. Connections is discussed on page 179.
	**Scheduled Profile:** Scheduled Profile provides an overview of connection profiles that are scheduled to run. Scheduled Profile is discussed on page 183.
	**Sessions:** Sessions provides a list of current user sessions. Sessions is discussed on page 185.
	**Refresh:** The Refresh button provides a way to update the information currently being displayed on the page.
	**To Top:** This button appears at the bottom right corner of the Interactive Display Panel and allows you to jump back to the top of the page.

Installation Wizard

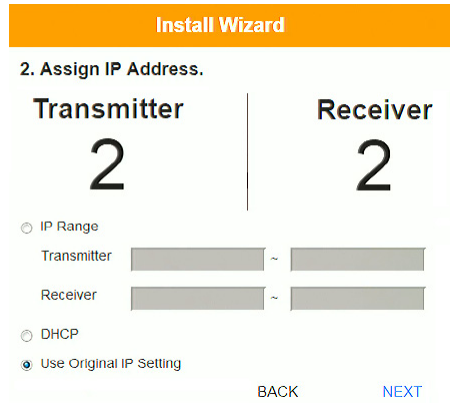
Use the *Install Wizard* to add transmitters and receivers to the CCKM. The wizard locates devices on the network and walks you through adding them. To add devices, do the following:

1. Connect all transmitters and receivers to the LAN.
2. On the CCKM main page, click the **Install Wizard** icon (page 95).
3. When the installation wizard appears, select options to locate devices:



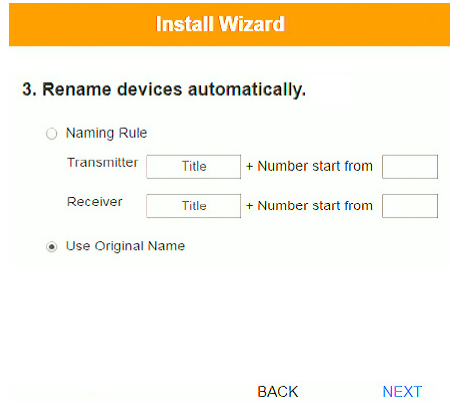
Item	Description
Search Local	Check this box and click the *Refresh* button to search the local area network for transmitters / receivers.
Search Subnet	Check this box, enter a subnet IP and then click the *Refresh* button to search the subnet for transmitters / receivers.
Transmitter / Receiver	Displays the number of *transmitters* and *receivers* that have been discovered on the network. Use the check boxes next to the transmitters / receivers to select the devices you want to add.
	The *Refresh* button provides a way to update the information currently being displayed in the install wizard window.

4. Check the boxes under *Transmitter* / *Receiver* to select the devices you want to add, then click **Next**.
5. Under *Assign IP Address*, select an option to configure the network settings, then click **Next**.

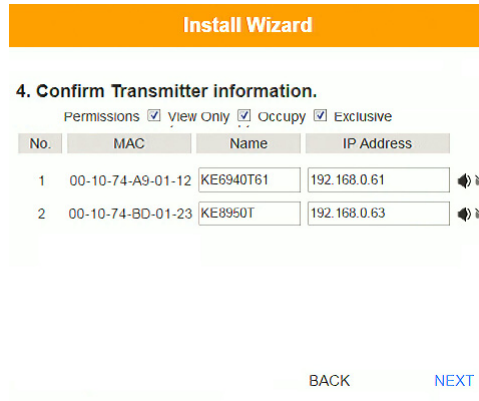


Item	Description
IP Range	Select the *IP Range* radio button to enter a series of static IP addresses to assign to the *transmitters*/*receivers* that you are adding.
DHCP	Select the *DHCP* radio button for dynamic IP address assignment.
Use Original IP Setting	Select this radio button to use the IP address currently configured on the transmitter / receiver.

6. Use the *Naming Rule* radio button to create a naming convention (*Title* + *Number*); or *Use Original Name* to use the name currently configured on the transmitter / receiver, then click **Next**.



7. Confirm each Transmitter's *Name*, *IP Address*, *Audio* setting and check the boxes to set *Permissions**, then click **Next** and repeat the process for Receivers.



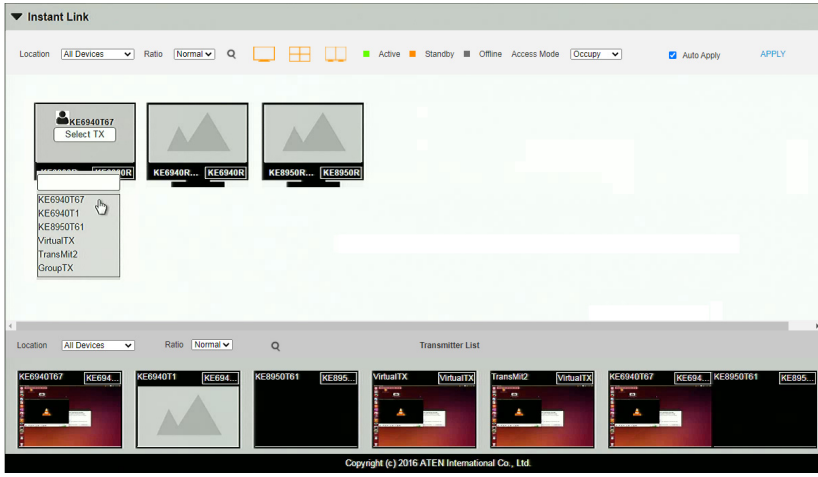
Note: See *Transmitter Permissions*, **page 127**, and *Receiver Permissions*, **page 139** for information about setting permissions.

8. Click **Done**.

Instant Link

At the bottom of the KVM over IP Matrix Manager main page is the *Instant Link* bar. In this section, you can quickly connect receivers to transmitters.

The top panel provides the **Receiver List**, and the bottom panel provides the **Transmitter List**. To create a connection, click a receiver in the top panel and use the drop-down menu to select a transmitter (as shown in the image below); or drag-and-drop transmitters from the bottom panel to receivers in the top panel. Configure as many receiver to transmitter connections as needed, and then click **Apply**.



Item	Description
Instant Link	The Instant Link bar provides access to quickly connect receivers to transmitters. Click the bar to open the panel, click again to minimize the panel. The top panel provides a list of all the receivers discovered on the LAN.Click a receiver and use the drop-down menu to select a transmitter.
Transmitter List	Click the Transmitter List bar to open the panel. The panel provides a list of all the transmitters discovered on the LAN. Drag-and-drop transmitters in the bottom panel to receivers in the top panel to establish connections. The panel size of the Transmitter List is adjustable by clicking-and-dragging its border.
Location	Use the drop-down menu to select a location to filter the receivers or transmitters displayed on the page.

Item	Description
Ratio	Use the drop-down list to adjust the icon size of the receivers / transmitters.
	Click and type keywords to filter/search for receivers / transmitters.
	Click this icon to show individual receivers.
	Click this icon to show only Video Wall receivers.
	Click this icon to show only Receiver Group receivers.
Access Mode	Click a device and use the drop-down box to set the access mode: *Occupy*, *View Only*, or *Exclusive*.
Auto Apply	Checking this box allows you to drag and drop devices and apply the connection immediately without having to click the *Apply* button.
Apply	Click **Apply** to connect the devices.
Cancel	Click **Cancel** to exit without connecting.

RS-232 / Telnet

The RCM/KE series can be operated and configured via a remote terminal session using Telnet. This is a useful means for configuring devices for first-time setup and connection to the network.

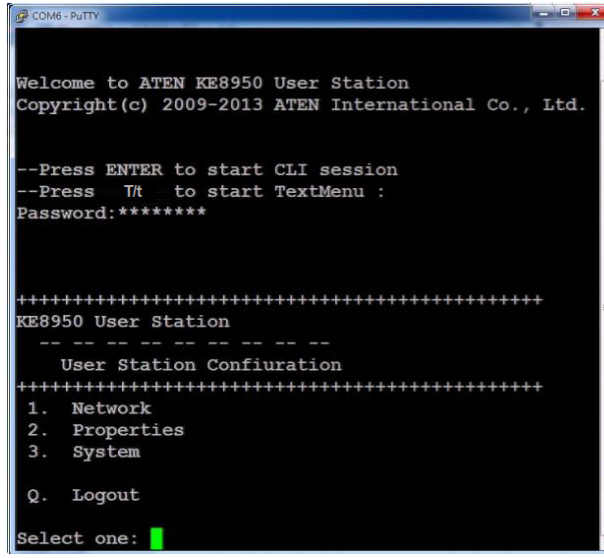
Telnet

To log into the RCM/KE series device by means of a Telnet session, do the following:

1. On your computer, open a terminal (command line) session.
2. At the prompt, key in the RCM/KE device's IP address with port 23 in the following way:

   ```
   telnet [IP address] [port]
   ```

3. Please press **[T/t]** to start "**TextMenu**" The login screen appears. At the login prompt, provide the Password.



Note: The default password for Telnet sessions is *password*.

RS-232

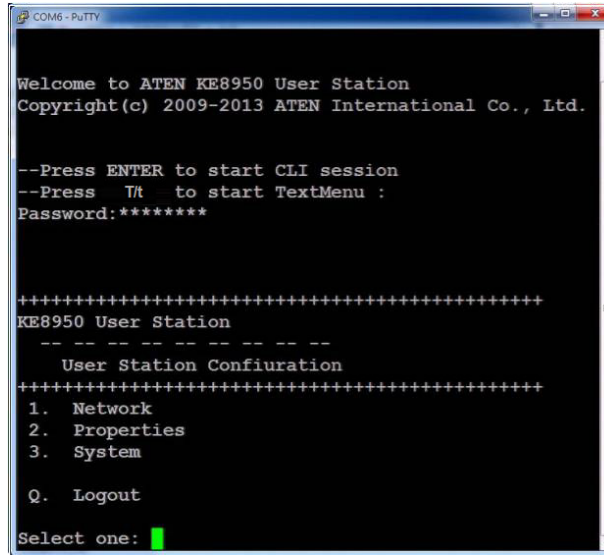
To log into the RCM/KE series device by means of a RS-232 session, do the following:

1. The controller's serial port should be configured the same as the receiver's default configuration, as shown below:

Baud Rate	9600
Data Bits	8
Parity	None
Stop Bits	1
Flow Control	None

The receiver's **Function Switch** should be set to *RS-232 Config* (see page 11). Before executing RS-232 commands across a network you must install the KVM over IP Matrix Manager on a computer and ensure that it is online. Please make sure the RS-232 Serial Port is not connected before executing commands.

2. Please press **[T/t]** to start "**TextMenu**" The login screen appears. At the login prompt, provide the Password.



Note: The default password for Telnet sessions is *password*.

Configuration Menu

Once a Telnet connection to the RCM/KE device is established, the device's text-based Configuration Menu comes up, allowing you to select options by entering a number on the following screens:

Main Menu

++

KE6940A Receiver

-- -- -- -- -- -- -- -- --

Receiver Configuration

++

1. Network
2. Properties
3. System

Q. Logout

Select one:

1. Network

```
++++++++++++++++++++++++++++++++++++++++++++++++
KE6940A Receiver
-- -- -- -- -- -- -- -- --
   Network Settings
++++++++++++++++++++++++++++++++++++++++++++++++
 1. IP Installer        [Enabled]
 2. DHCP                [Disabled]
 3. IP Address          [172.17.17.34]
 4. Subnet Mask         [255.255.255.0]
 5. Default Gateway     [172.17.17.254]

 Q. Exit

Select one:
```

2. Properties

```
++++++++++++++++++++++++++++++++++++++++++++++++
KE6940A Receiver
-- -- -- -- -- -- -- -- --
   Device Properties
++++++++++++++++++++++++++++++++++++++++++++++++
 1. Mode     [Matrix]
 2. Transmitter Video IP Address [172.17.17.35]
 3. Transmitter Audio IP Address [172.17.17.35]
 4. Transmitter USB IP Address   [172.17.17.35]
 5. Transmitter RS232 IP Address [172.17.17.35]
 6. UART Configuration
 7. Video    [Enabled]
 8. Audio    [Enabled]
 9. USB      [Enabled]
10. RS232    [Enabled]
11. KVM over IP Matrix Manager IP       [172.17.17.33]
12. KVM over IP Matrix Manager Port     [9110]
13. Beeper              [Enabled]
14. USB Mode            [VM]
15. USB Secure Transmit [Disabled]

 Q. Exit

Select one:
```

3. System

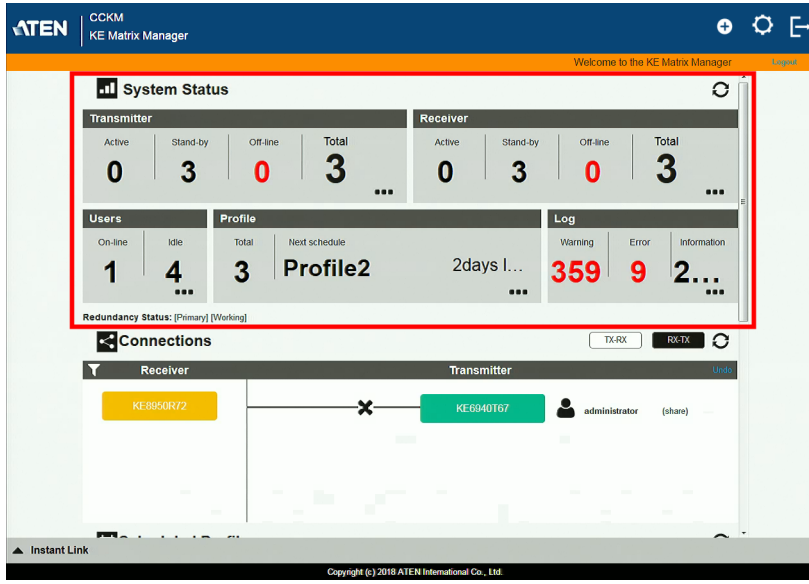
```
++++++++++++++++++++++++++++++++++++++++++++++++
KE6940A Receiver
-- -- -- -- -- -- -- -- --
   System Setting
++++++++++++++++++++++++++++++++++++++++++++++++
 1. Device Name        [KE6940AR]
 2. Device Description [Receiver1]

    Device IP Address: 172.17.17.34
    Device MAC Address: 00:10:74:A8:01:23
    Device FW Version: V1.1.109
    Device Serial Number:

 3. Password [Enabled]
 4. Change Password
 5. System Reboot/Reset to Factory Default

 Q. Exit

Select one:
```

Note: The Reset to Factory Default function resets everything but the login information to the factory default settings. To reset the login information, refer to *Reset All Information* on page 266.

Chapter 7
System Status

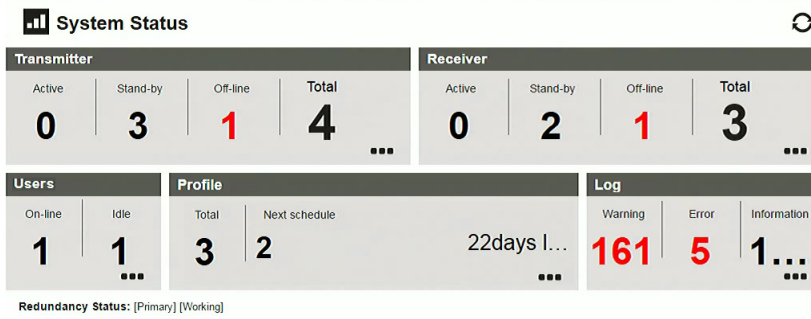
Overview

The *System Status* panel is found at the top of the **KVM over IP Matrix Manager** main page. This section provides status information about Transmitters, Receivers, Users, Profiles and Logs. Click on a selection to open a *Settings* page, which are discussed in the sections that follow.



System Status

The *System Status* panel has five sections that provide information and a link to each settings page. Each settings page can be accessed by **Clicking** within the section: Transmitter, Receiver, Users, Profile or Log. Each section is explained in the table below and the Settings on the pages that follow.

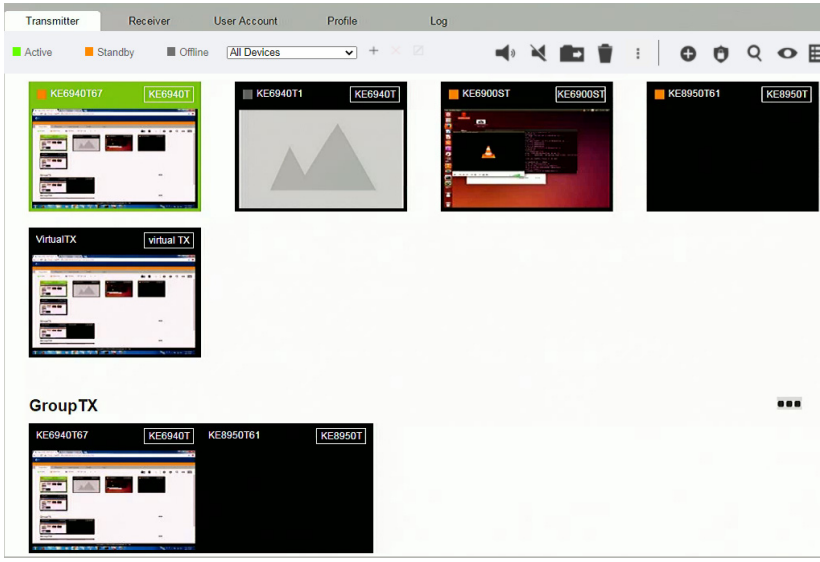


Item	Description
Transmitter	This section provides an overview of the transmitters added to the KVM over IP Matrix Manager: ◆ **Active**: Shows the number of transmitters that are currently online and connected to a receiver. ◆ **Standby**: Shows the number of transmitters that are online but not connected to a receiver. ◆ **Offline**: Shows the number of transmitters added to the KVM over IP Matrix Manager that are not online. ◆ **Total**: Displays the total number of transmitters added to the KVM over IP Matrix Manager.
Receiver	This section provides an overview of the receivers added to the KVM over IP Matrix Manager: ◆ **Active**: Shows the number of receivers that are currently online and connected to a transmitter. ◆ **Standby**: Shows the number of receivers that are online but not connected to a transmitter. ◆ **Offline**: Shows the number of receivers added to the KVM over IP Matrix Manager that are not online. ◆ **Total**: Displays the total number of receivers added to the KVM over IP Matrix Manager.

Item	Description
Users	This section provides an overview of users with KVM over IP Matrix Manager sessions: ◆ **Online**: Shows the number of users that are logged into OSD or KVM over IP Matrix Manager web sessions. ◆ **Idle**: Shows the number of users not logged into OSD or KVM over IP Matrix Manager web sessions.
Profile	This section provides an overview of Profile and Profile Schedules: ◆ **Total**: Shows the total number of Profiles available. ◆ **Next scheduled to run**: Shows the name of the next Profile scheduled to run. ◆ **Days later**: Shows the number of days until the next Profile is scheduled to run.
Log	This section provides an overview of system logs: ◆ **Warning**: Shows the number of warnings logs generated since the event log was cleared. ◆ **Error**: Shows the number of error logs generated since the event log was cleared. ◆ **Information**: Shows the number of information logs generated since the log was cleared.
Redundancy Status	This section provides information about the Redundancy mode. The first set of brackets shows which server is hosting the KVM over IP Matrix Manager database: **[Primary]** or **[Secondary]**. If Redundancy is disabled the first bracket will read: **[Standalone]**. The second set of brackets show the status: ◆ **[Working]**: The server is actively hosting the KVM over IP Matrix Manager database. ◆ **[Standby]**: This message appears when database operations are idle.

Transmitter

Click **Transmitter** in the *System Status* panel to open the settings. On this page, you can add, delete and configure *Transmitters* (physical transmitters), *Virtual Transmitters* (multi-source) and *Transmitter Groups* (multi-video source). The KVM over IP Matrix Manager automatically adds transmitters connected to the local area network with a valid IP address.



The meanings of the icons and headings on the page are straightforward and let you view and configure Transmitters.

- *Active* refers to a transmitter connection that is online and in use.
- *Standby* refers to a transmitter connection that is online.
- *Offline* refers to a transmitter connection that is offline.
- All Devices ▼ Use this drop-down menu to filter transmitters by location. Use Locations to limit the transmitters seen on the page.
  - Click to add a new **Location**.
  - Select a transmitter and click the **Move to** icon to add devices to a Location.
  - Select a Location from the drop-down menu and click this icon to delete it.

- Select a Location and click this icon to change the name.

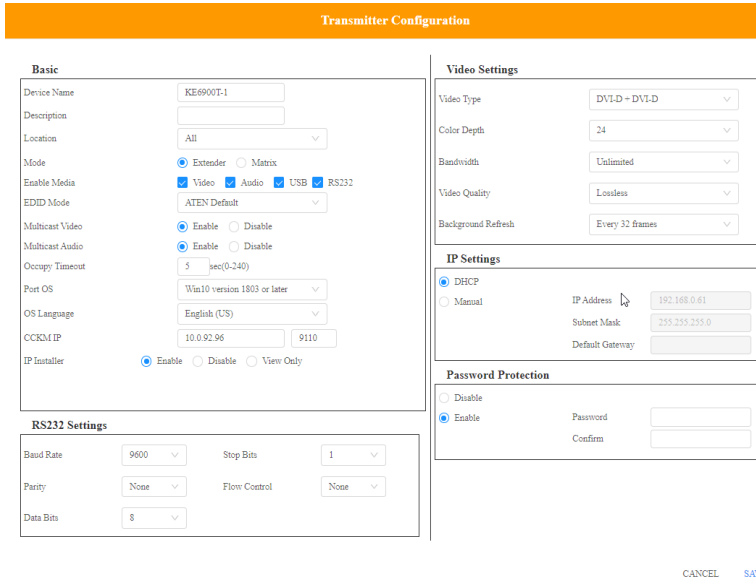
- / Click to turn Beeper & LED Flashing on/off.
- Click to delete selected transmitters.
- Click an option to have selected transmitters:
  - **Copy & Paste**: Copy settings from one transmitter and paste them to another (see *Copy & Paste*, **page 123**).
  - **Reboot**: Shut down and restart.
  - **Reset to Factory**: Reset all setting to the factory default.

Note: The Reset to Factory function resets everything but the login information to the factory default settings. To reset the login information, refer to *Reset All Information* on page 266.

- Click to *Create Virtual TX* or *Create TX Group* (*page 124 & 126*).
- Click to set transmitter permissions (*page 127*).
- Click to search for transmitters.
- Click to filter transmitters shown on the page.
- Click to switch between *Grid View* and *List View*.

Transmitter Configuration

When the KVM over IP Matrix Manager discovers transmitters on the network, they appear on the *Transmitter* settings page. Double-click a transmitter to configure its settings.



Item	Description
Basic	**Device Name:** Enter a name for the Transmitter. **Description:** Enter a description for the Transmitter. **Location:** Use the drop-down menu to select a Location for the device. Locations filter the transmitters seen on the settings page. **Mode:** Use the radio button to select how the Transmitter will be installed and managed: ◆ Select **Extender** mode for simple one-to-one (transmitter to receiver) setups that are managed at the receiver's OSD menu. ◆ Select **Matrix** mode to manage devices and connections over the LAN from the KVM over IP Matrix Manager. This mode is for advanced administration of transmitter and receiver connections configured within the CCKM. **Enable Media**: Select which source type the Transmitter can stream: Video, Audio, USB and RS-232.

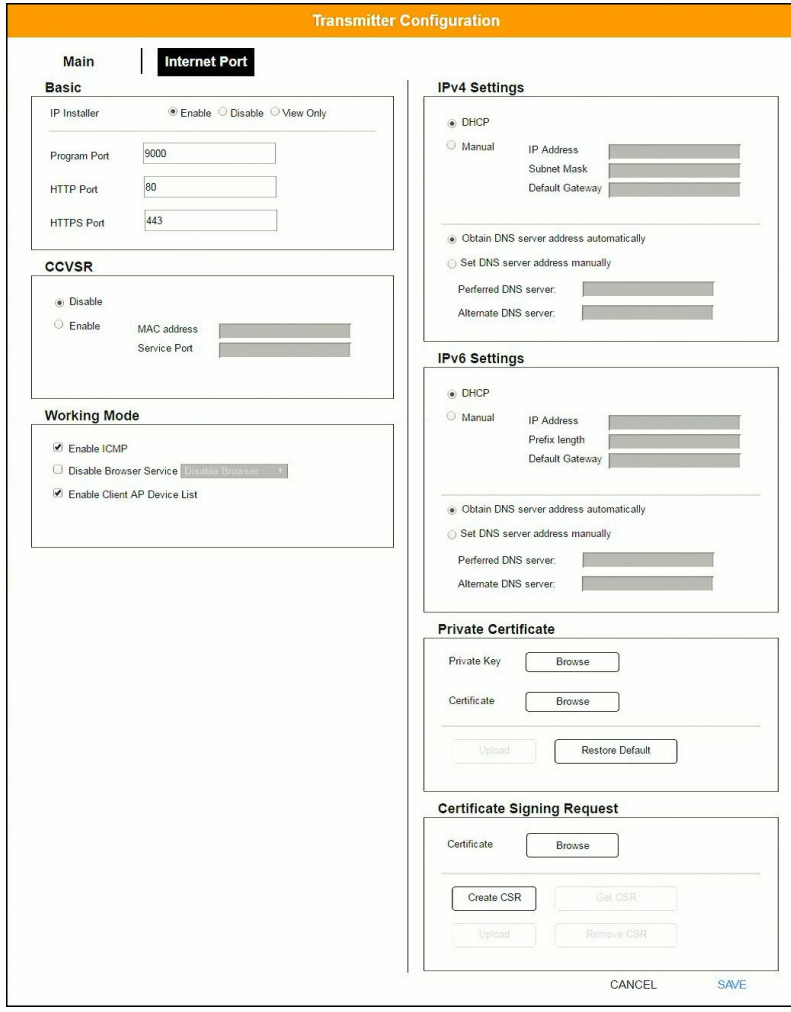
Item	Description
Basic	**EDID Mode**: EDID contains a display's basic information and is used by the source device to utilize the best resolution across different monitors. When *Manual* or *Remix* is selected, the receiver's OSD will have a button allowing the local EDID setting to be configured for the connection (see *EDID Mode*, page 76). Select how you want the source device to acquire the display's EDID: ◆ **ATEN Default**: EDID is set to the default ATEN configuration. ◆ **Auto**: Checks the EDID of all connected displays and the ATEN default EDID to use the best common resolution for all displays. ◆ **Manual**: Manually set the EDID configuration from the receiver's OSD (see *EDID Mode*, page 76). ◆ **Remix**: Manually checks the EDID of all connected displays and the ATEN default EDID to use the best common resolution for all displays (see *EDID Mode*, page 76). **Multicast Video:** Select **Enable** to allow a broadcast of the transmitter's video signal to be sent to multiple receivers. **Multicast Audio:** Select **Enable** to allow a broadcast of the transmitter's audio signal to be sent to multiple receivers. ◆ **Occupy Timeout**: Set a time threshold for receivers whose Access Mode has been set to Occupy**.** If there is no activity from the receiver occupying the port for the amount of time set here, the receiver is timed out and the port is released. The first receiver 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. **Port OS:** Use the drop-down menu to select the operating system on the computer connected to the transmitter. **OS Language:** Use the drop-down menu to select the operating system language on the computer connected to the transmitter. **CCKM IP:** Set the **IP** address and **Port** number of the computer running the KVM over IP Matrix Manager. The default port number is 9110. **IP Installer**: The IP Installer is an external Windows-based utility for assigning an IP address to the device. Click a radio button to select Enable, Disable or View Only for the IP Installer utility. See *IP Installer*, page 263 for instructions.

Item	Description
Video Settings	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, with the highest to lowest quality being Lossless > Light Compression > Medium Compression > Heavy Compression > Maximum Compression. **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.
IP Settings	For dynamic IP address assignment, select the **DHCP** radio button. To specify a fixed IP Address, Subnet Mask, and Default Gateway select the **Manual** 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 46.
Password Protection	Select **Enable** to require a password to access the transmitter's OSD configuration screens (see page 59). Enter a *Password*, and confirm the password in the *Confirm* box.
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

Item	Description
Replace Device	Click **Replace Device** in the top left corner to replace an old transmitter with a new one.* All settings are copied from the old transmitter to the new transmitter. Before using this feature, connect the new transmitter to the network. After clicking *Replace Device*, use the drop-down menu to select the new transmitter where the settings will be applied. **Note:** 1. This option only appears when a transmitter is offline. 2. This feature can be used for both receivers and transmitters. Replacement should be carried out on a similar model.
Save	Click **Save** to save changes to the properties.
Cancel	Click **Cancel** to exit without saving.

Internet Port

The *Internet Port* tab is used to configure the remote port of the RCMDVI00AT / RCMDVI40AT / RCMDVI00BT / RCMDVI40BT / RCMDVI50T.



Basic

■ IP Installer

The IP Installer is an external Windows-based utility for assigning IP addresses to the transmitter. Click one of the radio buttons to select *Enabled, Disabled, or View Only* for the IP Installer utility. See p. 263 for IP Installer details.

Note: 1. If you select *View Only*, you will be able to see the transmitter in the IP Installer's Device List, but you will not be able to change the IP address.

2. For security purposes, we strongly recommend you to set this to *View Only* or *Disabled* after using it.

■ Ports

Specify the ports that the transmitter uses for various network services.

- **Program**: This is the port number for connecting to the transmitter from Windows Client and Java Viewers, and from Windows and Java Client AP programs. The default is 9000.
- **HTTP**: The port number for a browser login. The default is 80.
- **HTTPS**: The port number for a secure browser login. The default is 443.

Note: 1. Valid entries for all of the Service Ports are from 1–65535.

2. The service ports cannot have the same value. You must set a different value for each one.

3. If there is no firewall (on an intranet, for example), it does not matter what these numbers are set to, since they have no effect.

If a firewall is being used, the Administrator can specify the port numbers that the firewall will allow (and set the firewall accordingly). If a port other than the default is set, users must specify the port number as part of the IP address when they log in. If not, an invalid port number (or no port number) is specified, the transmitter will not be found.

CCVSR

Important operations occur on the transmitter can be recorded using the CCVSR program.

Check **Enable** to enable the CCVSR function and specify the **MAC address** and the **Service Port** of the computer the CCVSR runs on.

Note: The valid port range is 1–65535. The port number must be different than the one used for the *Program* port (see *Ports*, page 117).

Mode

Use this section to set the working mode parameters.

- **Enable ICMP**: Check to enable ICMP service.
- **Disable Browser Service**: Check to disable a particular access. Available options are: browser, http or https.
- **Enable Client AP Device List**: Check to enable this function. When enabled, the unit will be discoverable in the Server List when using the WinClient or Java Client AP (see *Starting Up* on page 191). Disabling this function will render the unit undiscoverable in the Server List but can still be connected to.

IPv4 Settings

The transmitter can either have its IP address assigned dynamically at startup (DHCP), or it can be given a fixed IP address.

- For dynamic IP address assignment, select the **DHCP** radio button. (This is the default setting.)
- To specify a fixed IP address, select the **Manual** radio button and fill in the IP address.

Note: 1. If you choose *DHCP*, when the transmitter starts up it waits to get its IP address from the DHCP server. If it has not obtained the address after one minute, it automatically reverts to its factory default IP address, 192.168.0.61.

2. If the transmitter is on a network that uses DHCP to assign network addresses, and you need to ascertain its IP address, you can use the IP installer. See *IP Installer*, page 263 for information.

The transmitter can either have its DNS server address assigned automatically, or a fixed address can be specified.

- For automatic DNS Server address assignment, select the **Obtain DNS server address automatically** radio button.
- To specify a fixed address, select the **Set DNS server address manually** radio button and fill in the required information.

Note: Specifying at the alternate DNS Server address is optional.

IPv6 Settings

The transmitter can either have its IPv6 address assigned dynamically at startup (DHCP), or it can be given a fixed IPv6 address.

- For dynamic IP address assignment, select the **DHCP** radio button. (This is the default setting.)
- To specify a fixed IP address, select the **Manual** radio button and fill in the IP address.

The transmitter can either have its DNS server address assigned automatically, or a fixed address can be specified.

- For automatic DNS Server address assignment, select the **Obtain DNS server address automatically** radio button.
- To specify a fixed address, select the **Set DNS server address manually** radio button and fill in the required information.

Note: Specifying at the alternate DNS Server address is optional.

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 265 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, save it to a convenient location on your computer.

Importing the Private Certificate

To import the private certificate, do the following:

1. Click **Browse** to the right of **Private Key**, navigate to where your private encryption key file is located and select it.
2. Click **Browse** to the right of **Certificate**, navigate to where your certificate file is located and select it.
3. Click **Upload** to complete the procedure.

Note: Both the private encryption key and the signed certificate must be imported at the same time.

You can click **Restore Default** to restore any changes made previously.

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 **Create CSR**. 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
State or Province	Taiwan
Locality	Taipei
Organization	Your Company, Ltd.
Unit	Techdoc Department
Common Name	mycompany.com 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 transmitter.

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 **Browse** to locate the file; then click **Upload** to store it on the transmitter.

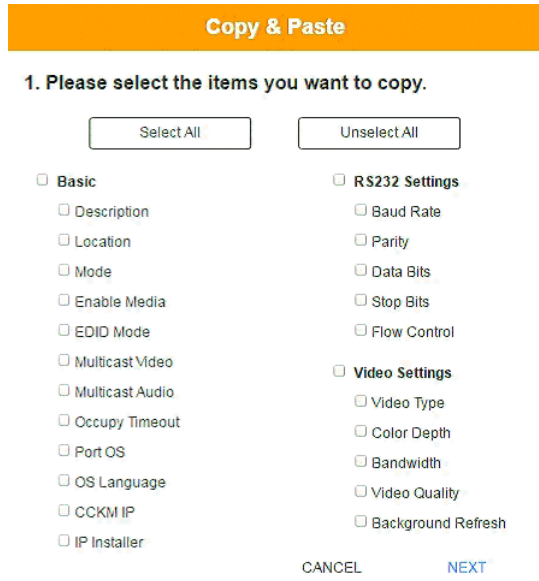
Note: When you upload the file, the transmitter checks the file to make sure the specified information still matches. If it does, the file is accepted; if not, it is rejected.

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

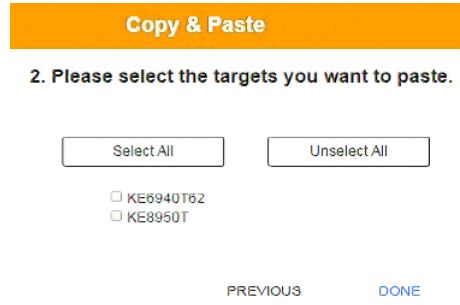
Copy & Paste

Copy & Paste allows you to copy settings from one transmitter and paste them to another. To copy transmitter settings to another device, do the following:

1. Select a physical transmitter.
2. On the Transmitter menu bar, click **Copy & Paste** (page 111).
3. Check the boxes of the settings you want to copy, and click **Next**.



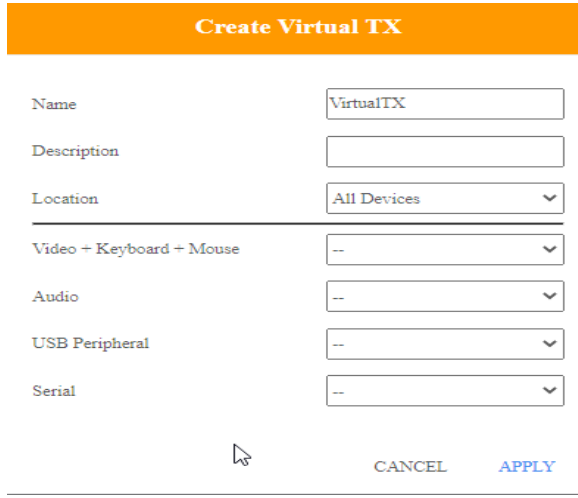
4. Select the transmitter(s) to which you want to apply the settings, and click **Done**.



Virtual Transmitter

Creating a *Virtual Transmitter* allows you to create one connection that sources media (KVM, audio, USB, serial) from different transmitters. Virtual Transmitters appear on the *Transmitter* settings page with **Virtual TX** in the top right corner. Simply select an online transmitter for each media source. dual-display transmitters can be added as two separate Virtual Transmitters.

To create a Virtual Transmitter, in *Transmitter* settings click ⊕ and then select **Create Virtual TX**.



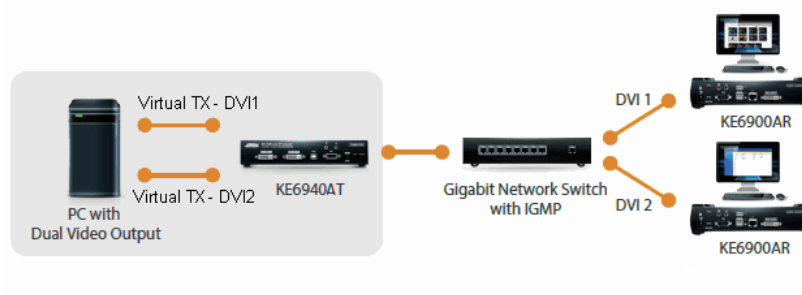
Item	Description
Name	Enter a name for the Virtual Transmitter.
Description	Enter a description for the Virtual Transmitter.
Location	Use the drop-down menu to select a location for the Virtual Transmitter or leave it as All Devices. See *Location*, page 110, for details.
Video + Keyboard + Mouse	Use the drop-down menu to select a KVM (keyboard, video, mouse) source for the Virtual Transmitter.
Audio	Use the drop-down menu to select an audio source for the Virtual Transmitter.
USB Peripheral	Use the drop-down menu to select a USB peripheral source for the Virtual Transmitter.
Serial	Use the drop-down menu to select a serial source for the Virtual Transmitter.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to exit without saving.

Intelligent Dual Video Output Management

For RCMDVI40AT / RCMDVI40BT, the *Intelligent Dual Video Output Management* feature allows the separation of its 2 video outputs (DVI:1 and DVI:2), to be managed as two separate Virtual Transmitters. These separated outputs can be accessed from different receivers. Receivers can switch between and connect to both Virtual Transmitters independently with the *Access Type* determining which receiver has control (see page 127).

To use this setup, install the KE devices as shown below and create two Virtual Transmitters, selecting **DVI:1** and **DVI:2** as the *KVM* source for each Virtual Transmitter.

For RCMDVI00AT / RCMDVI00BT / RCMDVI50T, you can select between DVI:1 or DVI:2, but you will always be getting video output from DVI:1.

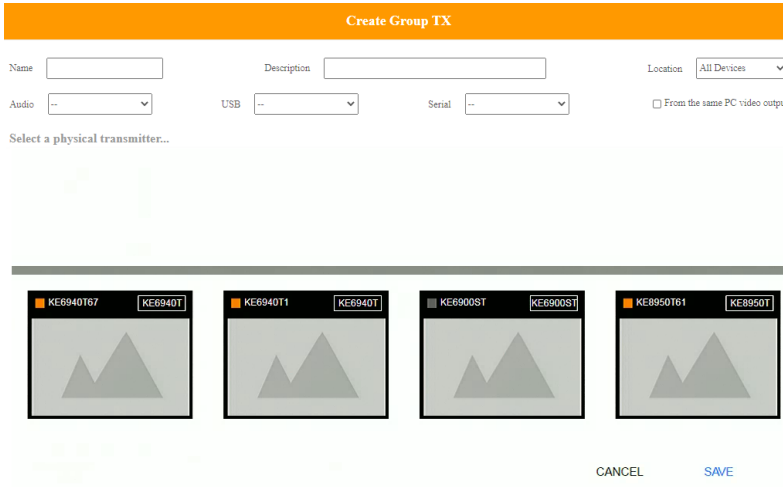


When connecting to either of the two Virtual Transmitters in the setup shown above, the mouse cursor may reside on the **main** or **extended** dual display screen, out of view. Therefore even if you have control of the mouse it may not be visible. To bring the mouse cursor into view on either of the dual display screens, first, enable Boundless Switching (see *Boundless Switching*, page 138) and then use the hotkey **F8+F9**.

Transmitter Group

Creating a *Transmitter Group* allows you to create a connection that sources the video from multiple transmitters to be viewed across multiple receiver displays. To use this feature, connect a **Transmitter Group** to a **Receiver Group** *(page 135)*. Transmitter Groups appear at the bottom of the *Transmitter* settings page.

To create a Transmitter Group, in *Transmitter* settings, click ⊕ and then select **Create Group TX**.



Fill in the appropriate information and then double-click or drag-and-drop transmitters to add or remove them in the top panel. The transmitters in the top panel will be used as the video source for the Receiver Group at the receiver.

Item	Description
Name	Enter a name for the Transmitter Group.
Description	Enter a description for the Transmitter Group.
Location	Use the drop-down menu to select a location for the Transmitter Group or leave as All Devices. See *Location*, page 110, for details.
From the same PC video output	Enable to indicate that all of the video outputs in this Transmitter Group are from the same multi-screen PC.
Save	Click **Save** to save the changes.
Cancel	Click **Cancel** to exit without saving.

Note: 1. You can create up to 4 Transmitter Groups.

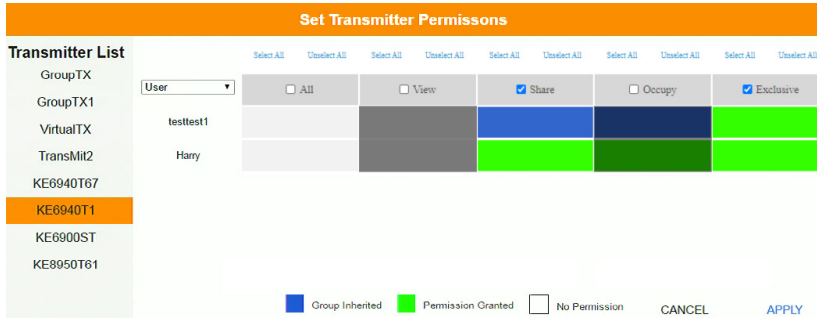
2. Any transmitter can only be added to 1 transmitter group with the *From the same PC video output* option selected at a time.

Transmitter Permissions

Transmitter Permissions sets the users and groups that can access a **Transmitter**, **Virtual Transmitter**, and **Transmitter Group**.

Select a device under **Transmitter List**, and then next to each user or group click *All*, *View*, *Occupy*, or *Exclusive* to grant them permission to connect to the Transmitter with this access type. A green block denotes that the user has access.

To set Transmitter Permissions, in *Transmitter* settings, click .

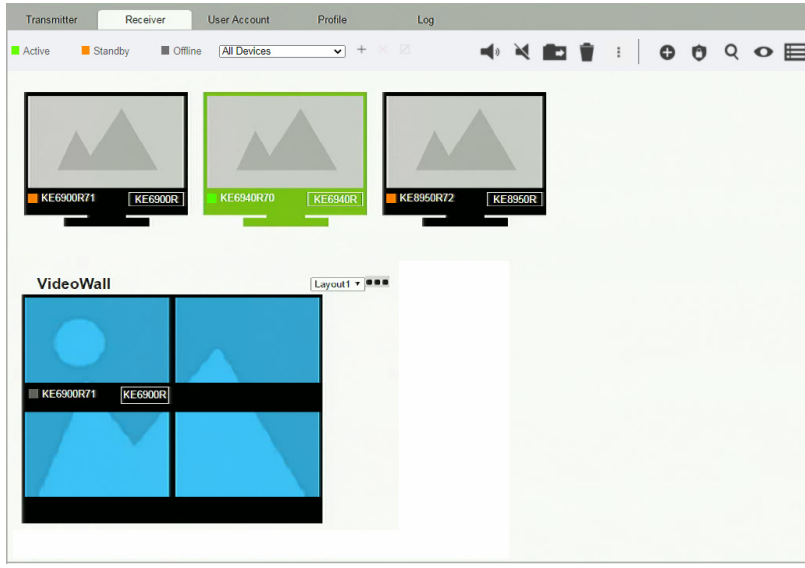


Item	Description
Transmitter List	Lists Transmitters, Virtual Transmitters and Transmitter Groups that can be selected to set permissions.
Drop-Down Menu	Use the drop-down menu to select **User** or **Group**. After making a selection, the list of users or groups appears. Set permissions by selecting the access type (All, View only, Share, Occupy, Exclusive) next to each user or group.

Item	Description
Access Type	Select the access you want to grant to a user or group by clicking the boxes under the headings. This defines how the transmitter can be accessed by a user or group. The access type will appear available for the user in the receiver's OSD Connections menu. To disable an access type, uncheck a box in the heading. **All**: Select to grant all access permissions, *View*, *Share*, *Occupy* and *Exclusive*, to the users or user groups. **View**: User can only view the remote screen, and cannot perform operations on it. **Share:** All users accessing the transmitter can simultaneously share control of the transmitter. Input from the users is placed in a queue and executed chronologically. **Occupy**: The first user to access the transmitter has control. However, additional users may view the transmitter's video. If the user who controls the transmitter is inactive for longer than the time set in the transmitter's timeout box, control is transferred to the first user to move the mouse or strike the keyboard.
Access Type	**Exclusive**: The first user to access the transmitter has exclusive control over the transmitter. No other users can view the transmitter. The Timeout function does not apply when transmitters are accessed with this setting.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to exit without saving.

Receiver

Click **Receiver** in the *System Status* panel to open the settings. The Receiver page allows you to add, delete and configure *Receivers* (physical receivers), *Receiver Groups, and Video Walls*. The KVM over IP Matrix Manager automatically adds Receivers connected to the local area network with a valid IP address.



The meanings of the icons and headings on the page are straightforward and let you view and configure receivers.

- *Active* refers to a receiver connection that is online and in use.
- *Standby* refers to a receiver connection that is online.
- *Offline* refers to a receiver connection that is offline.
- All Devices ▾ Use this drop-down menu to filter receivers by location. Use Locations to limit the receivers seen on the page.
  - Click to add a new **Location**.
  - Select a Receiver and click the **Move to** icon to add devices to a Location.
  - Select a Location from the drop-down menu and click this icon to delete it.

- Select a Location and click this icon to change the name.

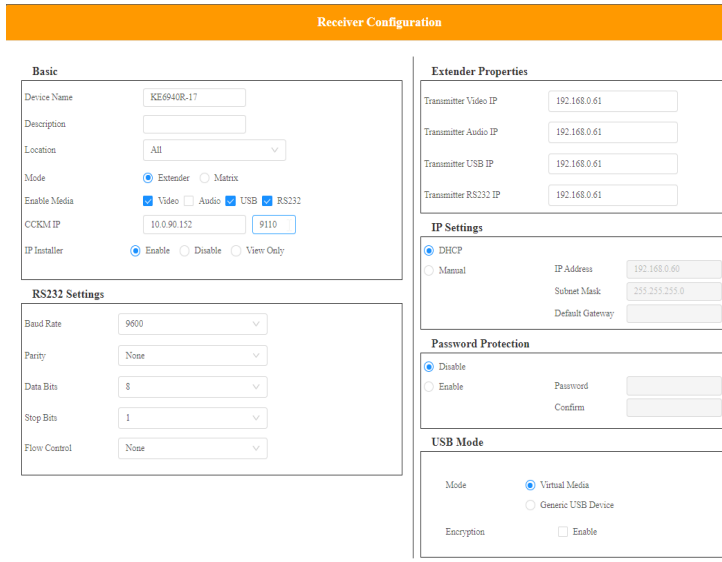
- / Click to turn Beeper & LED Flashing on/off.
- Click to delete selected receivers.
- Click an option to have selected receivers:
  - **Copy & Paste**: Copy settings from one receiver and paste them to another (see *Copy & Paste*, **page 134**).
  - **Reboot**: Shut down and restart.
  - **Reset to Factory**: Reset all setting to the factory default.

Note: The Reset to Factory function resets everything but the login information to the factory default settings. To reset the login information, refer to *Reset All Information* on page 266.

- Click to *Create Receiver Group* or *Video Wall* (*page 135 & 136*).
- Click to set receiver permissions (*page 139*).
- Click to search for receivers.
- Click to filter receivers shown on the page.
- Click to switch between *Grid View* and *List View*.

Receiver Configuration

When the KVM over IP Matrix Manager discovers receivers on the network they appear on the *Receiver* settings page. Double-click a receiver to configure its settings.



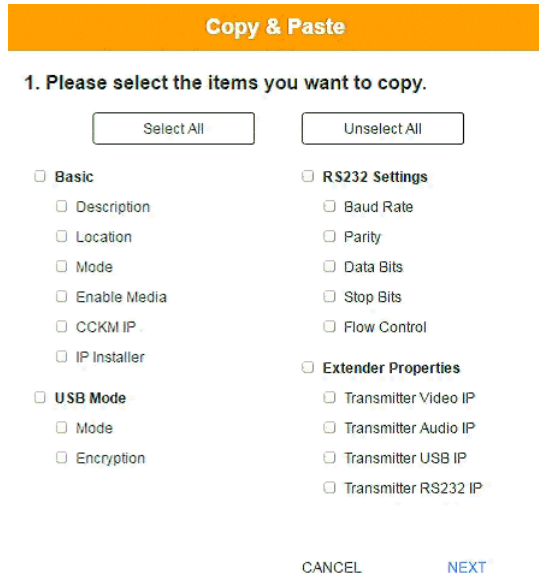
Item	Description
Basic	**Device Name:** Enter a name for the receiver. **Description:** Enter a description for the receiver. **Location:** Use the drop-down menu to select a Location for the device. Locations help organize how you view receivers on the settings page. **Mode:** Use the radio button to select how the receivers will be installed and managed: ◆ Select **Extender** mode for simple one-to-one (transmitter to receiver) setups that are managed with the receiver's OSD menu. ◆ Select **Matrix** mode to manage devices and connections over the LAN from the KVM over IP Matrix Manager. This mode is for advanced administration of transmitter and receiver connections configured within the KVM over IP Matrix Manager Web GUI. **Enable Media**: Select which source type the receiver can stream: Video, Audio, USB and RS-232. **Audio Output:** Use this option to independently stream the desired audio signals to digital or analog audio output devices (speakers) connected to the receiver. **CCKM IP:** Set the **IP** address and **Port** number of the computer running the KVM over IP Matrix Manager. The default port number is 9110. **IP Installer**: The IP Installer is an external Windows-based utility for assigning an IP address to the device. Click a radio button to select Enable, Disable or View Only for the IP Installer utility. See *IP Installer*, page 263 for instructions.
RS232 Settings	Configure the serial device settings for the receiver. The default settings are: Baud Rate: 9600 Parity: None Data Bits: 8 bits Stop bits: 1 bit Flow Control: None
Extender Properties	If you selected **Extender** mode (above) set the RCM transmitter's IP address as the source of video, audio, USB, and RS-232 source signals, to be sent to the receiver. If you selected **Matrix** mode (under Basic) the *Properties* will be grayed out. Use Transmitters, Virtual Transmitters, and Transmitter Groups to configure the connections (see *Transmitter*, page 110).

Item	Description
IP Settings	For dynamic IP address assignment, select the **DHCP** radio button. To specify a fixed IP Address, Subnet Mask, and Default Gateway select the **Manual** 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 46.
Password Protection	Select **Enable** to require a password to access the receiver's OSD configuration screen (see page 57). Enter a *Password*, and confirm the password in the *Confirm* box.
USB Mode	Select the type of USB device you will connect to the USB ports: **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. When receivers connected to the same transmitter mount or unmount USB disk drives, the keyboard and mouse operations will experience a brief delay. transmitters can support up to 12 virtual media connections at the same time (keyboard/mouse included). **vUSB (Generic USB device)**: Use this option to plug USB peripherals into the USB ports. In this mode, RCMDVI00AT / RCMDVI40AT / RCMDVI00BT / RCMDVI40BT / RCMDVI50T support up to 5 USB connections (keyboard/mouse excluded). **Encryption**: Check this box to encrypt USB disk drives plugged into the USB ports.
Replace Device	Click **Replace Device** in the top left corner to replace an old receiver with a new one.* All settings are copied from the old receiver to the new one. Before using this feature, connect the new receiver to the network. After clicking *Replace Device*, use the drop-down menu to select the new receiver where the settings will be applied. **Note:** 1. This option only appears when a receiver is offline. 2. This feature can be used for both receivers and transmitters. Replacement should be carried out on a similar model.
Save	Click **Save** to save changes to the properties.
Cancel	Click **Cancel** to exit without saving.

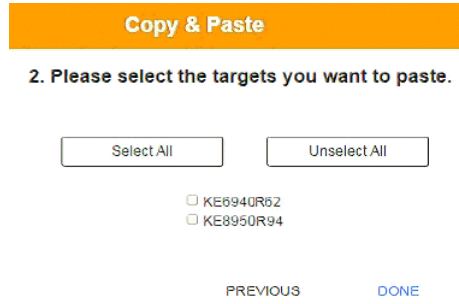
Copy & Paste

Copy & Paste allows you to copy settings from one receiver and paste them to another. To copy receiver settings to another device, do the following:

1. Select a physical receiver.
2. On the Receiver menu bar, click **Copy & Paste** (page 130).
3. Check the boxes of the settings you want to copy, and click **Next**.



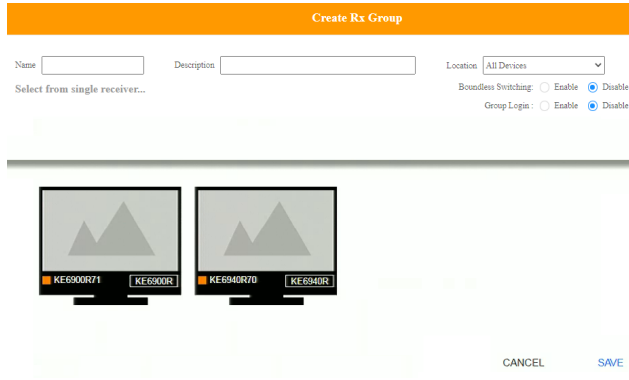
4. Select the receiver(s) where you want to apply the settings, and click **Done**.



Receiver Group

Creating a *Receiver Group* allows you to connect the video from multiple transmitters to multiple receiver displays. To use this feature, connect a **Transmitter Group** *(page 126)* to a **Receiver Group** (see *Instant Link*, page 100). Receiver Groups appear at the bottom of the *Receiver* settings page.

To create a Receiver Group, in *Receiver* settings, click ⊕ and then select **Create RX Group**.



Fill in the appropriate information and then double-click or drag-and-drop receivers to add or remove them in the top panel. The receivers in the top panel will be used to view the video from the Transmitter Group. To connect a Transmitter Group to a Receiver Group, see *Instant Link*, page 100.

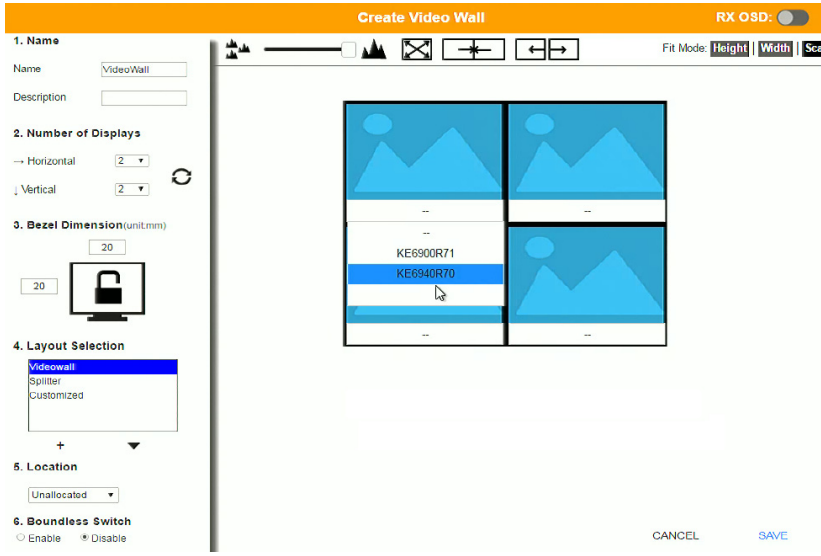
Item	Description
Name	Enter a name for the Receiver Group.
Description	Enter a description for the Receiver Group.
Location	Use the drop-down menu to select a location for the Receiver Group or leave it as All Devices. See *Location*, page 110, for details.
Boundless Switching	Use the radio button to enable or disable Boundless Switching. See *Boundless Switching*, page 138 for details.
Group Login	When enabled, users logging into or out of 1 receiver automatically logs into or out of all other receivers within the Receiver Group, using the same set of credentials.
Save	Click **Save** to save the changes.
Cancel	Click **Cancel** to exit without saving.

Note: You can create up to 4 receiver groups.

Video Wall

Creating a *Video Wall* allows you to create connections that combine receiver displays to form a large video wall. Use the options to group multiple receivers in the video wall. A video wall can contain multiple forms of single displays and grouped displays in various layouts. Video Walls are listed below Receivers, on the *Receivers* settings page.

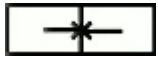
To create a Video Wall, in *Receiver* settings, click ⊕ and then select **Create Video Wall**.



Select the number of displays and then group multiple displays to form large screens and/or use single displays for independent screens to create the video wall's layout. Click the bar -- under the display icon to select a receiver for each display. This configuration should match the actual video wall layout.

Item	Description
Name	Enter a name for the Video Wall.
Description	Enter a description for the Video Wall.
Number of Displays	Use the Horizontal and Vertical drop-down menus to select the number of displays that make up the video wall (a maximum of 64 are supported). Match this to the physical layout of the displays. Click the refresh icon to update the layout.

Item	Description
Bezel Dimension	Use the two boxes to increase/decrease the frame size of each active display.
Lock / Unlock 	Click the monitor to **Lock** the (2) bezel settings, so that when one size is changed they all change. Click the monitor to **Unlock** the (2) bezel settings, so that each size can be set independently.
Layout Selection	Click **+** or X to add or remove additional layouts to the Video Wall. The options listed here will appear in a drop-down menu for the Video Wall, allowing you to quickly choose different layouts from the Receiver settings page. Arrows below the Layout Selection box allow you to move up or down in the list. Three layout templates are available for quick setup. The Videowall and Splitter options can not be changed but allow you to select the receivers. These three layouts can not be deleted. ◆ *Video Wall* provides a basic full screen layout where one transmitter connects to multiple receivers to display the video together as one full screen. ◆ *Splitter* provides a layout that connects a transmitter to multiple receivers that show the same video displayed on separate screens independently. ◆ *Customized* provides a basic full screen layout that can be configured into groups (see **Group** below) as desired.*When using the RCMDVI40AT / RCMDVI40BT in *Customized* layouts, only the its first video port will display video, because each port's video source is independent. When using the RCMDVI40AT / RCMDVI40BT in *Video Wall* or *Splitter* layouts, both video ports will display video. Video wall only supports Share, View Only and Occupy access modes.
Location	Use the drop-down menu to select a location for the Video Wall or leave it as All Devices. See *Location*, page 110, for details.
Group Login	When enabled, users logging into or out of 1 receiver automatically logs into or out of all other receivers within the Video Wall, using the same set of credentials.

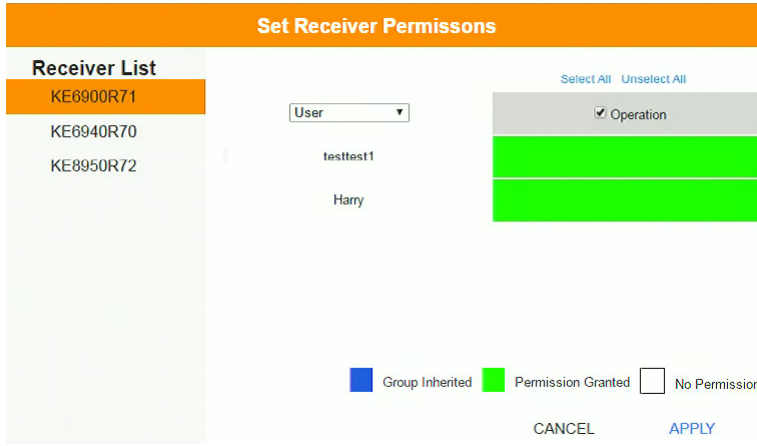
Item	Description
Boundless Switching	Enable this feature to allow you to switch KVM control between different receivers by moving the mouse cursor across screen boundaries. This option is disabled by default. When Boundless Switching is enabled, make sure to disable the following settings: ◆ On the computer, under Control Panel - Mouse Properties - Pointer Options, uncheck **Enhance pointer precision**. ◆ On the CCKM Main page, click *Settings* (page 155), then on the *General* tab scroll down and disable **Fast Switching**. **Note**: ◆ Dual-display transmitters can be set up as two independent Virtual Transmitters with Boundless Switching. The placement of the RCMDVI40AT / RCMDVI40BT setup must have DVI-1 as the main display on the left and DVI-2 as a secondary display on the right.Boundless Switching supports both single and dual video outputs from any one computer. ◆ For multi-display PCs, make sure of the following: 1. All video outputs are aligned in a row with top alignment and the main screen on the far left. 2. The transmitter's port OS has been properly set, see page 113. 3. Users can optionally group all video outputs from the same PC into a transmitter group. See p. 126. ◆ If the mouse cursor disappears under a Linux operating system, execute this command: *gsettings set org.gnome.setting-daemon.plugins.cursor active false*
	Use the slide bar to zoom in or out for a better view of the Video Wall layout.
	Click this icon to reset the zoom back to full size.
	Select multiple display icons and click the **Group** button to group the displays into one screen.
	Select a group and click **Ungroup** to ungroup the displays.
Fit Mode	Select how the video wall will be displayed: **Height**: Fits the video to the height of the display. **Width**: Fits the video to the width of the display. **Scale**: Fits the video on the entire display.

Item	Description
	Use the **RX OSD** button to enable/disable showing the receiver's name and IP address in the top left corner of the connected display. This helps identify which receiver is connected to the display.
Save	Click **Save** to save the changes.
Cancel	Click **Cancel** to exit without saving.

Receiver Permissions

Receiver Permissions sets which users and groups can access a receiver. Select a device under the **Receiver List**, and then click under Operation to grant a user or group permission to access the device. This will allow the user to log into the receiver's OSD menu to access the Connections tab.

To set Receiver Permissions, in *Receiver* settings, click  .

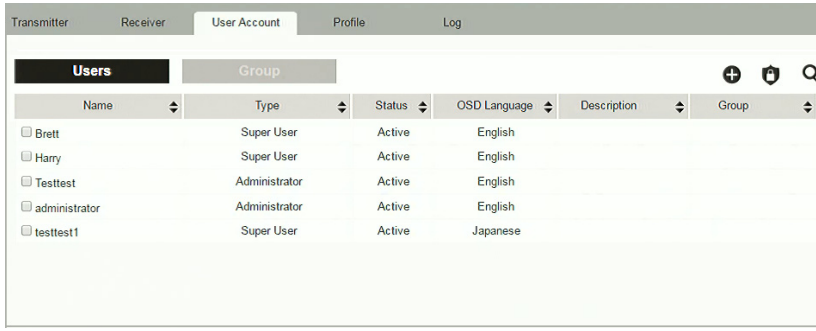


Item	Description
Receiver List	Lists the receivers which can be selected to set permissions.
Drop-Down Menu	Use the drop-down menu to select *User* or *Group*. After making a selection, the list of users or groups appears. Set permissions by selecting the Operation box next to each user or group.

Item	Description
Operation	Click the Operation box next to each user or group to apply access rights on the selected device. This gives users and groups permission to log in to the receiver's OSD. If a user inherits its permissions from a group, the box will be Blue. To disable access rights for all users, uncheck the box in the heading.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to exit without saving.

Account

Click **User**s in the *System Status* panel to open the settings. The *Account* page allows you to add, delete and configure users and groups. Instructions for adding users and groups is provide on page 141.



- The Users and Group buttons appear at the top of the page.
  - Depending on the item selected, either Users or Groups are listed on the page.
- The sort order of the information displayed can be changed by clicking the column headings.
- Three icons in the right corner are used to add users, groups and set permissions, as explained in the sections that follow.

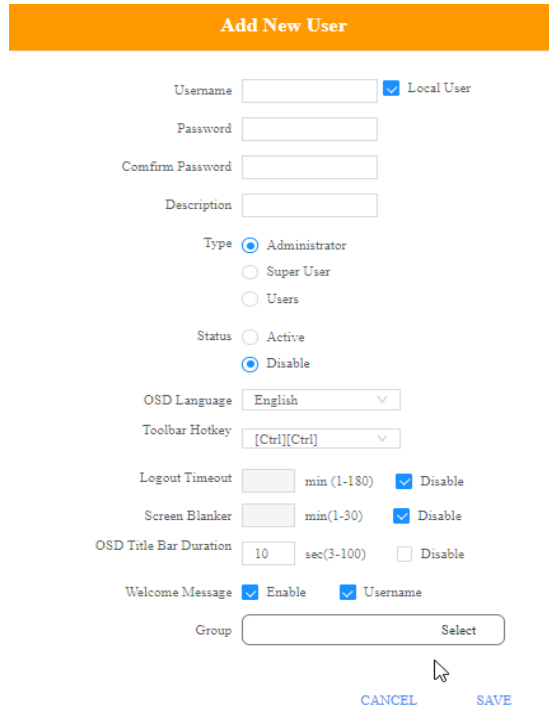
Users

The KVM over IP Matrix Manager supports three types of accounts, shown in the table below:

User Type	Role
Administrator	Access, push/pull and management of the KVM over IP Matrix Manager, including configuration and setting up of devices. Manage Users, Groups, Transmitters, Receivers, Profiles and Video Walls. Configure personal working environments.
Super User	Access and push/pull receivers, transmitters and Profiles they have been given permission for.
User	Access receivers to connect to transmitters they have been given permission for.

Adding Users

1. Click ⊕ on the menu bar.
2. Select **Add New User**. This window opens:



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

Field	Description
Username	From 1 to 32 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 KVM over IP Matrix Manager or a receiver. Uncheck the Local User box if the account is authenticated with a 3rd-party service, such as RADIUS, LDAP/AD, or TACACS+. See *ANMS*, page 162 for details.
Password	From 6 to 32 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.
Type	There are three account categories: Administrator, Super User and User. ◆ The Administrators have full access to make changes within the KVM over IP Matrix Manager, which includes adding and removing transmitters, receivers, accounts, preferences, and configuration settings. ◆ The Super Users have access to the receiver's OSD menu and can connect channels and Profiles. ◆ The Users can log in to Receivers to connect channels.
Status	Status allows you to control the user's account and access, as follows: ◆ *Active* provides the user with access and permissions as granted. ◆ *Disable* lets you suspend a user's account without actually deleting it, so that it can be easily reinstated in the future.
OSD Language	Click the drop-down menu to select the language you want to use during OSD sessions for this user. Options are: Chinese (Traditional), Simplified Chinese, Japanese, German, Korean, Russian, French, Spanish, and Portuguese.
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 KVM over IP Matrix Manager can be accessed again. The default is 30 minutes.
Screen Blanker	Sets how many minutes the device waits when a session is idle before turning off the display.

Field	Description
OSD Title Bar Duration	When accessing a port, the upper-left corner will show a title bar displaying the access mode and the device name. Select how long you wish the title bar to be displayed for, or check **Disable** to not show any title bar.
Welcome Message	If you want the Welcome Message to appear on screen when the user logs into the KVM over IP Matrix Manager, select **Enable**. If you want the user's Screen Name to appear with the Welcome Message, check the **Username** check box.
Group	Click **Select** and check a box to add the user to a group.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to exit without saving.

3. When your selections have been made, click **Apply**.
4. When the *Operation Succeeded* message appears, click **OK**.
5. The new user appears on the main panel.
   - The columns show the Username; User Level, Status, OSD Language, Description; and Group.

Modifying Users

1. In the main panel, double-click the user's name.
2. In the *Edit User* page that comes up, make your changes, then click **Apply**.

Deleting Users

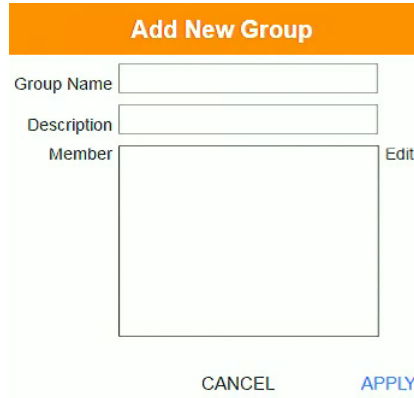
1. In the main panel, check the box next to the user's name.
2. Click  **.**
3. Click **OK**.

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. Device permissions are discussed on page 146.

Adding Groups

1. Click *Group* on the Account page.
2. Click ⊕ and then select **Add New Group**. The *Add New Group* window opens:



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 32 characters is allowed.
Description	Additional information about the user that you may wish to include. A maximum of 32 characters is allowed.
Member	Lists the users that are currently in the group. To add users, click the **Edit** button.

4. At this point you can assign users to the group by clicking **Edit**.
5. When your selections have been made click **Apply**.
6. When the *Operation Succeeded* message appears, click **OK**.

7. The new group appears in the main panel.
   - The columns show the Group Name, Description and Members that are in the group.

Repeat the above procedure to add additional groups.

Modifying Groups

1. In the main panel, double-click the group's name.
2. Make your changes, then click **Apply**.

Deleting Groups

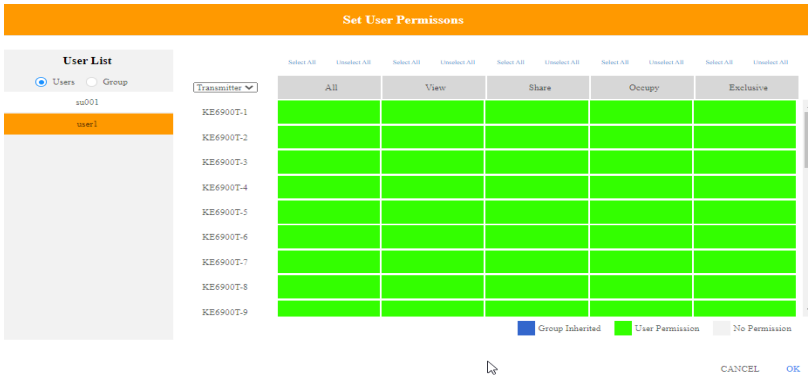
1. In the main panel, check the box next to the group's name.
2. Click  .
3. Click **OK**.

Permissions

You can assign Transmitter, Receiver and Profile permissions for users and groups from the *Account* page.

Assigning Device Permissions

1. Click  on the menu bar. The *Set User Permissions* window opens:



2. To set the permissions, select a user or group, then a device and select the Access Type under each column so that it turns green. Make your permission settings for each user or group on each device according to the information provided below:

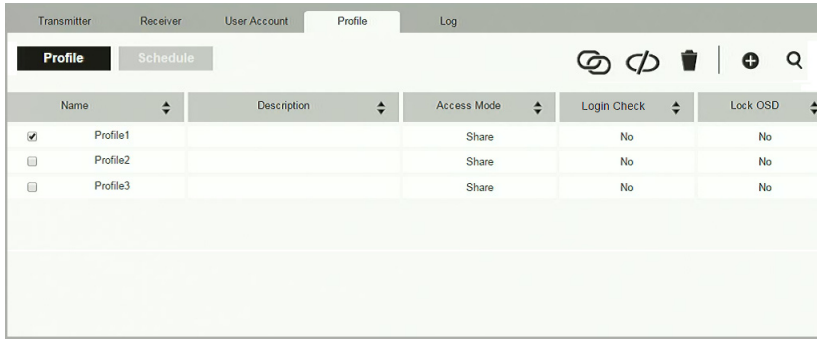
Item	Description
User List	Use the radio button to view the **Users** or **Group** list. Click a user or group to configure their permissions.
Drop-Down Menu	Use the drop-down menu to select *Transmitter*, *Receiver* or *Profile*. After making a selection, a list of devices or profiles appears. Set permissions by selecting the access type (All, View, Share, Occupy, Exclusive) next to the device.

Item	Description
Access Type	Select the access you want to grant to a user or group by clicking under the heading(s) next to each device. This defines how the device can be accessed by the user or group. When granted, the access types (All, View, Occupy, Exclusive) for transmitters will appear available for the user in the receiver's OSD Connection page (see page 74). **All**: Select to grant all access permissions, *View*, *Share*, *Occupy* and *Exclusive*, to the users or user groups. **View**: User can only view the remote screen, and cannot perform operations on it. **Share:** All users accessing the transmitter can simultaneously share control of the transmitter. Input from the users is placed in a queue and executed chronologically. **Occupy**: The first user to access the transmitter has control. However, additional users may view the transmitter's video. If the user who controls the transmitter is inactive for longer than the time set in the transmitter's Timeout box, control is transferred to the first user to move the mouse or strike the keyboard. **Exclusive**: The first user to access the transmitter has exclusive control over the transmitter. No other users can view the transmitter. The Timeout function does not apply when transmitters are accessed with this setting. **Operation** (Receiver and Profile): ◆ **Receivers:** allows users to log into receivers ◆ **Profiles:** allows a user to connect the Profile from a receiver.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to exit without saving.

3. When you have finished making your choices, click **Apply**.
4. In the confirmation popup that appears, click **OK**.

Profile

Click **Profile** in the *System Status* panel to open the settings. The *Profile* page allows you to create, run and schedule connection profiles. Profiles channel specific receiver to transmitter connections and can be instantly connected from the Profile page at anytime. Profiles can be also scheduled to run automatically at specific times.



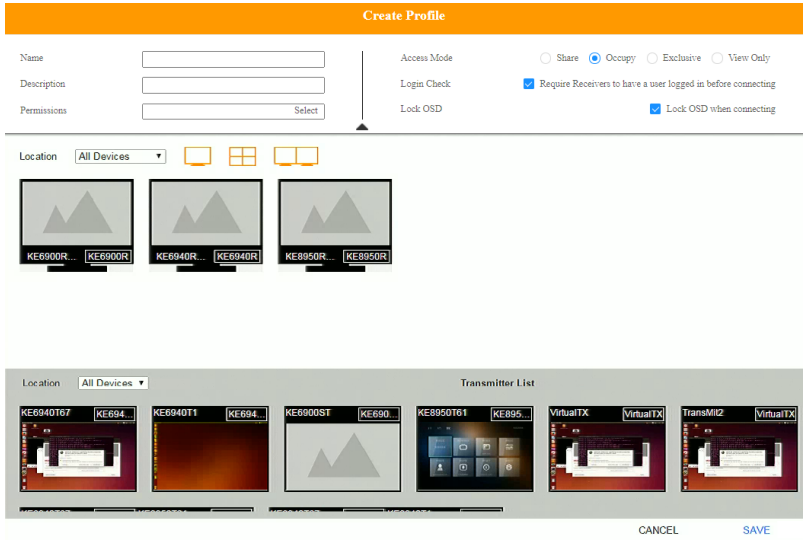
The meanings of the icons and headings on the page are straightforward and let you view and configure Profiles.

- Click to connect the selected Profile.
- Click to disconnect the selected Profile.
- Click to delete the selected Profile.
- Click to *Create Profile* or *Create Schedule* (page 149 & 151).
- Click and enter text to search for a Profile.
- Check the box next to a **Profile** and click the *Connect* or *Disconnect* icon to start/stop profile connections. Check the box next to a **Schedule** and click the *Enable* or *Disable* icon to enable/disable a schedule.
- Appears on the *Schedule* page, click to enable the selected schedule.
- Appears on the *Schedule* page, click to disable the selected schedule.

Adding a Profile

Creating a Profile allows you to quickly connect single or multiple receiver to transmitter connections.

1. On the *Profile* page click ⊕ and then select **Create Profile**. The *Create Profile* window appears:



Item	Description
Name	Enter a name for the Profile.
Description	Enter a description for the Profile.
Permissions	Click **Select** and check the box of the users / groups you want to allow to connect this Profile. When the user logs into a receiver, the profile will appear listed in the OSD menu on the Profile page (see page 78), allowing them to connect it.

Item	Description
Access Mode	This defines how the transmitters in a Profile can be accessed by receivers when multiple users attempt to access it. **View Only**: Receivers only have view access to the transmitter's video display. **Share:** All users accessing the transmitter can simultaneously share control of the transmitter. Input from the users is placed in a queue and executed chronologically. **Occupy**: Set a time threshold for receivers whose Access Mode has been set to Occupy If there is no activity from the receiver occupying the port for the amount of time set here, the receiver is timed out and the port is released. The first receiver 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. **Exclusive**: The first receiver to access the transmitter has exclusive control over the transmitter. No other users can view the transmitter. The Timeout function does not apply to transmitters which have this setting.
Login Check	Check this box to require a user to be logged in to the receiver before a Profile can connect it to a transmitter. When enabled, a user must be logged into the receiver or it will not connect to the transmitter when the Profile is initiated.
Lock OSD	Checking this box will lock the receiver's OSD screen when the Profile connects it to a transmitter.
Location	Use the drop-down menu to select a location to filter the receivers displayed on the page.
	Click this icon to show individual receivers.
	Click this icon to show only Video Wall receivers.
	Click this icon to show only Receiver Group receivers.
Save	Click to save the changes.
Cancel	Click to exit without saving.

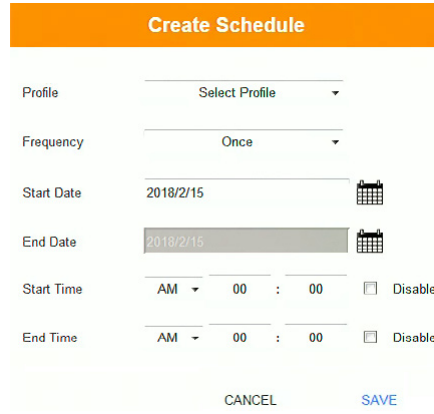
2. After filling in the information, click a receiver, select **Select TX** and use the drop-down menu select a transmitter; or use *Transmitter List* at the bottom of the page to drag-and-drop transmitters to receivers to create the connection.

3. After configuring the connections, click **Save**. The new Profile appears on the *Profile* page.
4. To connect Profiles, check the box of the Profile(s) you want to connect, and click .
5. To disconnect Profiles, click .

Adding a Schedule

Creating a Schedule allows you to connect Profiles at specific dates, times and intervals.

1. On the *Profile* page click **Schedule**.
2. Click and then select **Create Schedule**. The Create *Schedule* window appears:



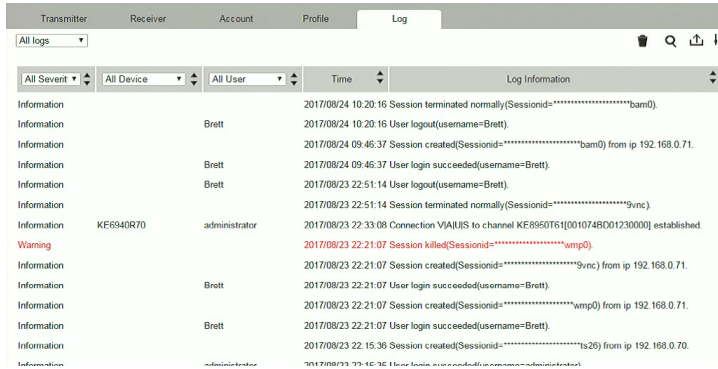
Item	Description
Profile	Use the drop-down menu to select a Profile to schedule.
Frequency	Use the drop-down menu to select how often the Profile should run: Once, Daily, Weekly and Monthly. When you select **Weekly/Monthly** an additional drop-down menu appears to select the *Week Day/Month Day* on which the profile will run.
Start Date	Enter the date on which you want the schedule to begin running.
End Date	Enter the date on which you want the schedule to stop running.

Item	Description
Start Time	Enter the time of day that you want the profile to connect.
End Time	Enter the time of day that you want the profile to disconnect.
Every	If you select Daily, Monthly or Weekly, the *Every* option appears allowing you to enter how often you want the schedule to run. For example, enter **3** months if you want the profile to run once every three months. If you want to run the schedule once a day, once a week or once a month, use the default entry of 1.

3. After the schedule is configured, click **Save**.

Log

Click **Log** in the *System Status* panel to open the settings. The *Log* page lists events that take place and provides a breakdown of the time, user, severity, device, and log information. You can change the sort order of the display by clicking on the column headings.



- Click the drop-down menu beside a heading to filter events into subcategories. Selecting a subcategory allows you to view only the logs that relate to the choice. The meanings of the headings at the top of the page are straightforward:
  - *All Severity* refers to the event's severity type: Information, Error, or Warning
  - *All Device* refers to the transmitter or receiver that relates to the event. If no device is listed the event refers to the KVM over IP Matrix Manager.
  - *All User* refers to the username that the event relates to. If no username appears, the event is general system information.
  - *Time* refers to the date and time that the event occurred.
  - *Log Information* provides detailed information about each event.
- Click to delete the logs currently displayed in the list.
- Click and enter text to search for an event log.
- Click to save the log contents to a file on your computer.
- Click to open a pop-up window that allows you to set how many days or the number of records to record before over-writing old log files. Use the radio button to select *By Period (Days)* or *By Records* and enter the number to use before overwriting the oldest log files.

This Page Intentionally Left Blank

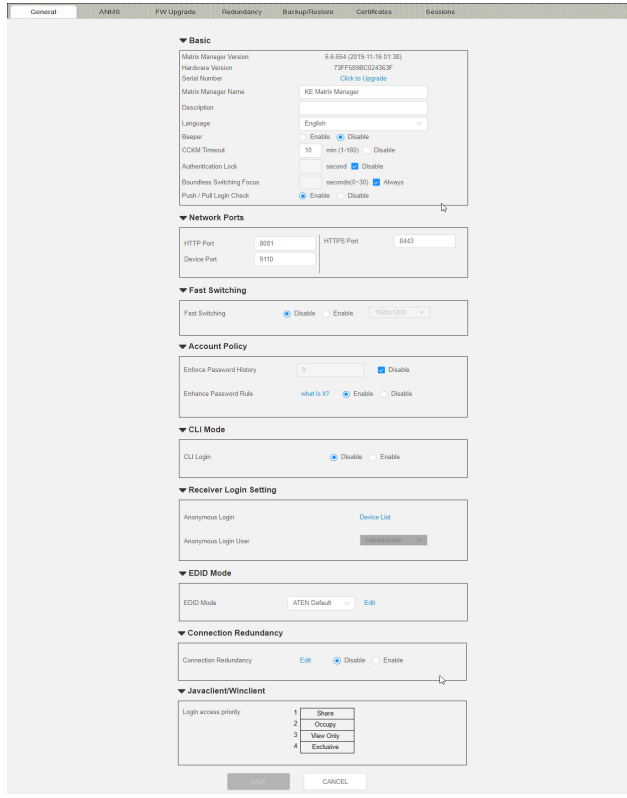
Chapter 8
System Settings

Overview

The *System Settings* are accessed by clicking from the **System Status** page (see *System Status*, page 107). There are 7 tabs to configure the RCM/KE Manager system settings: *General*, *ANMS*, *FW Upgrade*, *Redundancy*, *Backup/Restore*, *Certificates*, and *Sessions*.

General

Clicking from the system status page opens the *General* tab, as shown below:



Heading	Item	Description
Basic	RCM/KE Manager Version	This provides the version of the RCM/KE Manager software.
	Serial Number	This provides the serial number and a link to upgrade the software.
	RCM/KE Manager Name	Enter a name for the RCM/KE Manager.
	Description	Enter a description for the RCM/KE Manager.
	Language	Select the language for the RCM/KE Manager. Choices are: English, Chinese (Traditional), Simplified Chinese, Japanese, German, Korean, Russian, French, Spanish, and Portuguese.
	Beeper	Select **Enable** to sound a beep from the transmitter / receiver every time a configuration change is made.
	CCKM Timeout	If there is no user input for the amount of time entered in the box, a user logged into the CCKM is automatically logged out. Check **Disable** to turn this function off.
	Authentication Lock	When accidental power cut happens, the function allows the user to retain his/her settings as was shown before the power cut. The user keeps the same authentication and display. ◆ Uncheck **Disable** to turn this function on. ◆ Specify a time (in seconds) you wish to keep the authentication and display for. When disabled or, if enabled, after the time specified above, the manager will prompt you to authenticate when you wish to access the KE Manager.
	Boundless Switching Focus	When using Boundless Switching(see *Boundless Switching*, page 135) across multiple receivers within a receiver group or video wall, a colored border is shown on the receiver display currently being accessed (focus receiver). ◆ Uncheck **Always** to only display the colored border for a set time interval immediately after switching the focus receiver. ◆ Specify a time (in seconds) you wish to display the colored border for upon switching the focus receiver.
	Push / Pull Login Check	Enable to check the access rights of the users receiving transmitter sessions upon push / pull.

Heading	Item	Description
Network Ports	HTTP Port	Sets the HTTP service port used to access the RCM/KE Manager. This is the port number to use for a browser login. The default is 8080.
	Device Port	Sets the device service port used to access the RCM/KE Manager. Configure this port number on the transmitter and receiver to match the RCM/KE Manager software (see *Manager Address,* page 61 and 65). The default is 9110.
	HTTPS Port	Sets the HTTPS service port used to access the RCM/KE Manager, for secure browser login. The default is 8443. Example: To access the RCM/KE Manager with an IP address of 192.168.0.100 using a secure browser login, enter: *https://192.168.0.100:8443*
Fast Switching		Select the default resolution to use so that you can switch faster when changing receiver-to-transmitter connections. If the monitor you are using does not support fast switching, the video may not display correctly when this setting is enabled. **Note:** Make sure to disable Boundless Switching when Fast Switching is enabled.
Account Policy	Enforce Password History	This setting determines the number of unique new passwords that must be used before an old password can be reused. Uncheck the box and enter a number to enforce the password history policy.
	Enhance Password Rule	Select **Enable** to enforce rules for creating passwords, as follows: ◆ The password length must be at least 8 characters. ◆ The password must contain both upper and lowercase characters. ◆ The password must contain a number (0 through 9). ◆ If a user types in the wrong password 5 times consecutively, their account will be locked out for 10 minutes.

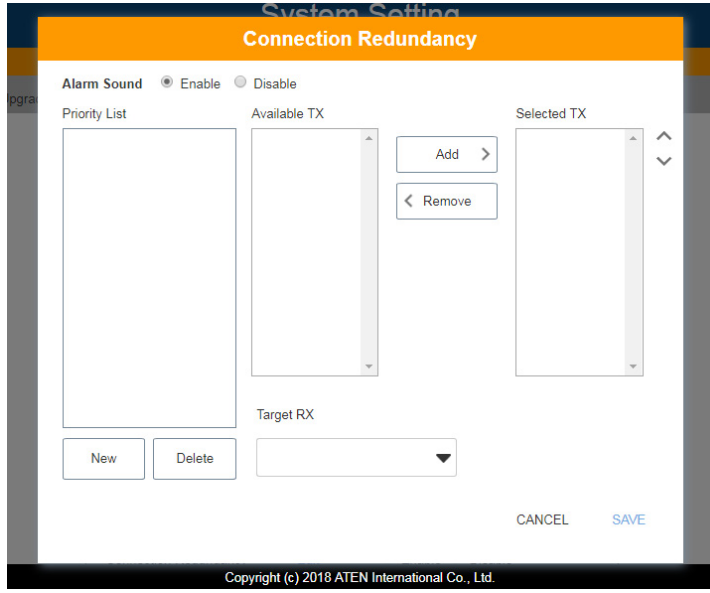
Heading	Item	Description
CLI Mode	CLI Mode Login	Use the radio button to Enable or Disable command line interface logins to the RCM/KE Manager. **Warning**: If *Disable* CLI Mode Login is selected, anybody can login via Telnet with administrator privileges without needing to authenticate, allowing control of the entire installation. For installations requiring a high level of security, it's recommended that *Enable* CLI Mode Login be applied.
Receiver Login Settings	Anonymous Login	Use this to anonymously log in a user at select receivers. This option allows users to access the receiver and connect to transmitters without login. Click **Device List** to display the list and check the box next to the receiver(s) to enable the *Anonymous Login* feature.
	Anonymous Login User	When *Anonymous Login* (above) is enabled for receivers, select a user from the drop-down menu to use as the default account for anonymous login to the receiver.
EDID Mode	EDID Mode	Use this drop-down menu to set the default EDID mode for all transmitters. To set a different EDID mode for each transmitter, use the drop-down menu to select **Customized** and then click **Edit**. A transmitter list will appear with drop-down menus to configure each device's EDID mode.
Connection Redundancy		Use this drop-down menu to set connection redundancy function. You can set up priority connection with this function. Please refer to *Connection Redundancy* on page 158.
Save		Click to save the changes.
Cancel		Click to cancel the changes.

Connection Redundancy

You can set up priority connection for receivers. Where a transmitter fails, this function allows the receiver to connect to the transmitter of the highest priority that is available.

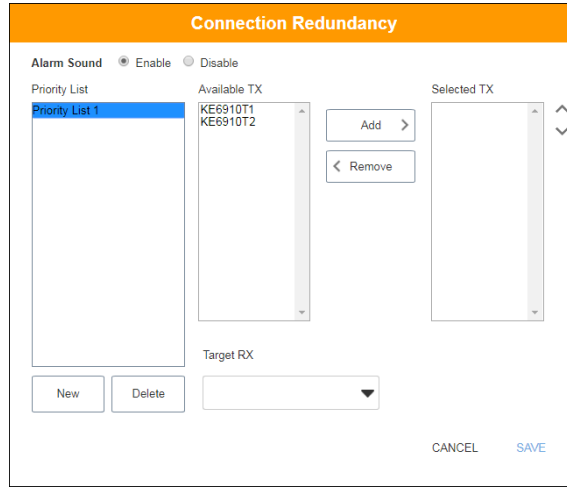
Follow the steps below to set up the priority list.

1. Click **Enable** to enable this function.
2. Click **Edit**. A window will pop-up to allow editing.

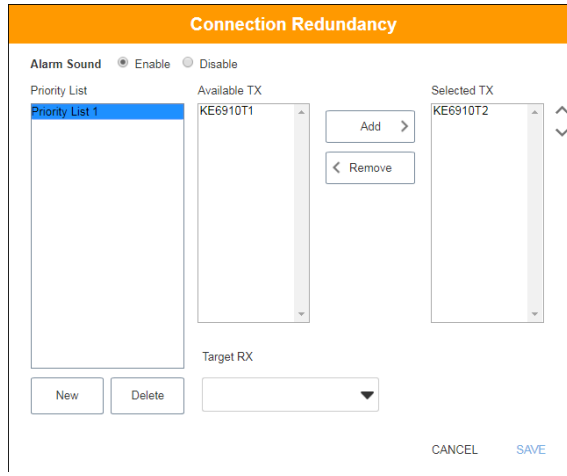


3. For Alarm Sound, click **Enable**.

4. To create a new list, click **New**. A Priority List 1 will be shown. (Click **New** again to create another list.)

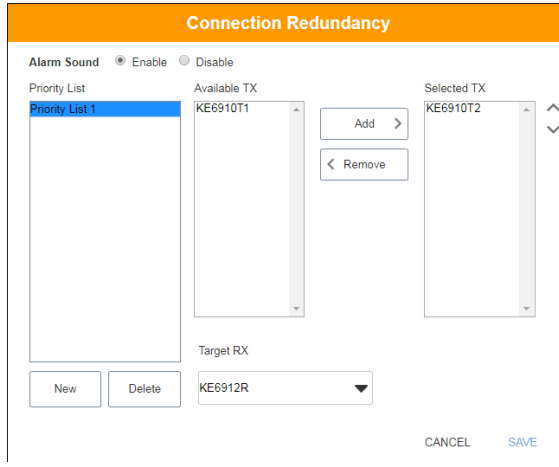


5. Select the transmitters you wish to be in the list from the “Available TX” list and click **Add**. The added transmitter will be shifted to the “Selected TX” list.



To deselect the transmitter, click to select the transmitter from the “Selected TX” list and click **Remove**. The transmitter will be shifted back to the “Available TX” list.

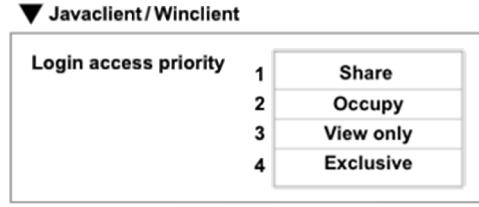
6. Select a target receiver by first clicking the drop-down menu “Target RX”, and select a receiver.



7. Repeat steps 4-6 to add more priority lists.
8. Click **Save** to save the settings.

Login Access Priority

"JavaClient/WinClient" shall appear at the bottom of the *General* tab to let you select the login access priority depending on the user.



Share: User has full control and can simultaneously share control of the remote viewer. Input from the users is placed in a queue and executed chronologically.

Occupy: The first user to access the remote viewer has control. However, additional users may view the remote viewer. If the user controlling the remote viewer is inactive for longer than the time set in the transmitter's Timeout box, control is transferred to the first user to move the mouse or strike the keyboard.

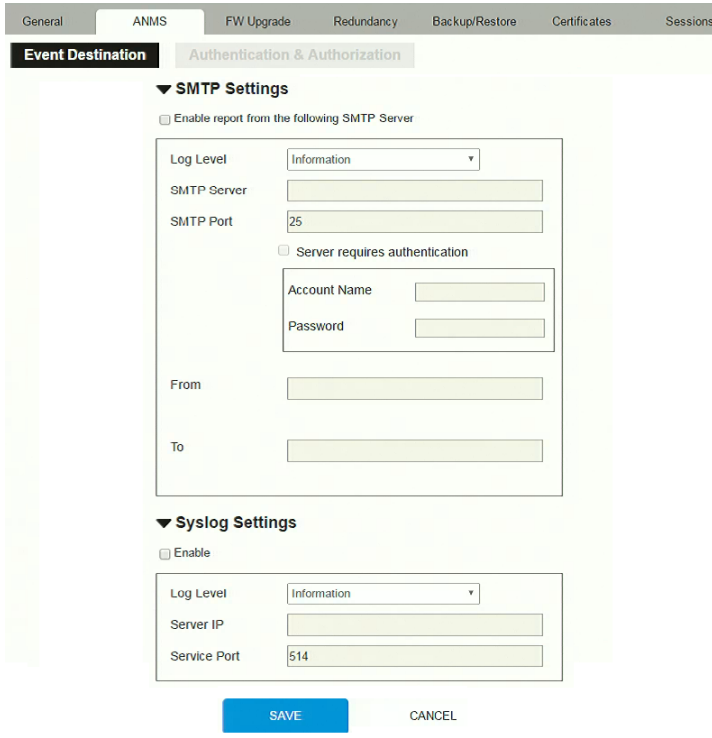
View only: User can only view the remote viewer but cannot perform operations on it.

Exclusive: The first user to access the remote viewer has exclusive control. No other users can view the remote viewer. The Timeout function does not apply when transmitters are accessed with this setting.

ANMS

The *ANMS* (Advanced Network Management Settings) tab is used to set up login authentication and authorization management from external sources, and SNMP configurations.

Event Destination



- *SMTP Settings*

  To have the RCM/KE Manager email reports from the SMTP server to you, do the following:

  1. Enable the *Enable report from the following SMTP Server*, select 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**.

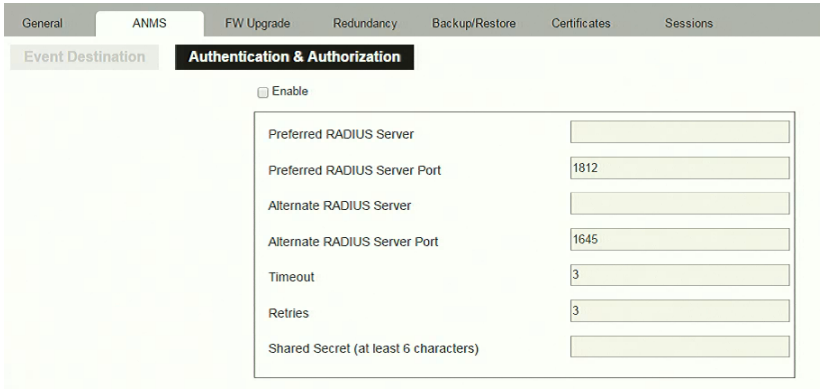
1. Once set, an SMTP report will be sent to the recipients for every 100 logs accumulated or once every 30 minutes.
2. An immediate SMTP report will also be sent whenever an error log occurs.

- *Syslog Settings*

To record all the events that take place on the RCM/KE 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



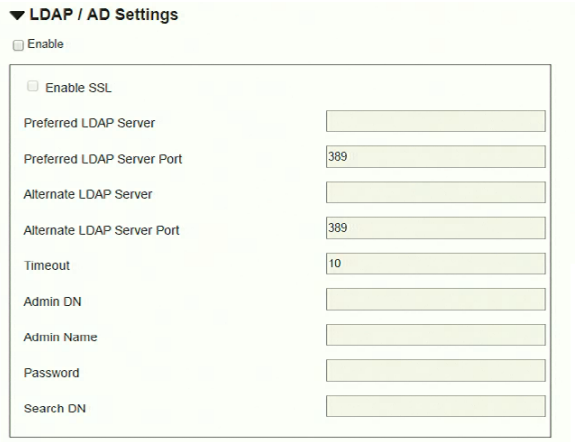
- *RADIUS Settings*

  To allow authentication and authorization 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 RCM/KE 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 RCM/KE 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:
     - Use the same Username on both the RADIUS server and the RCM/KE Manager.
     - Use the same Group name on both the RADIUS server and the RCM/KE Manager.
     - Use the same Username/Group name on both the RADIUS server and the RCM/KE Manager.

     In each case, the user's access rights are the ones assigned that were assigned when the User or Group was created on the RCM/KE Manager.

- *LDAP / AD Settings*:



To allow authentication and authorization for the RCM/KE 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 RCM/KE 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.

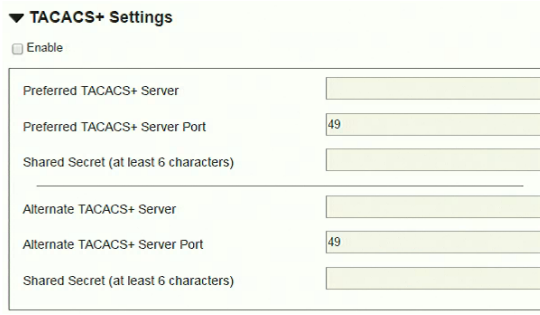
On the LDAP / AD server, Users can be authenticated with any of the following methods:

- 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 RCM/KE Manager are matched to the names on the LDAP / AD server. User privileges are the same as the ones configured in the RCM/KE Manager.

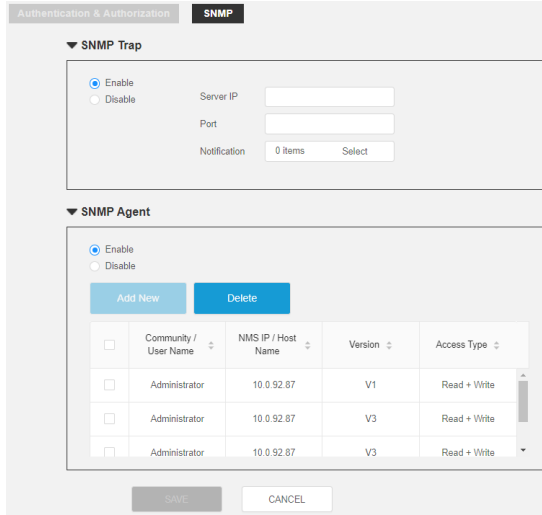
- Without schema – Only the Usernames used on the RCM/KE Manager are matched to the names on the LDAP server. User privileges are the same as the ones configured in the RCM/KE Manager software.
- Without schema – Only Groups in AD are matched. User privileges are the ones configured for the groups he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

- *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

SNMP



- *SNMP Trap & SNMP Agent*

  To be notified of SNMP trap events, do the following:

  1. Check **Enable** SNMP Trap.
  2. Enter the **Server IP** and the **Port** of the PC / server to be notified of SNMP trap events.
  3. Next to **Notification**, click **Select** and check the types of events for sending SNMP notifications.
  4. Check **Enable** SNMP Agent.
  5. Check / uncheck the SNMP Agents for sending SNMP trap events.

  Note: To add additional SNMP Agents, you must first **Disable** SNMP Agent.

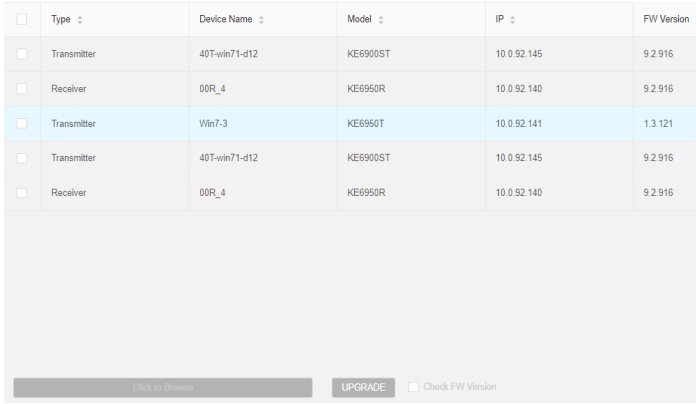
  6. Click **Save**.

FW Upgrade

In *FW Upgrade* all RCM/KE devices that are online are listed, allowing you to select which devices get upgraded. New firmware versions can be downloaded from our website as they become available. Check the website regularly to find the latest upgrade packages.

To upgrade the firmware do the following:

1. Go to our website and download the firmware upgrade package appropriate to your RCM/KE device.
2. Open your browser and log in to the RCM/KE Manager with an administrator's account.
3. Click the **Settings** icon; select the **FW Upgrade** tab, the *FW Upgrade* page appears:



All the devices that are capable of being upgraded are listed.

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

4. Check the checkbox in front of the devices you want to upgrade. Uncheck the devices that you do not want to upgrade.
5. Click **Browse**. Navigate to the directory where the firmware upgrade file is located and select it.
6. Enable or disable *Check FW Version*
   - If you enabled *Check FW 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 FW Version*, the upgrade file is installed without checking what its level is.
- If you cancel the firmware upgrade, you have to wait 12 seconds before you can disable *Check FW Version* and restart the firmware upgrade.

7. 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.
8. Log in to each device 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 RCM/KE device.
2. Press the **Reset** button, then power on the RCM/KE device while holding Reset.
3. Hold **Reset** for 7 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.

Redundancy

The *Redundancy* tab allows you to set up a backup computer in case the computer hosting the RCM/KE Manager goes offline. If the RCM/KE Manager goes offline, the secondary computer will automatically take over operations, allowing all connections to continue without disruption – with only a brief period of 30 seconds when new connections can't be started. When the primary computer comes back online it retrieves the updated database from the secondary computer and re-takes all RCM/KE Manager operations.

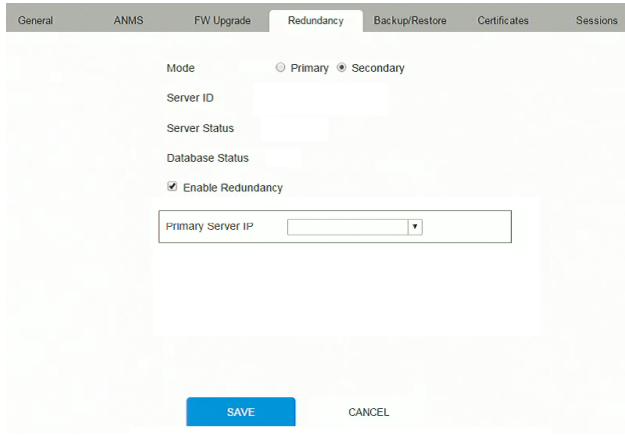
Note: A CCKM supports up to 5 secondary servers.

To set up Redundancy, do the following:

1. Install RCM/KE Manager on a secondary computer with a USB license key. For detailed instructions, see page 88.

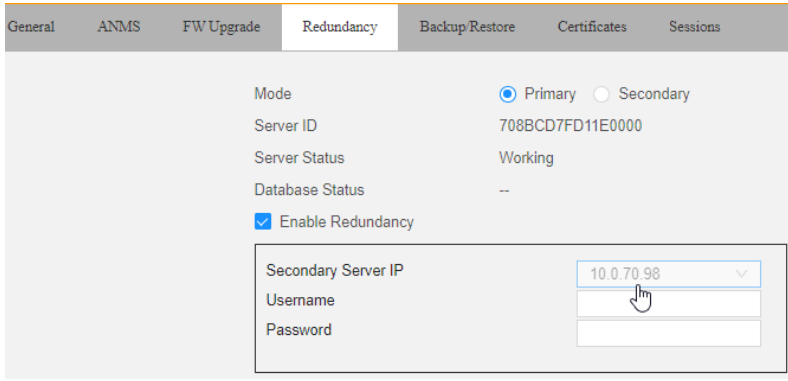
   Note: A second USB license key is required if you have more than 8 KE Series devices in your setup.

2. On the secondary computer, log in to the RCM/KE Manager, click  and go to the *Redundancy* tab.



3. Check **Enable Redundancy** and select the **Secondary** radio button.
4. Use the **Primary Server IP** drop-down menu to select the primary IP address.
5. Click **Save**.

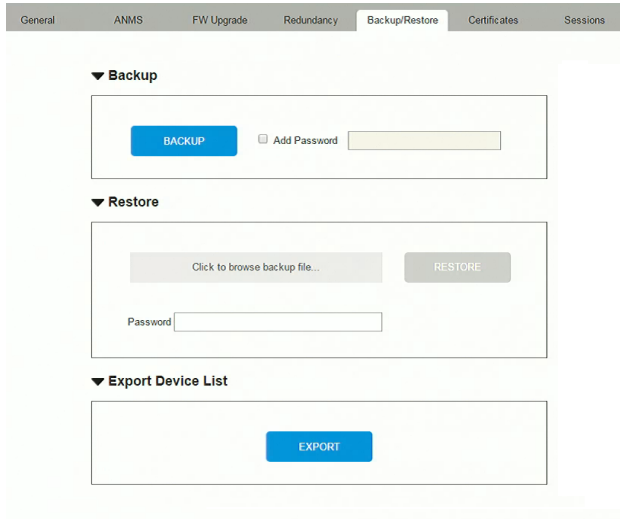
6. Redundancy is now running on the secondary computer.
7. On the primary computer, log in to the RCM/KE Manager, click and go to the *Redundancy* tab.



8. Check **Enable Redundancy** and select the **Primary** radio button.
9. Use the **Secondary Server IP** drop-down menu to select the secondary IP address.
10. Enter the **Username** and **Password** of the secondary computer's local administrator account.
11. Click **Save**.
12. Information about the *Redundancy* status can be found in the event log (see *Log*, page 153 for details).

Backup / Restore

The *Backup/Restore* tab is divided into three panels: **Backup**, **Restore**, and **Export Device List**:



The operations to perform backup/restore procedures are described in the table below and in the section that follows:

Procedure	Operation
Backup	Backs up theRCM/KE Manager configuration – including profile and schedule configurations, user and group accounts, user profiles, logs, and system settings.
Restore	Deletes the current profile and schedule 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.
Export Device List	Clicking **Export** allows you to save a file with a complete list of the devices added to the RCM/KE Manager. The file contains the ID, name, description and IP address of each transmitter and receiver. An Existing column also lists if the device is available: Yes, it exists and is available, or No, it is offline or has been removed.

Backup

To back up system configuration settings, do the following:

1. (Optional) In the *Backup* panel, check **Add Password**, and provide a password for the backup file.

   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.

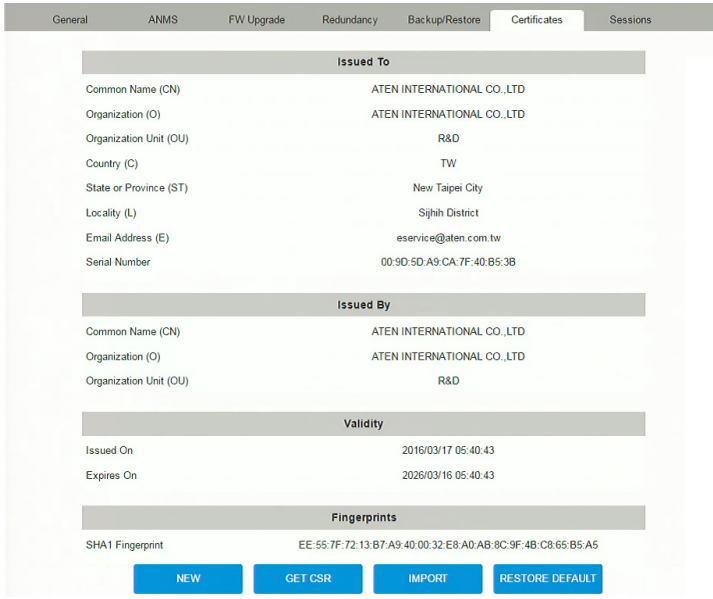
   Note: If you did not set a password for the file, leave the field blank.

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 RCM/KE Manager will restart will appear. After a short while the RCM/KE 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.

Certificates

This tab provides information about *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 265 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.

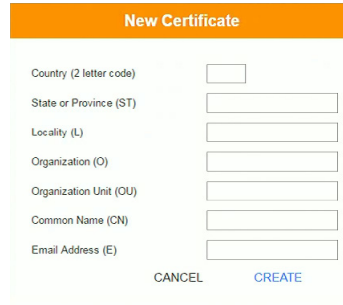
Note: Clicking Restore Defaults returns the device to using the default ATEN certificate.

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
State or Province	Taiwan

Information	Example
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 RCM/KE Manager software.

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.

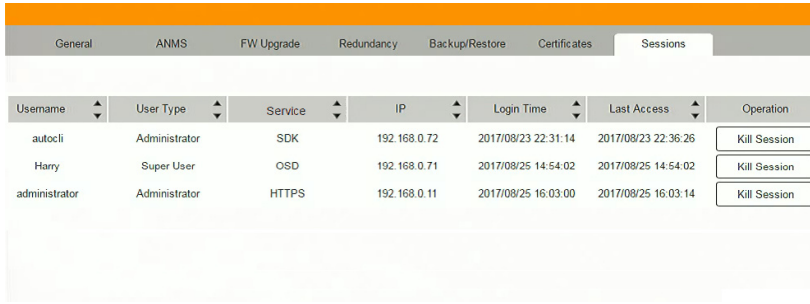
5. After the CA sends you the certificate, save it to a convenient location on your computer. Click **Import** to locate the file; then click **Import** to store it on the RCM/KE Manager.

Note: When you upload the file, the RCM/KE 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**.

Sessions

The *Sessions* tab shows all of the users that are logged into RCM/KE Manager and OSD sessions 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** next to each user.



- *Username* refers to the user that logged in to establish a session.
- *User Type* refers to the account type of the user.
- *Service* refers to how the user logged into their session – via RCM/KE Manager, Command Line, or OSD.
- *IP* refers to the IP address from which the user has logged in.
- *Login Time* refers to the date/time that the user logged into the session.
- *Last Access* refers to the last time the user session was active.
- *Operation* provides the **Kill Session** button to force a user logout.

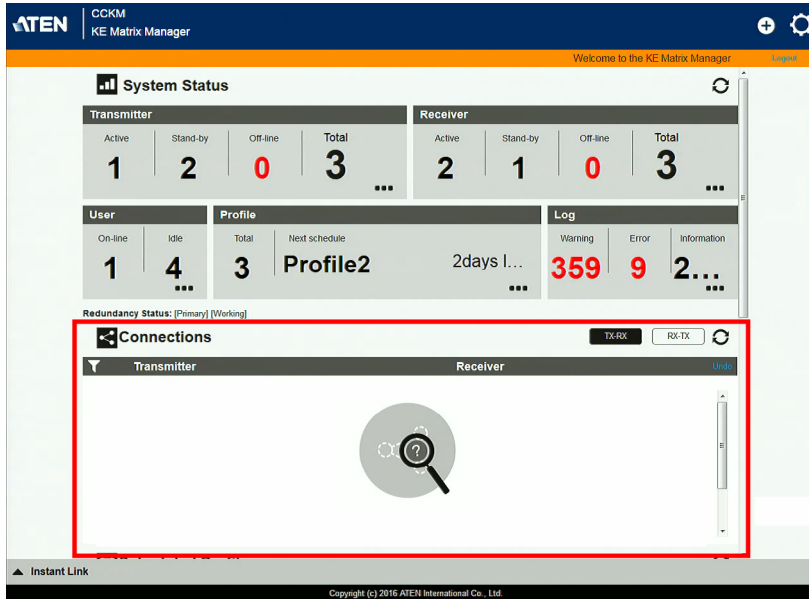
This Page Intentionally Left Blank

Chapter 9
Connections

Overview

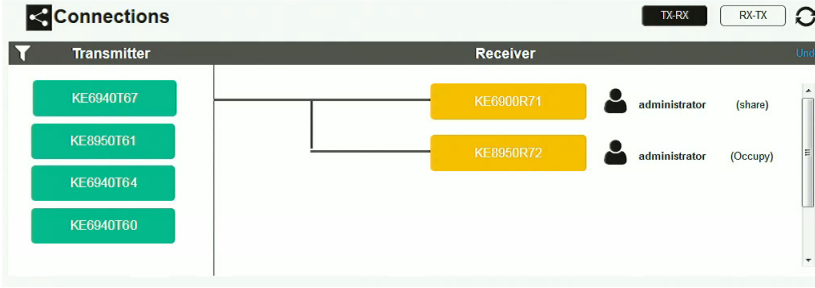
The *Connections* panel is found on the **KVM over IP Matrix Manager** main page, just below System Status. Connections provides a diagram of current transmitter-to-receiver connections. Before connections are established, the panel appears blank, as shown below. To connect receivers to transmitters, use the *Instant Link* panel (page 100), or create a connection *Profile* (page 148).

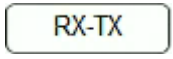
When connections are made, clicking a device in the left column provides a way to view the connection, hovering the mouse cursor over the connection diagram in the right column allows you to disconnect the device, as explained in the sections that follows.



Connections

When receivers connect to transmitters, they appears in the *Connections* panel. There are two columns – each lists either Transmitters or Receivers. The columns can be swapped by clicking the **TX-RX** or **RX-TX** button. Devices in the left column can be clicked to display their connection to devices, shown in the right column. Connections, shown in the right column, can be disconnected by clicking the **X** over the connection diagram.



Item	Description
	On the heading bar under *Connections*, click this icon to change the sort order of the transmitters or receivers listed in the left column.
Left Column	Click a device in the left column to view its connection in the right column. A diagram to its connected device(s) appears in the right column.
Right Column	The right column displays a connection diagram when a device in the left column is selected. Move the mouse cursor over the diagram and click **X** to disconnect the devices. This column also shows the user and access type (Exclusive, Occupy, Share, View Only) used to establish the connection.
Transmitter	Lists transmitters that are online and connected to receivers.
Receiver	Lists receivers that are online and connected to transmitters.
	Click to view transmitter-to-receiver connections. This will list transmitters in the left column so that they can be selected to view their connection diagram, shown in the right column.
	Click to view receiver-to-transmitter connections. This will list receivers in the left column so that they can be selected to view their connection diagram, shown in the right column.

Item	Description
	Click this icon to Refresh the Transmitters and Receivers list in Connections panel.
Undo	Click this icon to undo the most recent disconnection.

Based on the different access types, users attempting to connect to device ports that are already being accessed by another user may or may not be able to connect. See the table below for scenarios where users are granted (O) or denied access (X).

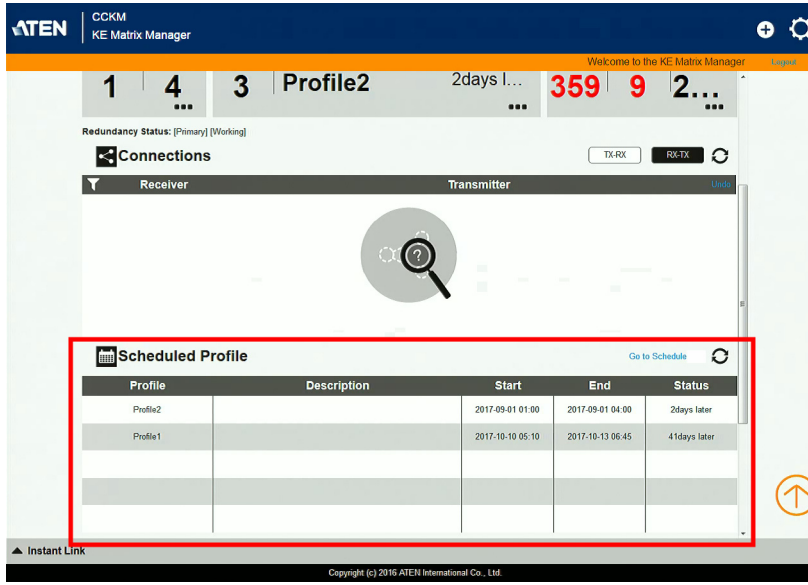
New Connect Attempt / Currently Connected	Exclusive	Share	Occupy	View Only
EXCLUSIVE	X	X	X	X
Share	X	O	X	O
Occupy	X	X	O	O
View Only	X	O	O	O
None	O	O	O	O

This Page Intentionally Left Blank

Chapter 10
Scheduled Profile

Overview

The *Scheduled Profile* panel is found on the **KVM over IP Matrix Manager** main page, just below Connections. Scheduled Profiles displays connection profiles that have been scheduled. Click **Go to Schedule** to edit and create profile schedules (page 151). To create Profiles, see page 149.



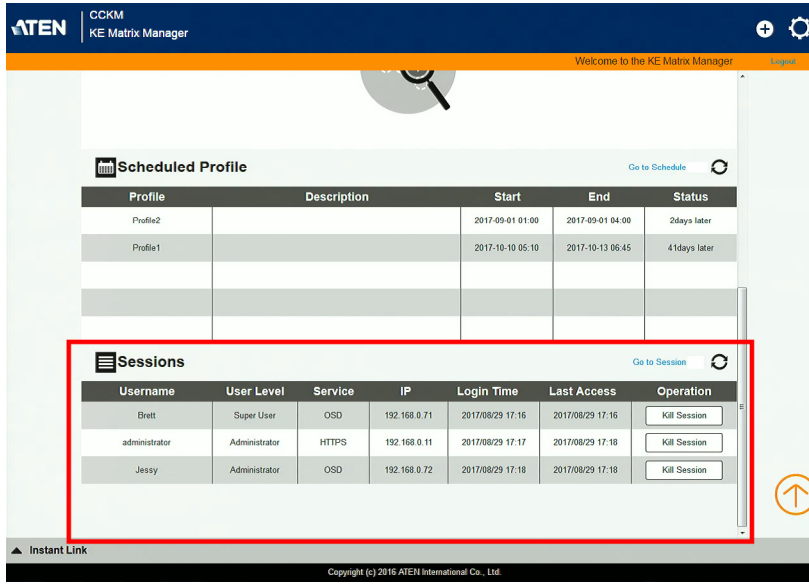
Item	Description
Headings	The headings provide the schedules: *Name*, *Description*, *Start*, *End*, and *Status*. **Start** and **End** show the time/date the profile is scheduled to begin and end. **Status** displays the number of days until to the next scheduled run.
Go to Schedule	Clicking **Go to Schedule** opens the *Profile* settings page which allows you to create and edit connection profiles. See *Profile*, page 148 for details.
	Click this icon to Refresh the connections list in the right column.
Undo	Click this icon to undo the most recent disconnection.

This Page Intentionally Left Blank

Chapter 11
Sessions

Overview

The *Sessions* panel is found at the bottom of the **KVM over IP Matrix Manager** main page, just below Scheduled Profile. Sessions displays information about users logged into devices and the KVM over IP Matrix Manager web GUI. Click **Go to Sessions** to view the settings page (see page 177).



Item	Description
Headings	The headings provide information about each user session: *Username*, *User Level*, *Service*, *IP*, *Login Time*, and *Last Access*. For more details about each heading, see *Sessions*, page 177.
Go to Sessions	Clicking **Go to Sessions** opens the *Sessions* settings page which provides a page displaying the same information found in this panel.
	Click this icon to Refresh the Sessions list.

This Page Intentionally Left Blank

Chapter 12
Remote Viewer

Introduction

If the video source(s) of your RCMDVI00AT / RCMDVI40AT / RCMDVI00BT / RCMDVI40BT / RCMDVI50T is connected, the remote viewer can be used to access these video source(s) as if it were on your local system.

A window will be presented and the remote server is displayed inside this window.

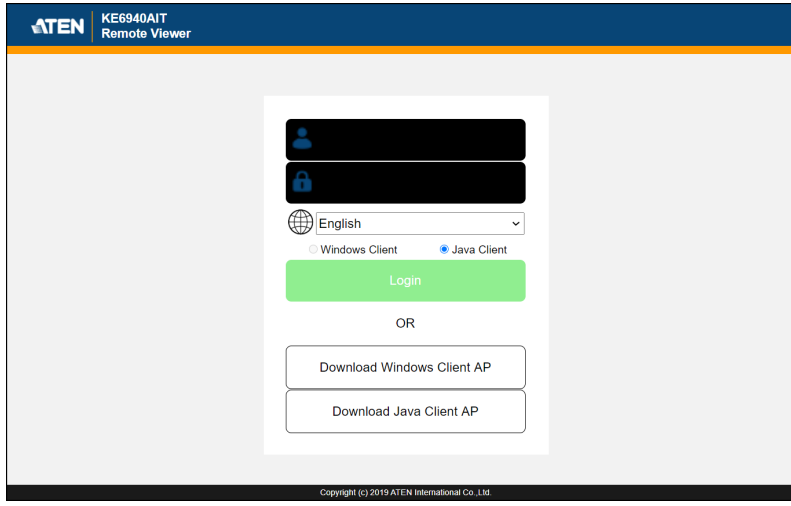
- You can maximize the window, drag the borders to resize the window and use the scrollbars to move around the screen.
- Due to net lag, there might be a slight delay before your keystrokes show up. You may also have to wait a bit for the remote mouse to catch up to your local mouse before you click.
- Due to net lag, or insufficient computing power on the local machine, some images, especially motion images, may display poorly.

There are several ways you can access the remote servers and are listed below:

1. **Windows viewer** accessed directly from the web browser GUI.
2. **Java viewer** accessed directly from the web browser GUI.
3. **Windows Client Viewer AP** (without browser). On the browser login page, a “Download Windows Client AP” is available. Refer to *The Windows/Java Client AP* on page 190 for more information.
4. **Java Client Viewer AP** (without browser). Since the control is identical to the windows client viewer, refer to *The Control Panel* on page 193 on the control of the viewer interface.

Windows and Java Client Viewer (web access)

The Windows and Java Client Viewer is accessible via a web browser.



At the login screen of the Remote Viewer page, enter the username/password and click **Login**. You can change the login language by using the language drop-down menu.

A second or two after, the video source(s)' display appears as a window on your desktop:

The control/access is laid out in the control panel. Refer to *The Control Panel* on page 193 for access/control information.

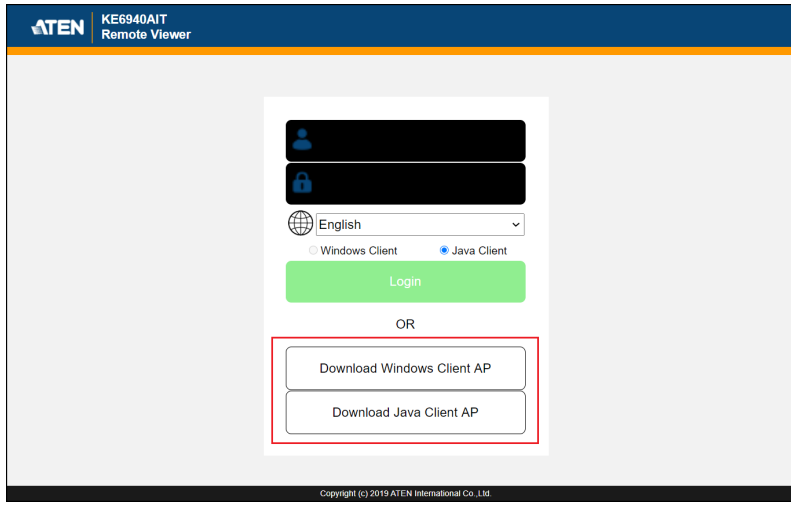
By default, if you use Internet Explorer as your browser, the Windows Client viewer is used. If you use other browsers, the Java Client viewer is used.

If you manually set the preference to Java Client when you use Internet Explorer as your browser, the Java Client viewer is also used.

The Windows/Java Client AP

Download

To download the stand-alone Windows or Java Client program, go to the browser login page and click the **Download Windows Client AP** or **Download Java Client AP** button.

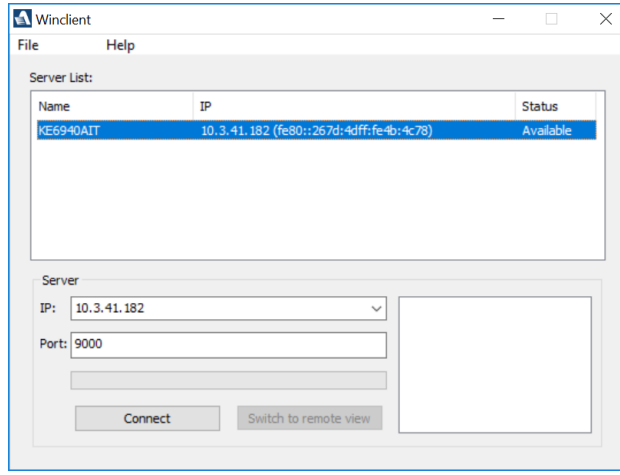


Note: Make sure your system has JRE 6 Update 3 or later installed. Java is available for free download from Sun's Java web site (http://java.sun.com).

Starting Up

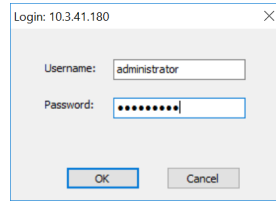
For the first time running the AP, right-click the Windows/Java Client AP and click “Run as administrator” to start.

The Client Connection Screen is shown below and each components are described in the table. Windows Client will be the example shown here.



Item	Description
Server List	When you run the Client program, it automatically searches the user’s local LAN segment for the transmitters (via remote port access), and lists whichever ones it finds in this box. If you want to connect to one of these units, double-click to connect.
Server	If the transmitters you wish to connect to is at a remote location, it will not be found on your LAN. You can enter its IP address and port yourself. If you don’t know the Port number, contact the Administrator. When the IP address and Port number for the unit you wish to connect to have been specified, click **Connect** to start the connection.
Connect	Starts connecting to the transmitters.
Disconnect	These buttons become active once you log into the transmitters.
Switch to remote view	
Message panel	The blank field on the right of the Server section shows the current status of the server connection.

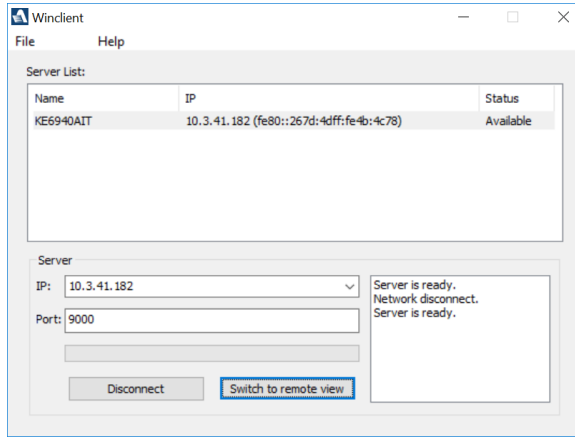
1. Double-click the unit. When the unit is connected, a login window appears:



2. Provide a valid Username and Password and click **OK** to continue.

Note: The default Username is *administrator* and the default Password is *password*.

After you have successfully logged in, the connection screen reappears:



At this time there are two active buttons and are described in the table below:

Button	Action
Disconnect	Breaks the connection to the unit.
Switch to remote view	Opens a window on the user's desktop containing the remote server's display that is the same as the one that appears with the browser-based Windows client.

3. Click **Switch to remote view** to access the video source(s)' display(s).

Refer to *The Control Panel* on page 193 for information about the remote access interface.

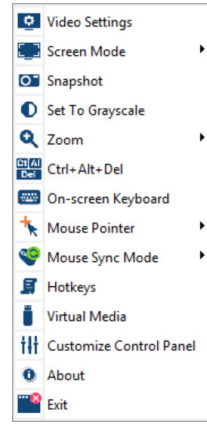
The Control Panel

The control panel is hidden at the upper or lower center of the screen (the default is up). It becomes visible when you move the mouse pointer over it:

Note: 1. The above image shows the complete Control Panel. The icons that appear can be customized. See *Control Panel Configuration*, page 208, for details.

2. To move the Control Panel to a different location, click and drag the Control Panel.

- The panel is consisted of two rows.
- The second row shows the video resolution of the remote display, the bus the user is on, and an information button where you can click it for a menu-style version of the control panel toolbar (see below).
- Right clicking the second row area also brings up the menu-style control panel. This menu allows you to select options for the *Screen Mode*, *Zoom*, *Mouse Pointer type*, and *Mouse Sync Mode.* These functions are discussed in the sections that follow.



Control Panel Functions

The Control Panel functions are described in the table below.

Icon	Function
	This is a toggle. Click to ping the Control Panel to the window where it is always displayed on top of other screen elements. Click again to have it display normally.
	Click to bring up the Video Options dialog box. (See *Video Settings*, page 198, for details).
	Toggles the display between *Full Screen Mode* and *Windowed Mode*.
	Click to take a snapshot (screen capture) of the remote display. To configure the Snapshot parameters, refer to *Snapshot* on page 209.
	Click to toggle the remote display between color and grayscale.
	Click to zoom the remote display window. **Note:** This feature is only available in windowed mode (Full Screen Mode is off). See *Zoom*, page 204 for details.
	Click to send a *Ctrl+Alt+Del* signal to the remote system.
	Click to bring up the on-screen keyboard (see *The On-Screen Keyboard*, page 205).
	Click to select the mouse pointer type. **Note:** This icon changes depending on which mouse pointer type is selected (see *Mouse Pointer Type*, page 206).
	Click to toggle Automatic or Manual mouse sync. ◆ When the selection is *Automatic*, a green mark appears on the icon. ◆ When the selection is *Manual*, a red mark appears on the icon. See *Mouse DynaSync Mode*, page 206 for a complete explanation of this feature.

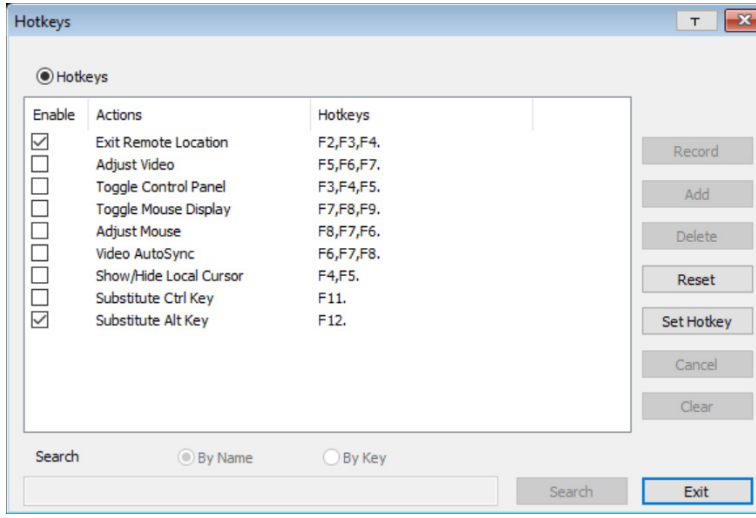
Icon	Function
	These icons show the Num Lock, Caps Lock, and Scroll Lock status of the remote computer. ◆ When the lock state is *On*, the LED is bright orange. ◆ When the lock state is *Off*, the LED is dull blue. Click on the icon to toggle the status. **Note:** These icons and your local keyboard icons are in sync. Clicking an icon causes the corresponding LED on your keyboard to change accordingly. Likewise, pressing a Lock key on your keyboard causes the icon's color to change accordingly.
	Click to bring up the Macro dialog box (see *Macros*, page 196 for more details).
	Click to bring up the *Virtual Media* dialog box. The icon changes when a virtual media device is mounted on the port. See *Virtual Media*, page 201, for specific details. **Note:** This icon displays in gray when the function is disabled or not available to the user.
	Click to bring up the Control Panel Configuration dialog box. See *Control Panel Configuration*, page 208, for details on configuring the Control Panel.

Macros

The Macros icon provides access to three functions found in the Macros dialog box: Hotkeys, User Macros, and System Macros. Each of these functions is described in the following sections.

Hotkeys

Various actions, corresponding to clicking the Control Panel icons, can be accomplished directly from the keyboard with hotkeys. Selecting the Hotkeys radio button lets you configure which hotkeys perform the actions. The actions are listed to the left; their hotkeys are shown to the right. Use the checkbox to the left of an action's name to enable or disable its hotkey.



If you find the default Hotkey combinations inconvenient, you can reconfigure them as follows:

1. Highlight an *Action*, then click **Set Hotkey**.
2. Press your selected Function keys (one at a time). The key names appear in the **Hotkeys** field as you press them.
   - You can use the same function keys for more than one action, as long as the key sequence is not the same.
   - To cancel setting a hotkey value, click **Cancel**; to clear an action's Hotkeys field, click **Clear**.
3. When you have finished keying in your sequence, click **Save**.

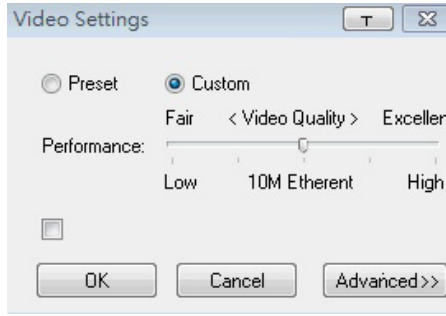
To reset all the hotkeys to their default values, click **Reset**.

An explanation of the Hotkey actions is given in the table below:

Action	Explanation
Exit remote location	Exits the remote view. This is equivalent to clicking the *Exit* icon on the Control Panel. The default keys are F2, F3, F4.
Adjust Video	Brings up the *Video Settings* dialog box. This is equivalent to clicking the *Video Settings* icon on the Control Panel. The default keys are F5, F6, F7.
Toggle Control Panel	Toggles the Control Panel **Off** and **On**. The default keys are F3, F4, F5.
Toggle Mouse Display	If you find the display of the two mouse pointers (local and remote) to be confusing or annoying, you can use this function to shrink the non-functioning pointer down to a barely noticeable tiny circle, which can be ignored. Since this function is a toggle, use the hotkeys again to bring the mouse display back to its original configuration. This is equivalent to selecting the *Dot* pointer type from the *Mouse Pointer* icon on the Control Panel. The default keys are F7, F8, F9. **Note:** The Java Control Panel does not have this feature.
Adjust mouse	This synchronizes the local and remote mouse movements. The default keys are F8, F7, F6.
Video Auto-sync	This combination performs an auto-sync operation. It is equivalent to clicking the *Video Autosync* icon on the Control Panel. The default keys are F6, F7, F8.
Show/Hide Local Cursor	Toggles the display of your local mouse pointer off and on. This is equivalent to selecting the *Null* pointer type from the *Mouse Pointer* icon on the Control Panel. The default keys are F4,F5.
Substitute Ctrl key	If your local computer captures Ctrl key combinations, preventing them from being sent to the remote system, you can implement their effects on the remote system by specifying a function key to substitute for the Ctrl key. If you substitute the F11 key, for example, pressing [F11 + 5] would appear to the remote system as [Ctrl + 5]. The default key is F11.
Substitute Alt key	Although all other keyboard input is captured and sent to the remote system, [Alt + Tab] and [Ctrl + Alt + Del] work on your local computer. In order to implement their effects on the remote system, another key may be substituted for the Alt key. If you substitute the F12 key, for example, you would use [F12 + Tab] and [Ctrl + F12 + Del]. The default key is F12.

Video Settings

The *Video Settings* dialog box allows you to adjust the placement and picture quality of the remote screen display on your monitor.



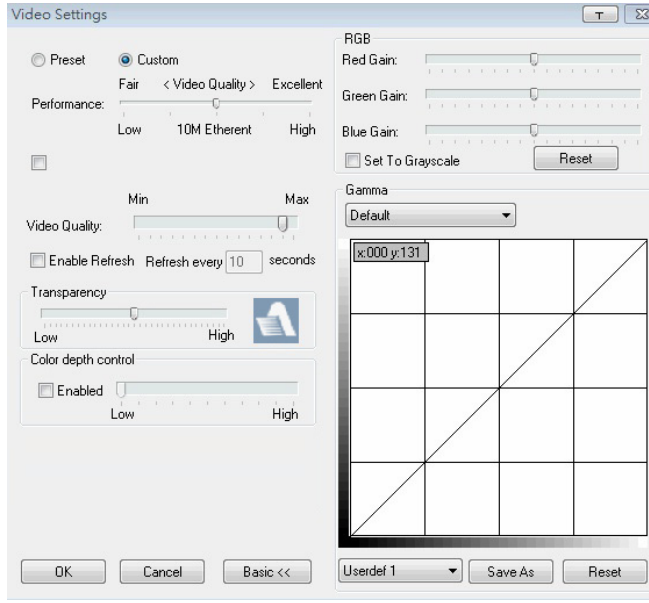
The adjustment options are as follows:

Option	Usage
	Click this to control the transparency of the Video Settings dialog box.
Performance	Select the type of Internet connection that exists between the Local Client computer and the unit. The unit will use that selection to automatically adjust the *Video Quality* settings to optimize the quality of the video display. Since network conditions vary, if none of the preset choices seem to work well, you can select *Customize* and use the **Video Quality** slider bars to adjust the settings to suit your conditions.
Advanced	See page 199 for details.

Gamma Adjustment

For greater control and if it is necessary to correct the gamma level for the remote video display, use the Gamma function of the **Advanced** Video Settings by clicking the **Advanced** button.

For gamma level, there are ten preset and four user-defined levels to choose from. Click the drop-down menu and choose the most suitable one.



The additional options in the Advanced screen are as follows:

Option	Usage
RGB	Drag the slider bars to adjust the RGB (Red, Green, Blue) values. When an RGB value is increased, the RGB component of the image is correspondingly increased. If you enable *Set to Grayscale*, the remote video display is changed to grayscale.
Gamma	This section allows you to adjust the video display's gamma level. Click and drag the diagonal line at as many points as you wish to achieve the display output you desire. Click *Save As* to save up to four user-defined configurations derived from this method. Saved configurations can be recalled from the list box at a future time. Click *Reset* to abandon any changes and return the gamma line to its original diagonal position.

Option	Usage
Video Quality	Drag the slider bar to adjust the overall video quality. The larger the value, the clearer the picture and the more video data goes through the network. Depending on the network bandwidth, a high value may adversely affect response time.
Enable Refresh	The unit can redraw the screen every 1 to 99 seconds, eliminating unwanted artifacts from the screen. Select **Enable Refresh** and enter a number from 1 through 99. The unit will redraw the screen at the interval you specify. This feature is disabled by default. Click to put a check mark in the box next to *Enable Refresh* to enable this feature. **Note:** 1. The switch starts counting the time interval when mouse movement stops. 2. Enabling this feature increases the volume of video data transmitted over the network. The lower the number specified, the more often the video data is transmitted. Setting too low a value may adversely affect overall operating responsiveness.
Transparency	Drag the slider bars to adjust the transparency of the remote display.
Color Depth Control	This setting determines the richness of the video display by adjusting the amount of color information.

Click **OK** to save your changes and close the dialog box.

Click **Cancel** to abandon your changes and close the dialog box.

Note: For best results, change the gamma while viewing a remote computer.

Virtual Media

The *Virtual Media* feature allows a drive, folder, image file, or removable disk on a local client computer to appear and act as if it were installed on the remote server.

Virtual Media also supports a smart card reader function that allows a reader plugged into a local client computer to appear as if it were plugged into the remote server.

Virtual Media Icons

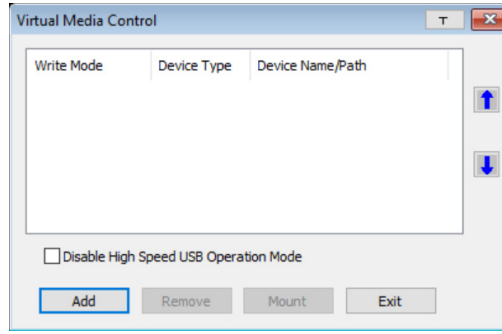
The *Virtual Media* icon on the **Control Panel** changes to indicate whether the virtual media function is available, or if a virtual media device has already been mounted on the remote server, as shown in the table below:

Icon	Function
	The icon displays as shown on the left to indicate that the virtual media function is disabled or not available.
	The icon displays as shown on the left to indicate that the virtual media function is available. Click the icon to bring up the virtual media dialog box.
	The icon displays as shown on the left to indicate that a virtual media device has been mounted on the remote server. Click the icon to unmount all redirected devices.

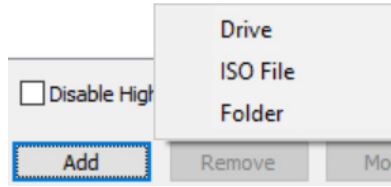
Virtual Media Redirection

To implement the virtual media redirection feature, do the following:

1. Click the Virtual Media icon to bring up the *Virtual Media* dialog box:



2. Click **Add** and select the media source.

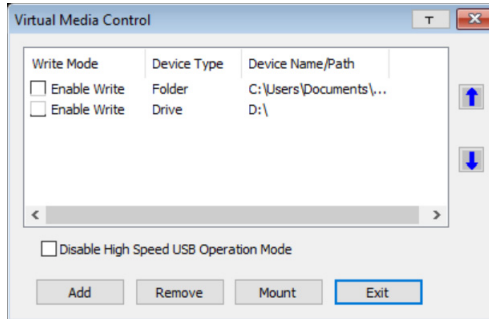


Depending on your selection, additional dialog boxes appear enabling you to select the drive, file, folder, or removable disk you desire. See *Virtual Media Support*, page 279 for details about mounting these media types.

3. To add additional media sources, click **Add**, and select the source.

Up to three virtual media choices can be added. To rearrange the selection order, highlight the device you want to move, then click the **Up** or **Down** Arrow button to promote or demote it in the list.

4. *Read* refers to the redirected device being able to send data to the remote server. *Write* refers to the redirected device being able to have data from the remote server written to it. The default is *Read*. If you want the redirected device to be writable, check the *Enable Write* checkbox:

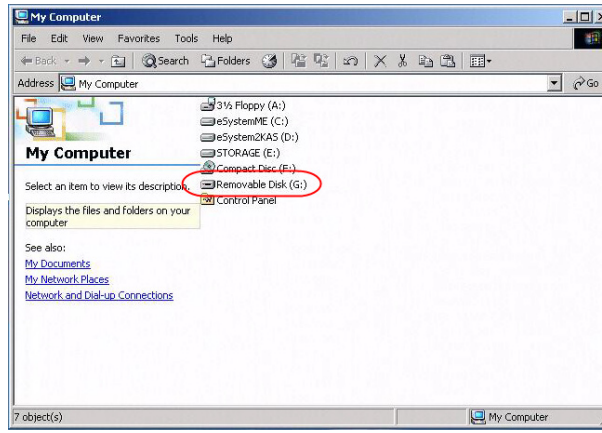


Note: 1. If a redirected device cannot be written to, or if a user does not have write permissions, it appears in gray and cannot be selected.

2. See *Virtual Media Support*, page 279, for a list of supported virtual media types.

5. To remove an entry from the list, highlight it and click **Remove**.

6. After you have made your media source selections, click **Mount**. The dialog box closes. The virtual media devices that you have selected are redirected to the remote system, where they show up as drives, files and folders on the remote system's file system.



Once mounted, you can treat the virtual media as if they were really on the remote server – drag and drop files to/from them; open files on the remote system for editing and save them to the redirected media, etc.

Files that you save to the redirected media will actually be saved on your local system. Files that you drag from the redirected media will actually come from your local system.

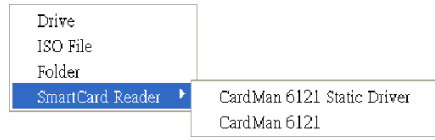
7. To end the redirection, bring up the *Control Panel* and click on the *Virtual Media* icon. All mounted devices are automatically unmounted.

Smart Card Reader

Note: This feature is only available when using the *WinClient Viewer* or the *Windows Client AP*.

The smart card reader function allows a reader plugged into a local client computer's USB port to be redirected, and appear as if it were plugged into the remote server. One purpose of smart cards (Common Access Cards, for example), is to allow authentication to the remote server from the local client.

When a smart card reader is connected to the local client computer, an entry for it appears when you bring up the **Virtual Media** dialog box and click **Add**:



Make your selection and click **Mount** to complete the redirection.

Zoom

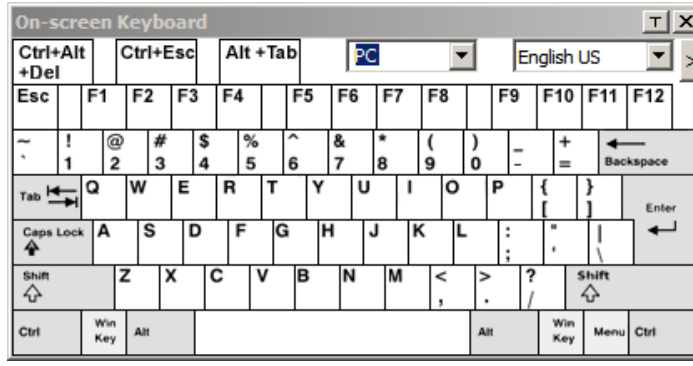
The *Zoom* icon controls the zoom factor for the remote view window. Settings are as follows:

Setting	Description
100%	Sizes and displays the remote view window at 100%.
75%	Sizes and displays the remote view window at 75%.
50%	Sizes and displays the remote view window at 50%.
25%	Sizes and displays the remote view window at 25%.
1:1	Sizes and displays the remote view window at 100%. The difference between this setting and the 100% setting is that when the remote view window is resized its contents don't resize – they remain at the size they were. To see any objects that are outside of the viewing area move the mouse to the window edge, to have the screen scroll.

The On-Screen Keyboard

The unit supports an on-screen keyboard, available in multiple languages, with all the standard keys for each supported language.

Click this icon to pop up the on-screen keyboard:

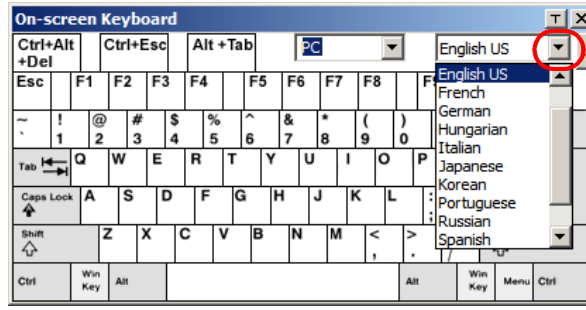


One of the major advantages of the on-screen keyboard is that if the keyboard languages of the remote and local systems are not the same, you do not have to change the configuration settings for either system. The user just has to bring up the on-screen keyboard; select the language used by the computer on the port he is accessing; and use the on-screen keyboard to communicate with it.

Note: You must use your mouse to click on the keys. You cannot use your actual keyboard.

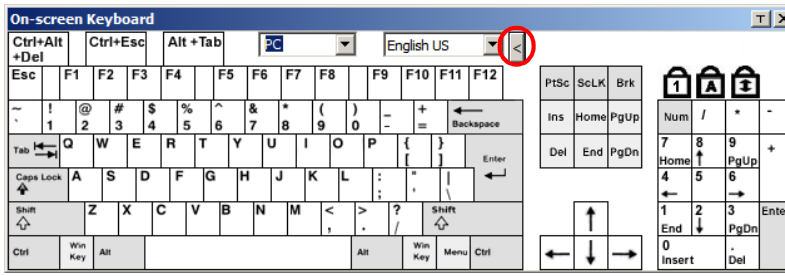
To change languages, do the following:

1. Click the down arrow next to the currently selected language to drop down the language list.



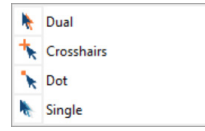
2. Select the new language from the list.

To display/hide the expanded keyboard keys, click the arrow to the right of the language list arrow.



Mouse Pointer Type

The CN9600 offers a number of mouse pointer options when working in the remote display. Click this icon to select the type that you would like to work with:



Note: 1. The Dot pointer is not available with the Java Client Viewer or the Java Client AP.

2. Selecting the Single pointer has the same effect as the *Toggle mouse display* hotkey function (see *Toggle Mouse Display*, page 197 for details).

3. The icon on the Control Panel changes to match your choice.

Mouse DynaSync Mode

Clicking this icon selects whether synchronization of the local and remote mouse pointers is accomplished either automatically or manually.

The icon on the toolbar indicates the synchronization mode status as follows:

Icon	Function
	The green mark on this icon indicates that Mouse DynaSync is available and is **enabled**. This is the default setting when Mouse DynaSync is available.

Icon	Function
	The red mark on this icon indicates that Mouse DynaSync is available but is **not enabled**.

When *Mouse DynaSync is available,* clicking the icon toggles between enabled and disabled. If you choose to disable Mouse DynaSync mode, you must use the manual syncing procedures described in the next section.

Automatic Mouse Synchronization (DynaSync)

Mouse DynaSync provides automatic locked-in syncing of the remote and local mouse pointers – eliminating the need to constantly re-sync the two movements.

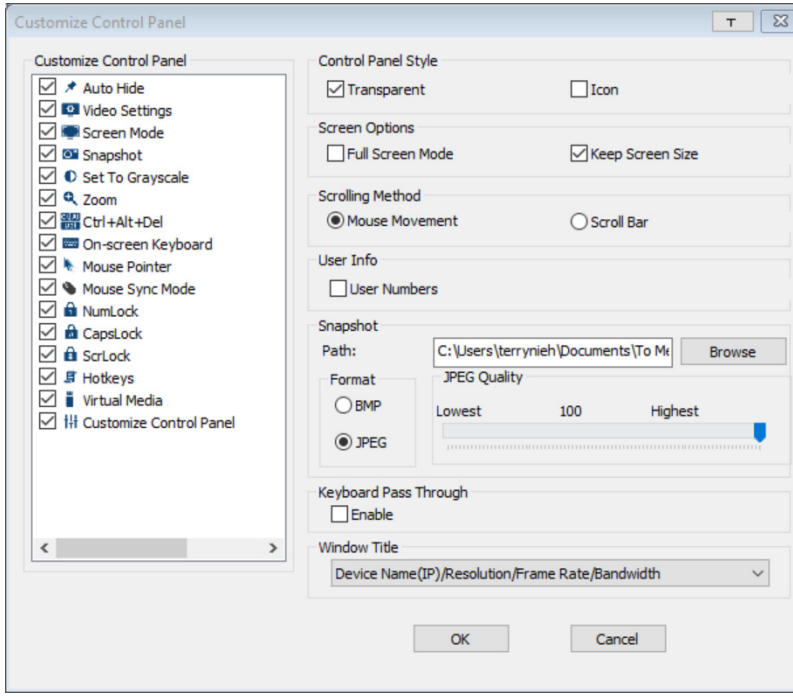
Manual Mouse Synchronization

If you are using Manual mouse synchronization instead of automatic DynaSync and the local mouse pointer goes out of sync with the remote system's mouse pointer, there are a number of methods to bring them back into sync:

1. Invoke the **Adjust Mouse** function with the *Adjust Mouse* hotkeys (see *Adjust mouse*, page 197, for details).
2. Move the pointer into all 4 corners of the screen (in any order).
3. Drag the Control Panel to a different position on the screen.
4. Set the mouse speed and acceleration for each problematic computer attached to the switch. See *Additional Mouse Synchronization Procedures*, page 277, for instructions.

Control Panel Configuration

Clicking the *Customize Control Panel* icon brings up a dialog box that allows you to configure the items that appear on the Control Panel, as well as its graphical settings:



The dialog box is organized into five main sections as described in the table below:

Item	Description
Customize Control Panel	Allows you to select which icons are displayed in the Control Panel.
Control Panel Style	◆ Enabling *Transparent* makes the Control Panel semi-transparent, so that you can see through it to the display underneath. ◆ Enabling *Icon* causes the Control Panel to display as an icon until you mouse over it. When you mouse over the icon, the full panel comes up.

Item	Description
Screen Options	◆ If **Full Screen Mode** is enabled, the remote display fills the entire screen. ◆ If **Full Screen Mode** is not enabled, the remote display appears as a window on the client desktop. If the remote screen is larger than what is able to fit in the window, scroll bars will appear. ◆ If **Keep Screen Size** is enabled, the remote screen is not resized. ◆ If the remote resolution is smaller than that of the client monitor, its display appears like a window centered on the screen. ◆ If the remote resolution is larger than that of the client monitor, its display is scaled to the client monitor size. ◆ If **Keep Screen Size** is not enabled, the remote screen is resized to fit the client monitor's resolution.
Scrolling Method	In cases where the remote screen display is larger than your monitor, you can choose how to scroll to the areas that are off-screen. ◆ If you select *Mouse Movement*, the screen will scroll when you move the mouse pointer to your screen border. ◆ If you select *Scroll Bars*, scroll bars appear around the screen borders that you can use to scroll to the off-screen areas.
User Info	If *User Numbers* is enabled, the total number of users logged into the unit displays beside the resolution on the second row of the Control Panel (See the *Control Panel* diagram on page 193 for an example.)
Snapshot	These settings let the user configure the unit's screen capture parameters (see the *Snapshot* description under *The Control Panel*, page 193): ◆ Path lets you select a directory that the captured screens automatically get saved to. Click **Browse**; navigate to the directory of your choice; then click **OK**. If you don't specify a directory here, the snapshot is saved to your desktop. ◆ Click a radio button to choose whether you want the captured screen to be saved as a BMP or a JPEG (JPG) file. ◆ If you choose JPEG, you can select the quality of the captured file with the slider bar. The higher the quality, the better looking the image, but the larger the file size.
Keyboard Pass Through	When this is enabled, the Alt-Tab key press is passed to the remote server and affects that server. If it is not enabled, Alt-Tab acts on your local client computer.
Window Title	Use the drop-down menu to select which remote server information is displayed on the window title.

This Page Intentionally Left Blank

Chapter 13
Firmware Upgrade Utility

The Windows-based Firmware Upgrade Utility (FWUpgrade.exe) provides a smooth, automated process for upgrading the 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
```

For browser based firmware upgrade, please refer to *FW Upgrade* on page 168.

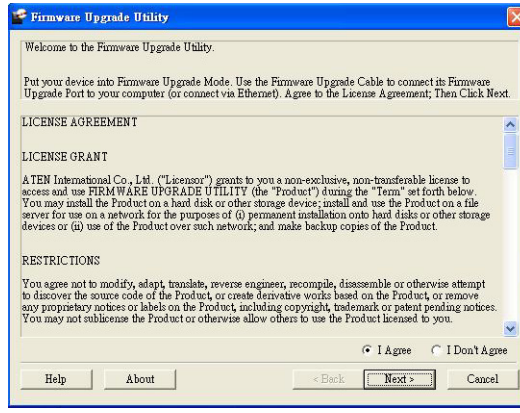
Preparation

1. From a computer that is not part of your installation go to our Internet support site and choose the model name that relates to your RCM/KE device 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 RCM/KE devices.

Starting the Upgrade

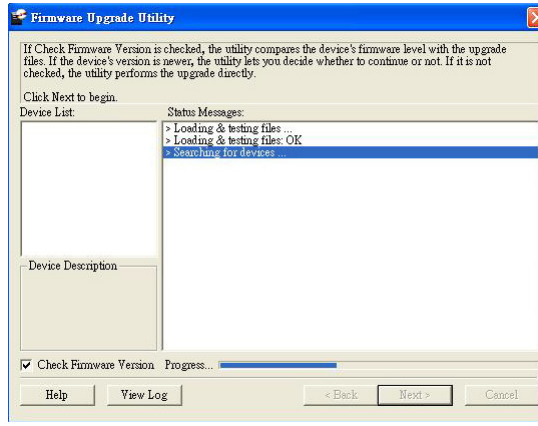
To upgrade your firmware:

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:

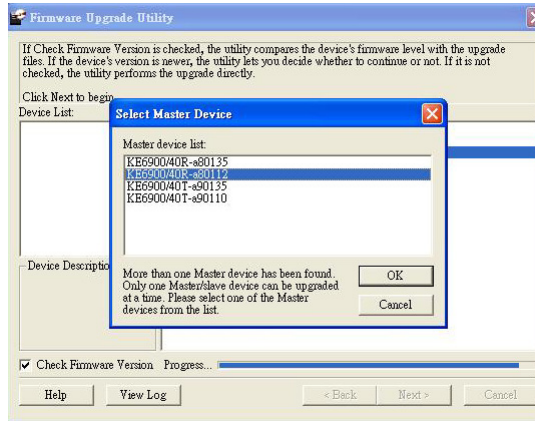


Note: The screens shown in this section are for reference only.

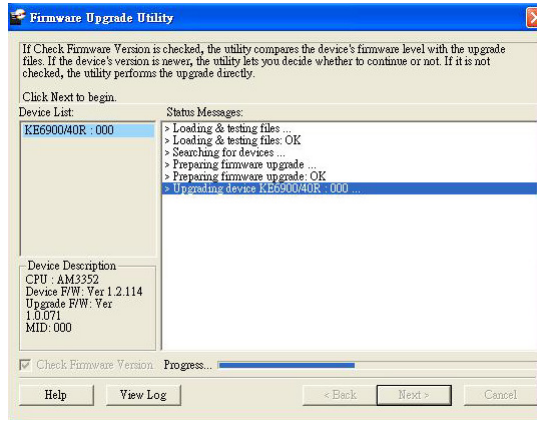
2. Read the License Agreement (enable the *I Agree* radio button).
3. Click **Next**. The Firmware Upgrade Utility main screen appears:



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.



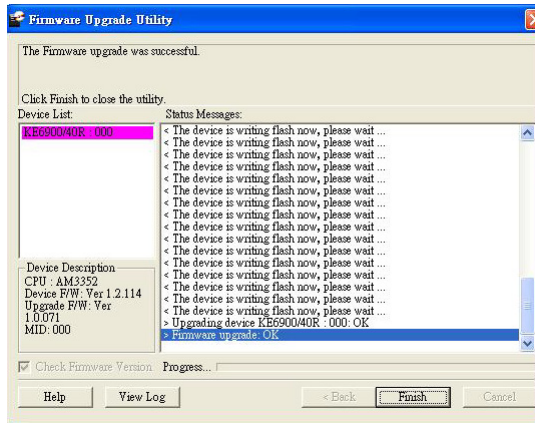
If you enabled Check Firmware Version, the Utility compares the device's firmware level with that of the upgrade files. If it finds that the device's version is higher than the upgrade version, it brings up a dialog box informing you of the situation and gives you the option to **Continue** or **Cancel**.

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 RCM/KE device.
2. Press the **Reset** button, then power on the RCM/KE device while holding Reset.
3. Hold **Reset** for 7 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.

Chapter 14
CLI Commands

Serial Control Protocol Commands

The RCM/KE series' built-in bi-directional RS-232 serial interface and LAN port connection allows system control via receivers through a high-end controller or PC. This control feature can also be accessed via TCP/IP through a computer running Telnet. The port for Telnet commands should be set to 9130.

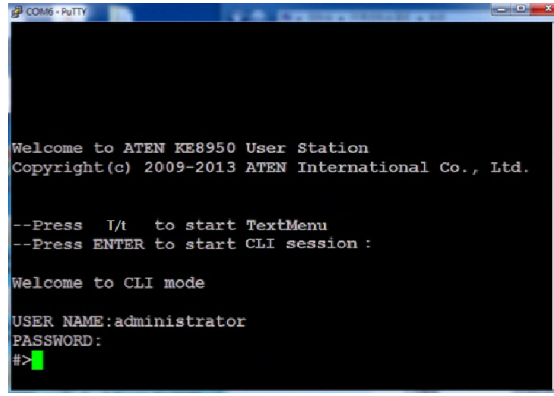
Configuring the Serial Port

The controller's serial port should be configured the same as the receiver's default configuration, as shown below:

Baud Rate	9600
Data Bits	8
Parity	None
Stop Bits	1
Flow Control	None

The receiver's **Function Switch** should be set to *RS-232 Config* (see page 11). Before executing RS-232 commands across a network you must install the KVM over IP Matrix Manager on a computer and ensure that it is online.

On your computer, open a terminal (command line) session. Please press **[Enter]** to start "**CLI Session**".



Device/Profile Commands

When typing a device or profile into a command string, you can enter the name by: **IP address** (device only), **ID** or **@** with the List number for the device/ profile in the command line interface.

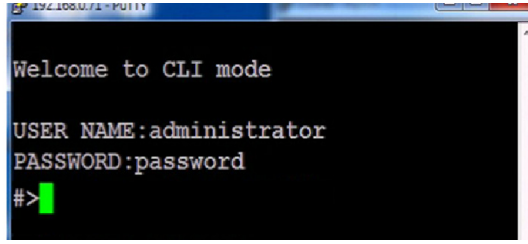
Note: To find out about the List number for a device/profile, execute a List command (page 232).

Telnet

The RCM/KE Series can be operated and configured via a remote terminal session using Telnet. This is a useful means for configuring devices when they are first setup and connected to the network.

To log into the RCM/KE Series device by means of a Telnet session, do the following:

1. On your computer, open a terminal (command line) session.
2. At the prompt, key in the RCM/KE device's IP address with port 9130 in the following way:
   telnet [IP address] [port]
3. Press Enter. The login screen appears. At the login prompt, provide the Password.



Verification

After sending a command, a verification message appears at the end of the command line. Use the echo command to identify a command by number:

- **Command OK** - the command is correct and performed successfully
- **Command incorrect** - the command has the wrong format and/or values.
- **Echo Command** - at the end of a command string, type: **e1234** – where 1234 can be any number. The verification message returns with the echo number.

Switch Port Command

The formula for Switch Port commands is as follows:

Command + Output + Num1 + Input + Num2 + Mode + Stream + Connect + **[Enter]**

1. For example, if you want to switch the receiver's connection to transmitter (192.168.0.20), type the following:

   sw i192.168.0.20 [Enter]

2. For example, if you want to disconnect the receiver from its transmitter connections, type the following:

   sw off [Enter]

3. For example, if you want to connect receiver (192.168.0.99) to transmitter (192.168.0.79) with exclusive access to stream video and audio, type the following:

   sw o192.168.0.99 i192.168.0.79 exclusive video audio on [Enter]

4. For example, to disconnect receiver (192.168.0.11) from the video stream and return it to the OSD menu, type the following:

   sw o192.168.0.11 off [Enter]

5. For example, to disconnect receiver (192.168.0.09) from the video stream and logout the OSD, type the following:

   sw o192.168.0.09 logout [Enter]

6. For example, to disconnect the receiver's USB stream, type the following:

   sw usb off [Enter]

7. For example, to switch the receiver to the 5th transmitter listed in the command line interface, type the following:

   sw i@5 exclusive all on [Enter]

8. For example, to switch the receiver to the 7th transmitter listed in the command line interface with echo command 4312, type the following:

   sw i@7 exclusive all on e4312

9. For example, to switch receiver (192.168.0.12) to the 14th transmitter listed in the command line interface with occupy access to stream video audio and USB, type the following:

   sw o192.168.0.12 i@14 occupy video audio usb on [Enter]

The following tables show the possible values for the Switch Port commands:

Command	Description
sw	Switch port command

Output	Description
o	Output port command (RX)

Num1	Description
xx	Output port xx: receiver ID or IP address
@zz	List # zz: 1~99 To use the 4th receiver listed in the command line interface, type: o@4

Input	Description
i	Input command (TX)

Num2	Description
yy	Input port yy: transmitter ID or IP address
@zz	List # zz: 1~99 To use the 8th transmitter listed in the command line interface, type: i@8

Mode	Description
exclusive	Sets the Access Mode to exclusive.
share	Sets the Access Mode to share.
occupy	Sets the Access Mode to occupy.
viewonly	Sets the Access Mode to view only. If the mode is omitted, view only is used by default.

Stream	Description
video	Sets the video source stream
audio	Sets the audio source stream
serial	Sets the serial source stream

Stream	Description
usb	Sets the USB source stream
all	Sets all source streams

Connect	Description
on	Connect
off	Disconnect
logout	Logout OSD

The following table lists the available Switch Port commands:

Command	Output	Num1	Input	Num2	Mode	Stream	Con-nect	Description
sw	o	xx	i	yy	exclusive	video audio serial usb all	on	Switch output xx to input yy with exclusive access to source(s). xx: receiver ID yy: rransmitter ID
sw	o	xx	i	yy	share	video audio serial usb all	on	Switch output xx to input yy with share access to stream source(s). xx: receiver ID yy: transmitter ID
sw	o	xx	i	yy	occupy	video audio serial usb all	on	Switch output xx to input yy with occupy access to stream source(s). xx: receiver ID yy: transmitter ID
sw	o	xx	i	yy	viewonly	video audio serial usb all	on	Switch output xx to input yy with viewonly access to stream source(s). xx: receiver ID yy: transmitter ID
sw	o	xx					off	Switch output xx, disconnect streams, return to OSD menu. xx: receiver ID
sw	o	xx					logout	Switch output xx, disconnect streams and logout from OSD menu. xx: receiver ID
sw						video audio serial usb all	off	Switch receiver stream(s) to disconnect.

Command	Output	Num1	Input	Num2	Mode	Stream	Con-nect	Description
sw							off	Switch receiver disconnect streams, return to OSD menu.
sw			i	@zz	exclusive share occupy viewonly	video audio serial usb all	on	Switch receiver to input @zz with [mode] access to stream source(s). zz: transmitter # by order listed in the command line interface.
sw	o	xx	i	@zz	exclusive	video audio serial usb all	on	Switch output xx to input @zz with [mode] access to stream source(s). xx: receiver ID zz: transmitter # by order listed in command line interface.

Note: 1. Each command string can be separated with a space.

2. The **Mode** command string can be skipped and **view only** will be used by default.

3. Skip the **Output** and **Num1** command strings to configure the local receiver.

Mute Command

The Mute command allows you to enable or disable the audio.

The formula for the Mute command is as follows:

Command + Output + Num1 + Control + [Enter]

1. For example, to turn mute off (audio on) for the receiver, type the following:

   mute off [Enter]

2. For example, to turn mute on for receiver (192.168.0.11), type the following:

   mute o192.168.0.11 on [Enter]

3. For example, to turn mute off for receiver (192.168.0.18), type the following:

   mute o192.168.0.18 off [Enter]

The following tables show the possible values for the Mute commands:

Command	Description
mute	Mute command

Output	Description
o	Output port command

Num1	Description
xx	Output number xx: receiver ID or IP address

Control	Description
on	Mute on; audio disabled
off	Mute off; audio enabled (default)

The following table lists the available Mute commands:

Command	Output	Num1	Control	Description
mute	o	xx	on	Turn mute on for output xx xx: receiver ID
mute	o	xx	off	Turn mute off for output xx xx: receiver ID

Command	Output	Num1	Control	Description
mute			on	Turn mute on for receiver
mute			off	Turn mute off for receiver

Note: 1. Each command string can be separated with a space.

2. The **Control** command string can be skipped and **off** will be used by default.

3. Skip the **Output** and **Num1** command strings to configure the local receiver.

Profile Command

The Profile command allows you to connect profiles and video walls.

The formula for Profile commands is as follows:

Command + Profile + Num1 + Control + [Enter]

1. For example, to connect profile 8 and lock the OSD menu, type the following:

   profile f8 [Enter]

2. For example, to connect profile 4 with access to the OSD menu, type the following:

   profile f4 release [Enter]

3. For example, to disconnect profile 12 and return to the receiver to the OSD menu, type the following:

   profile f12 back [Enter]

The following tables show the possible values for the Profile commands:

Command	Description
profile	Profile command

Profile	Description
f	Profile ID

Num1	Description
xx	Profile or Video Wall ID xx: 1-99

Control	Description
lock	Connect profile, lock access to OSD menu (default)
release	Connect profile, allow access to OSD menu
back	Disconnect profile, return receiver to OSD menu

The following table lists the available Profile commands:

Command	Profile	Num1	Control	Description
profile	f	xx	lock	Connect profile xx, lock OSD access xx:1~99
profile	f	xx	release	Connect profile xx, allow OSD access xx:1~99
profile	f	xx	back	Disconnect profile xx and return receiver to OSD menu xx: 1~99

Note: 1. Each command string can be separated with a space.

2. The **Control** command string can be skipped and **lock** will be used by default.

3. For functional **lock** and **release** commands, make sure the **Lock OSD when connecting** option is checked during *Create Profile*. Refer to *Lock OSD*, page 150 for more information.

EDID Command

Extended Display Identification Data (EDID) is a data that contains a display's basic information and is used to communicate with the video source. The EDID commands allow you to change the EDID setting of a transmitter. For more information on configuring EDID settings, see *Properties*, page 60.

The formula for the EDID command is as follows:

Command + Address + Number + Control + [Enter]

1. For example, if you want to configure device (192.168.0.3) to use the remix EDID mode, type the following:

   edid a192.168.0.3 remix [Enter]

The following tables show the possible values for the EDID commands:

Command	Description
edid	EDID command

Address	Description
a	Address command

Number	Description
xx	Address number xx: receiver ID or IP address

Control	Description
auto	Checks the EDID of all connected displays and the ATEN default EDID to use the best common resolution for all displays.
remix	Manually checks the EDID of all connected displays and the ATEN default EDID to use the best common resolution for all displays (see *EDID Mode*, page 76).
default	Implements ATEN's default EDID. (default)
manual	Manually set the EDID configuration from the receiver's OSD (see *EDID Mode*, page 76).

The following table lists the available EDID commands:

Command	Address	Number	Control	Enter	Description
edid	a	xx	auto	[Enter]	Set EDID of address xx to auto. xx: Device ID or IP Address
edid	a	xx	remix	[Enter]	Set EDID of address xx to remix. xx: Device ID or IP Address
edid	a	xx	default	[Enter]	Set EDID of address xx to default. xx: Device ID or IP Address
edid	a	xx	manual	[Enter]	Set EDID of address xx to manual. xx: Device ID or IP Address

Reset Command

The Reset command allows you to reset a device back to the default factory settings. Reset includes resetting the devices IP address.

Note: The Reset command resets everything but the login information to the factory default settings. To reset the login information, refer to *Reset All Information* on page 266.

The formula for the Reset command is as follows:

Command + Address + Number + [Enter]

1. For example, to reset device (192.168.0.95), type the following:

   reset a192.168.0.95 [Enter]

2. For example, to reset the receiver, type the following:

   reset [Enter]

The following tables show the possible values for the **Reset** command:

Command	Description
reset	Reset command

Address	Description
a	Address command

Number	Description
xx	Address number xx: receiver ID or IP address

The following table lists the available Reset commands:

Command	Address	Num	Enter	Description
reset	a	xx	[Enter]	Reset address xx back to the factory default settings xx: Device ID or IP Address
reset			[Enter]	Resets the receiver settings

Note: 1. Each command string can be separated with a space.

2. Skip the **Address** and **Number** command strings to reset the local receiver.

RS-232 Command

The RS-232 command allows you to set the RS-232 settings for a device.

The formula for the RS-232 command is as follows:

Command + Address + Number + Baud Rate + Parity + Data Bit + Stop Bit + Flow Control [Enter]

1. For example, to set device (192.168.0.33) with a baud rate of 38400, parity of none, data bit of 8, and stop bit of 1, type the following:

   baud a192.168.0.33 38400 none 8 1 [Enter]

2. For example, to set the local device with a baud rate of 19200, type the following:

   baud 19200 [Enter]

The following tables show the possible values for the RS-232 command:

Command	Description
baud	RS-232 command

Address	Description
a	Address command

Num1	Description
xx	Address number xx: Device ID or IP address

Baud Rate	Description
9600	Use 9600 baud rate
19200	Use 19200 baud rate
38400	Use 38400 baud rate
115200	Use 115200 baud rate

Parity	Description
None	Sets the parity to none
Even	Sets the parity to even
Odd	Sets the parity to odd

Data Bit	Description
5	Sets the data bit to 5
6	Sets the data bit to 6

Data Bit	Description
7	Sets the data bit to 7
8	Sets the data bit to 8

Stop Bit	Description
1	Sets the stop bit to 1
2	Sets the stop bit to 2

Flow Control	Description
None	Sets flow control to none
Hardware	Sets flow control to hardware
Xon	Sets flow control to Xon
Xoff	Sets flow control to Xoff

The following table lists the available Baud Rate commands:

Command	Address	Num 1	Baud Rate	Parity	Data Bit	Stop Bit	Flow Control	Description
baud	a	xx	9600	None Even Odd	5 6 7 8	1 2	None Hardware Xon/Xoff	Set address xx baud rate to 9600, with parity/ data bit/ stop bit / flow control setting
baud	a	xx	19200	None Even Odd	5 6 7 8	1 2	None Hardware Xon/Xoff	Set address xx baud rate to 19200, with parity/ data bit/ stop bit / flow control setting
baud	a	xx	38400	None Even Odd	5 6 7 8	1 2	None Hardware Xon/Xoff	Set address xx baud rate to 38400, with parity/ data bit/ stop bit / flow control setting
baud	a	xx	115200	None Even Odd	5 6 7 8	1 2	None Hardware Xon/Xoff	Set address xx baud rate to 115200, with parity/ data bit/ stop bit / flow control setting

Command	Address	Num 1	Baud Rate	Parity	Data Bit	Stop Bit	Flow Control	Description
baud			9600					Set local device baud rate to 9600
baud			19200					Set local device baud rate to 19200
baud			38400					Set local device baud rate to 38400
baud			115200					Set local device baud rate to 115200

Note: 1. Each command string can be separated with a space.

2. The **Baud Rate** value is required but **Parity**, **Data Bit** and **Stop Bit** can be skipped and their setting will not change.

3. Skip the **Address** and **Number** command strings to configure the local device settings.

OSD Command

To enable or disable the On-Screen Display (OSD) menu for a receiver, use the following command:

Command + Output + Number + Control + [Enter]

1. For example, to enable the OSD for receiver 192.168.0.51, type:

   osd o192.168.0.51 on [Enter]

2. For example, to disable the OSD for the local receiver, type:

   osd off [Enter]

The following tables show the possible values for the OSD command:

Command	Description
osd	OSD command

Output	Description
o	Output command

Number	Description
xx	Output number xx: receiver ID or IP address

Control	Description
on	Enable OSD functions
off	Disable OSD functions (default)

The following table lists the available OSD commands:

Command	Output	Number	Control	Enter	Description
osd	o	xx	on	[Enter]	Enable OSD functions for output xx xx: receiver ID or IP address
osd	o	xx	off	[Enter]	Disable OSD functions for output xx off (default) xx: receiver ID or IP address

Note: 1. Each command string can be separated with a space.

2. Skip the **Output** and **Number** command strings to configure the local receiver.

List Command

The List command allows you to retrieve information about users, settings and connections.

The formula for the List command is as follows:

Command + Output + Input + Number + Control [Enter]

1. For example, for a complete list of available channels, type the following:
   list channel [Enter]
2. For example, for a complete list of available profiles, type the following:
   list profile [Enter]
3. For example, to list all users logged into all OSD menus, type the following:
4. **list login [Enter]**
5. For example, to list the user logged into the OSD on receiver (192.168.0.44), type the following:
   list o192.168.0.44 login [Enter]
6. For example, for a complete list of available connections, type the following:
   list connection [Enter]
7. For example, to list the current connections on transmitter (192.168.0.88), type the following:
   list i192.168.0.88 connection [Enter]

The following tables show the possible values for the List command:

Command	Description
list	List command

Output	Description
o	Output command

Input	Description
i	Input command

Number	Description
xx	Output or Input number xx: Device ID or IP address

Control	Description
channel	Lists information about the available channel(s)
profile	Lists information about the available profile and TV wall connections
rx	Lists information about the receiver
login	Lists information about users logged into to the OSD menu
connection	Lists information about a transmitters current connections

The following table lists the available List commands:

Command	Output	Input	Number	Control	Description
list	o		xx	login	List output xx user logged into OSD.
list	o		xx	rx	List output xx receiver information
list		i	xx	connection	List input xx transmitter information
list				channel	List all available channel information
list				profile	List all available profile information
list				rx	List information about all receivers
list				login	List information about all OSD logins
list				connection	List information about all connections

Note: 1. Each command string can be separated with a space.

2. Skip the **Output** or **Input** and **Number** command strings to view the local receiver.

Read Command

The Read command allows you to retrieve the properties of a device.

The formula for the Read command is as follows:

Command + Output + Input + Number + Control [Enter]

1. For example, to read all of the local receiver's properties, type the following:

   read all [Enter]

2. For example, to read all of receiver (192.168.0.19) device properties, type the following:

   read o192.168.0.19 all [Enter]

3. For example, to read all of transmitter (192.168.0.28) device properties, type the following:

   read i192.168.0.28 all [Enter]

4. For example, to read the basic properties of receiver (192.168.0.61), type the following:

   read o192.168.0.61 basic [Enter]

5. For example, to read the network properties of transmitter (192.168.0.71), type the following:

   read i192.168.0.71 network [Enter]

The following tables show the possible values for the Read command:

Command	Description
read	Read command

Output	Description
o	Output command

Input	Description
i	Input command

Number	Description
xx	Output or Input number xx: Device ID or IP address

Control	Description
all	Read all device properties

Control	Description
basic	Read basic properties
network	Read network properties
ipsettings	Read IP settings
rs232	Read RS232 properties
properties	Read connection properties
manager	Read KVM over IP Matrix Manager properties
streams	Read enable media properties
tx	Read source stream IP properties (receiver)
usbmode	Read USB mode properties (receiver)
multicast	Read multicast properties (transmitter)
videoqtyadvanced	Read advanced video properties (transmitter)
ossettings	Read OS properties (transmitter)

The following table lists the available Read commands:

Command	Output	Input	Number	Control	Description
read	o	i	xx	all	Read output or input xx all device properties xx: Device ID or IP address
read	o	i	xx	basic	Read output or input xx basic properties xx: Device ID or IP address
read	o	i	xx	network	Read output or input xx network properties xx: Device ID or IP address
read	o	i	xx	ipsettings	Read output or input xx IP address properties xx: Device ID or IP address

Command	Output	Input	Number	Control	Description
read	o	i	xx	rs232	Read output or input xx RS-232 properties xx: Device ID or IP address
read	o	i	xx	properties	Read output or input xx connection properties xx: Device ID or IP address
read	o	i	xx	manager	Read output or input xx KVM over IP Matrix Manager IP and port properties xx: Device ID or IP address
read	o	i	xx	streams	Read output or input xx enable media properties xx: Device ID or IP address
read	o		xx	tx	Read output xx source stream IP address properties xx: receiver ID or IP address
read	o		xx	usbmode	Read output xx USB mode properties xx: receiver ID or IP address
read	i		xx	multicast	Read input xx multicast properties xx: transmitter ID or IP address
read	i		xx	videoqtyadvanced	Read input xx advanced video properties xx: transmitter ID or IP address
read	i		xx	ossettings	Read input xx OS properties xx: transmitter ID or IP address
read				all	Read all properties of local receiver

Command	Output	Input	Number	Control	Description
read				basic network ipsettings rs232 properties manager streams tx usbmode	Read [**control**] properties of local receiver.

Note: 1. Each command string can be separated with a space.

2. Skip the **Output** or **Input** and **Number** command strings to read the local receiver properties.

Set Command

The Set command allows you to configure the properties of a device. Some settings require that both the device and Matrix Manager are online or the command will fail.

The formula for the Set command is as follows:

Command + Output + Input + Number + Control + Value + [Enter]

1. For example, to set the name of the local receiver to RCMDVI00ATX1, type the following:

   set Name=RCMDVI00ATX1 [Enter]

2. For example, to set the description of transmitter (192.168.0.33) to RCM Room B, type the following:

   set o192.168.0.19 Description=RCM Room B [Enter]

3. For example, to set the DHCP settings of transmitter (192.168.0.28) to static, type the following:

   set i192.168.0.28 dhcpFlag=STATIC [Enter]

4. For example, to set the IP settings of the local receiver to 192.168.0.2, type the following:

   set ipAddr=192.168.0.2 [Enter]

5. For example, to set the transmitter video IP setting to 192.168.0.44 for receiver (192.168.0.56), type the following:

   set o192.168.0.56 TxVideoIP=192.168.0.44 [Enter]

The following tables show the possible values for the Set command**:**

Command	Description
set	Set command

Output	Description
o	Output command

Input	Description
i	Input command

Number	Description
xx	Output or Input number xx: Device ID or IP address

Control	Description
Name	Sets the device name
Description	Sets the device description
ipInstallerFlag	Sets the IP installer option
dhcpFlag	Sets the DHCP setting
ipAddr	Sets the IP address
netmask	Sets the subnet mask
gw	Sets the default gateway
modeFlag	Sets the device mode
BaudRate	Sets the baud rate setting
Parity	Sets the parity setting
DataBit	Sets the data bit setting
StopBit	Sets the stop bit setting
FlowCtrl	Sets the flow control setting
TxVideoIP	Sets the transmitter video IP setting
TxAudioIP	Sets the transmitter audio IP setting
TxUSBIP	Sets the transmitter USB IP setting
TxRSIP	Sets the transmitter RS-232 IP setting
VideoEnFlag	Sets the (enable media) video source stream
AudioEnFlag	Sets the (enable media) audio source stream
USBEnFlag	Sets the (enable media) USB source stream
RSEnFlag	Sets the (enable media) RS232 source stream
ManagerIP	Sets the KVM over IP Matrix Manager IP
ManagerPort	Sets the KVM over IP Matrix Manager port
Beeper	Sets the beeper
RxVM	Sets the USB mode setting
USBSecure	Sets the USB encryption
PortOS	Sets the port OS setting
OSLanguage	Sets the OS language
videoMCastEn	Sets the enable multicast video setting

Control	Description
audioMCastEn	Sets the enable multicast audio setting
Edid	Sets the EDID mode selection setting
VideoType	Sets the video type setting
ColorDepth	Sets the color depth setting
BandwidthLimit	Sets the bandwidth limit setting
VideoQty	Sets the video quality setting
BGRefresh	Sets the background refresh setting
Beeper	Sets the beeper setting
OccupyTimeout	Sets the occupy timeout setting
Resolution	Sets the resolution setting

Value	Description
=yy	Set value to yy yy: Enter a value that corresponds to the control being used

The following table lists the available Set commands:

Command	Output	Input	Number	Control	Value	Description
Set	o	i	xx	Name	yy	Set output or input xx Name to yy xx: Device ID or IP address yy: Name value
Set	o	i	xx	Description	yy	Set output or input xx Description to yy xx: Device ID or IP address yy: Description value
Set	o	i	xx	ipInstallerFlag	yy	Set output or input xx ipInstallerFlag to yy xx: Device ID or IP address yy: enable, viewonly, disable

Command	Output	Input	Number	Control	Value	Description
Set	o	i	xx	dhcpFlag	yy	Set output or input xx dhcpFlag to yy xx: Device ID or IP address yy: dhcp, static
Set	o	i	xx	ipAddr	yy	Set output or input xx ipAddr to yy xx: Device ID or IP address yy: IP address value
Set	o	i	xx	netmask	yy	Set output or input xx netmask to yy xx: Device ID or IP address yy: Subnet mask value
Set	o	i	xx	gw	yy	Set output or input xx gw to yy xx: Device ID or IP address yy: Default gateway value
Set	o	i	xx	modeFlag	yy	Set output or input xx modeFlag to yy xx: Device ID or IP address yy: extender, matrix
Set	o	i	xx	BaudRate	yy	Set output or input xx BaudRate to yy xx: Device ID or IP address yy: 9600, 19200, 38400, 115200
Set	o	i	xx	Parity	yy	Set output or input xx Parity to yy xx: Device ID or IP address yy: none, even, odd
Set	o	i	xx	DataBit	yy	Set output or input xx DataBit to yy xx: Device ID or IP address yy: 5, 6, 7, 8

Command	Output	Input	Number	Control	Value	Description
Set	o	i	xx	StopBit	yy	Set output or input xx StopBit to yy xx: Device ID or IP address yy: 1, 1.5, 2
Set	o	i	xx	FlowCtrl	yy	Set output or input xx FlowCtrl to yy xx: Device ID or IP address yy: none, hardware, Xon, Xoff
Set	o	i	xx	TxVideoIP	yy	Set output xx TxVideoIP to yy xx: Device ID or IP address yy: IP address value
Set	o		xx	TxAudioIP	yy	Set output xx TxAudioIP to yy xx: Device ID or IP address yy: IP address value
Set	o		xx	TxUSBIP	yy	Set output xx TxUSBIP to yy xx: Device ID or IP address yy: IP address value
Set	o		xx	TxRSIP	yy	Set output xx TxRSIP to yy xx: Device ID or IP address yy: IP address value
Set	o	i	xx	VideoEnFlag	yy	Set output or input xx VideoEnFlag to yy xx: Device ID or IP address yy: enable, disable
Set	o	i	xx	AudioEnFlag	yy	Set output or input xx AudioEnFlag to yy xx: Device ID or IP address yy: enable, disable

Command	Output	Input	Number	Control	Value	Description
Set	o	i	xx	USBEnFlag	yy	Set output or input xx USBEnFlag to yy xx: Device ID or IP address yy: enable, disable
Set	o	i	xx	RSEnFlag	yy	Set output or input xx RSEnFlag to yy xx: Device ID or IP address yy: enable, disable
Set	o	i	xx	ManagerIP	yy	Set output or input xx ManagerIP to yy xx: Device ID or IP address yy: KVM over IP Matrix Manager IP address
Set	o	i	xx	ManagerPort	yy	Set output or input xx ManagerPort to yy xx: Device ID or IP address yy: KVM over IP Matrix Manager port
Set	o	i	xx	Beeper	yy	Set output or input xx Beeper to yy xx: Device ID or IP address yy: enable, disable
Set	o		xx	RxVM	yy	Set output xx RxVM to yy xx: Device ID or IP address yy: vm, vusb
Set	o		xx	USBSecure	yy	Set output xx USBSecure to yy xx: Device ID or IP address yy: on, off
Set		i	xx	PortOS	yy	Set input xx PortOS to yy xx: Device ID or IP address yy: win, mac, sun, other

Command	Output	Input	Number	Control	Value	Description
Set		i	xx	OSLanguage	yy	Set input xx OSLanguage to yy xx: Device ID or IP address yy: english, japanese, french, german, spanish, korean, chinese(traditional), english(uk), swedish, arabic, belgian, canadian-bilingual, french(canada), czech, danish, finnish, greek, hebrew, hungarian, international(iso), italian, latin american, dutch, norwegian, persian(farsi), polish, portuguese, russian, slovak, french (switzerland), german (switzerland), switzerland, reserved, turkish-q, reserved, serbo-croatian
Set		i	xx	videoMCastEn	yy	Set input xx videoMCastEn to yy xx: Device ID or IP address yy: enable, disable
Set		i	xx	audioMCastEn	yy	Set input xx audioMCastEn to yy xx: Device ID or IP address yy: enable, disable
Set		i	xx	Edid	yy	Set input xx Edid to yy xx: Device ID or IP address yy: default, auto, manual, remix
Set		i	xx	VideoType	yy	Set input xx VideoType to yy xx: Device ID or IP address yy: dvi-d, dvi-a

Command	Output	Input	Number	Control	Value	Description
Set		i	xx	ColorDepth	yy	Set input xx ColorDepth to yy xx: Device ID or IP address yy: 8, 16, 24
Set		i	xx	BandwidthLimit	yy	Set input xx BandwidthLimit to yy xx: Device ID or IP address yy: unlimited, 100, 200, 500
Set		i	xx	VideoQty	yy	Set input xx VideoQty to yy xx: Device ID or IP address yy: 1, 2, 3, 4, 5
Set		i	xx	BGRefresh	yy	Set input xx BGRefresh to yy xx: Device ID or IP address yy: off, 16, 32, 64, 128, 256
Set		i	xx	OccupyTimeout	yy	Set input xx OccupyTimeout to yy xx: Device ID or IP address yy: 1~240
Set		i	xx	Resolution	yy	Set input xx Resolution to yy xx: Device ID or IP address yy: 1920x1200, 1920x1080, 1680x1050, 1600x1200, 1600x900, 1440x900, 1400x1050, 1366x768, 1280x1024, 1280x960, 1280x720, 1152x864, 1024x768, 800x600, 720x400, 640x480

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.
- Avoid circuit overloads. Before connecting equipment to a circuit, know the power supply's limit and never exceed it. Always review the electrical specifications of a circuit to ensure that you are not creating a dangerous condition or that one doesn't already exist. Circuit overloads can cause a fire and destroy equipment.
- 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.
- To prevent damage to your installation it is important that all devices are properly grounded.
- 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.
- 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.

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 iv.

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 1-949-428-1111

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

RCMDVI00AT / RCMDVI40AT

Function			RCMDVI00AT	RCMDVI40AT
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 (Green)	
		Mic.	1 x Mini Stereo Jack (Pink)	
		RS-232	1 x DB-9 Male (Black)	
	KVM Ports	KB / Mouse	1 x 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		2 x DC Jack (Black)	
	LAN Ports		1 x RJ-45 (Black) 1 x SFP Slot	
	Internet Port		1 x RJ-45 (Black)	
Switches	Mode Selection		1 x Slide Switch (Auto, RS-232 Config/Access Control, Local)	
	Reset		1 x Semi-recessed Pushbutton	
LEDs	Link		1 (10: Orange / 100: Orange & Green / 1000: Green)	
	Power		1 x Blue	
	Local		1 x Green	
	Remote		1 x Green	
Emulation	Keyboard / Mouse		USB	
Power Consumption			DC12V:12W:60BTU	DC12V:18.36W:90 BTU
Video Resolution			Up to 1920 x 1200 @ 60Hz	
Environment	Operating Temp.		0 – 50 ºC	
	Storage Temp.		-20 – 60 ºC	
	Humidity		0 – 95% RH, Non-condensing	

Function		RCMDVI00AT	RCMDVI40AT
Physical Properties	Housing	Metal	
	Weight	1.16 kg (2.56 lb)	1.18 kg (2.60 lb)
	Dimensions (L x W x H)	21.50 x 16.33 x 4.18 cm (8.46 x 6.43 x 1.65 in)	

RCMDVI00BT / RCMDVI40BT

Function			RCMDVI00BT	RCMDVI40BT
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 (Green)	
		Mic.	1 x Mini Stereo Jack (Pink)	
		RS-232	1 x DB-9 Male (Black)	
	KVM Ports	KB / Mouse	1 x 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		2 x DC Jack (Black)	
	LAN Ports		1 x RJ-45 (Black) 1 x SFP Slot	
	Internet Port		1 x RJ-45 (Black)	
	USB Port		1 x USB Type-A Female (White)	
	Control		1 x 6-Pin Mini-DIN (Purple)	
	I/O		9 x DI (0 - 24V) (Front) 1 x DO (0 - 24V) (Rear)	
	Relay		8 x Relay (Max 24VDC, 1.2A) (Rear)	
Switches	OSD		N/A	
	Video		N/A	
	Graphics		N/A	
	Mode Selection		1 x Slide Switch (Auto, RS-232 Config/Access Control, Local)	
	Reset		2 x Semi-recessed Pushbutton	

Function		RCMDVI00BT	RCMDVI40BT
LEDs	Power	2 x Green	
	Local	1 x Green	
	Remote	1 x Green	
	10 / 100 / 1000 Mbps	2 x LAN (100: Orange / 1000: Green)	
	Link	2 x LAN (Green) 1 x SFP (Green)	
Emulation	Keyboard / Mouse	USB	
Power Consumption		DC12V:16.9W: 133BTU	DC12V:19.7W: 147BTU
Video Resolution		Up to 1920 x 1200 @ 60Hz	
Environment	Operating Temp.	0 – 50 ºC	
	Storage Temp.	-20 – 60 ºC	
	Humidity	0 – 95% RH, Non-condensing	
Physical Properties	Housing	Metal	
	Weight	1.51 kg (3.33 lb)	1.53 kg (3.37 lb)
	Dimensions (L x W x H)	21.50 x 21.33 x 4.18 cm (8.46 x 8.40 x 1.65 in)	

RCMDVI50T

Function			RCMDVI50T
Connectors	Console Ports	Keyboard	1 x USB Type-A Female (White)
		Video	1 x DVI-I Female (White)
		Mouse	1 x USB Type-A Female (White)
		Speaker	1 x Mini Stereo Jack (Green)
		Mic.	1 x Mini Stereo Jack (Pink)
		RS-232	1 x DB-9 Male (Black)
	KVM Ports	KB / Mouse	1 x 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)
		RS-232	1 x DB-9 Female (Black)
	Power		2 x DC Jack (Black)
	LAN Ports		1 x RJ-45 (Black) 1 x SFP Slot
	Internet Port		1 x RJ-45 (Black)
	USB Port		1 x USB Type-A Female (White)
	Control		1 x 6-Pin Mini-DIN (Purple)
	I/O		9 x DI (0 - 24V) (Front) 1 x DO (0 - 24V) (Rear)
	Relay		8 x Relay (Max 24VDC, 1.2A) (Rear)
Switches	OSD		N/A
	Video		N/A
	Graphics		N/A
	Mode Selection		1 x Slide Switch (Auto, RS-232 Config/Access Control, Local)
	Reset		2 x Semi-recessed Pushbutton
LEDs	Power		2 x Green
	Local		1 x Green
	Remote		1 x Green
	10 / 100 / 1000 Mbps		2 x LAN (100: Orange / 1000: Green)
	Link		2 x LAN (Green) 1 x SFP (Green)
Emulation	Keyboard / Mouse		USB

Function		RCMDVI50T
Power Consumption		DC12V:17.3W:135BTU
Video Resolution		Up to 2560 x 1600 @ 60Hz
Environment	Operating Temp.	0 – 50 ºC
	Storage Temp.	-20 – 60 ºC
	Humidity	0 – 95% RH, Non-condensing
Physical Properties	Housing	Metal
	Weight	1.51 kg (3.33 lb)
	Dimensions (L x W x H)	21.50 x 21.33 x 4.18 cm (8.46 x 8.40 x 1.65 in)

Optional Rack Mount

For convenience and flexibility, three optional rack mount kits are available as shown in the following table:

Mounting Type	Model
Dual Rack Mount Kit*	2X-021G
Single Rack Mount Kit*	2X-031G

*Supports RCMDVI00AT / RCMDVI40AT / RCMDVI00BT / RCMDVI40BT / RCMDVI50T.

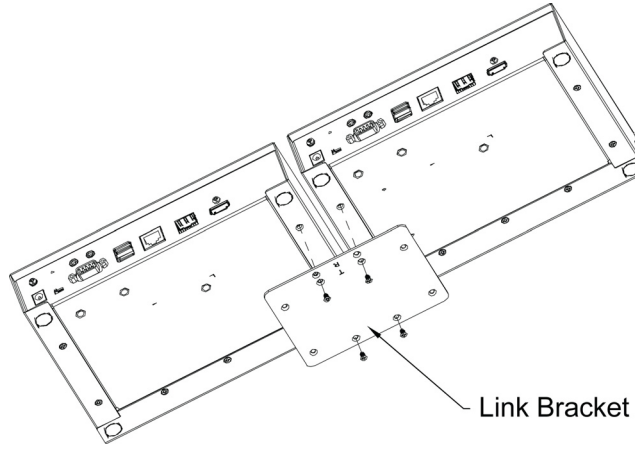
Dual Rack Mount

The 2X-021G Dual Rack Mount Kit installs two RCM units side by side in 1U of server rack space.

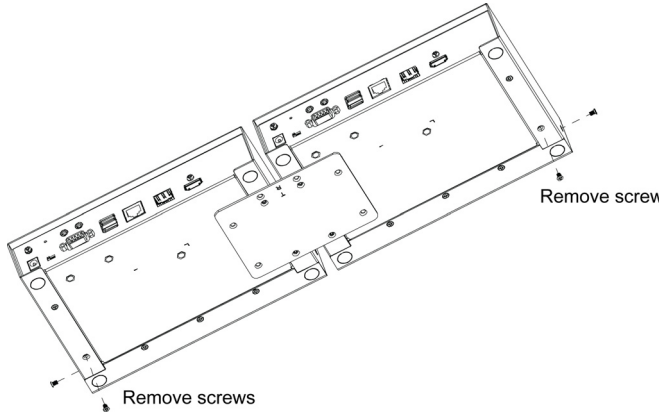
Transmitter Dual Rack Mount

KE8950T is the example used here.

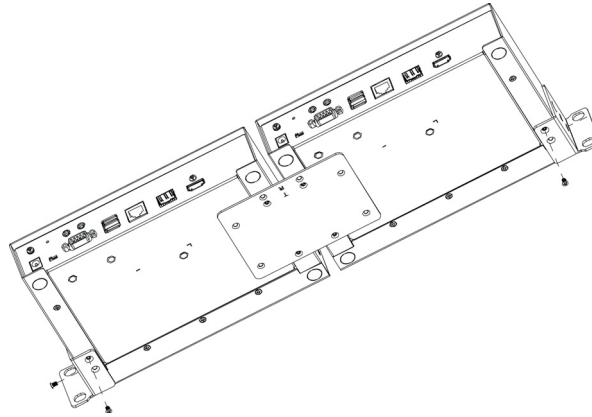
1. Remove four screws from the units and then use the same screws to secure the units together with the link bracket provided with the kit.



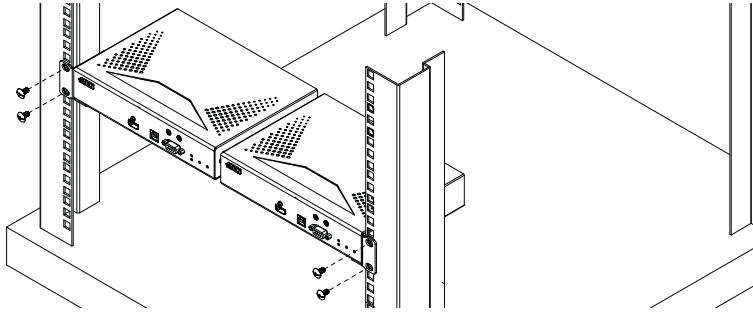
2. Remove the bottom and side screws from each unit.



3. Use the screws in step 2 to install the left and right mounting brackets.



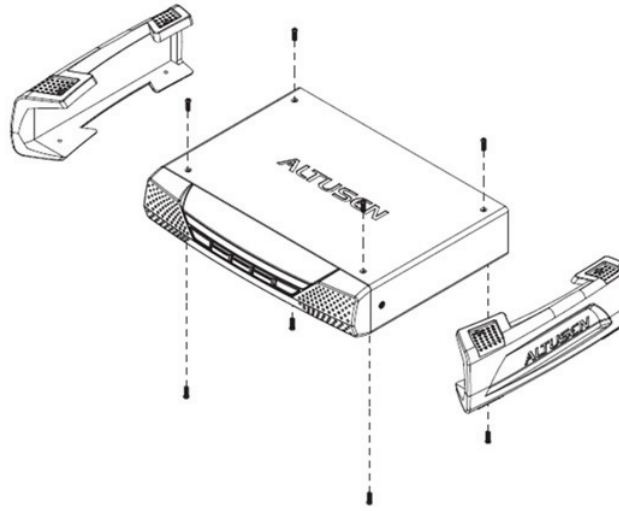
4. Screw the mounting brackets to the rack.



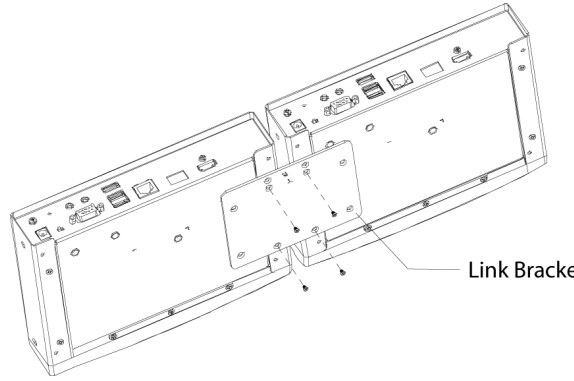
Receiver Dual Rack Mount

KE8950R is the example used here.

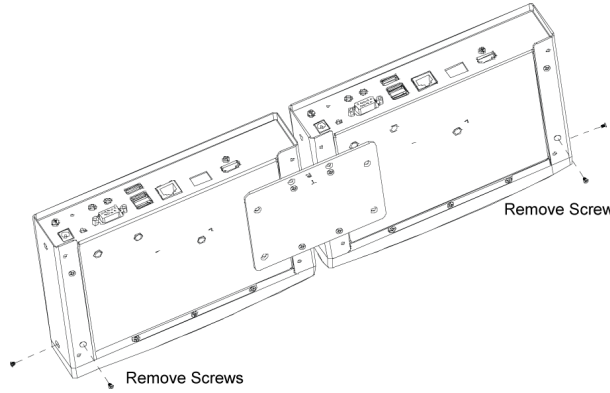
1. Remove the eight screws and plastic guards from the receiver units.



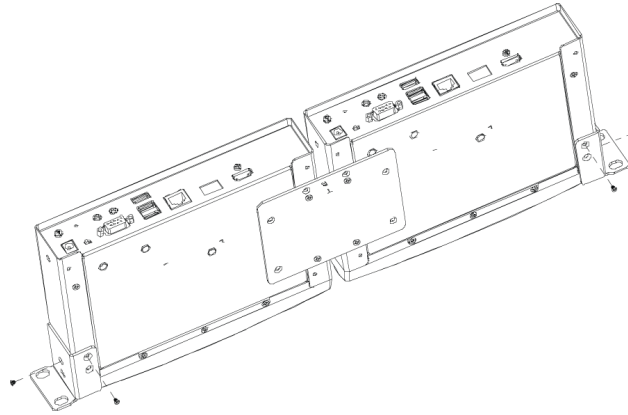
2. Remove four screws from the units and then use the same screws to secure the units together with the link bracket provided with the kit.



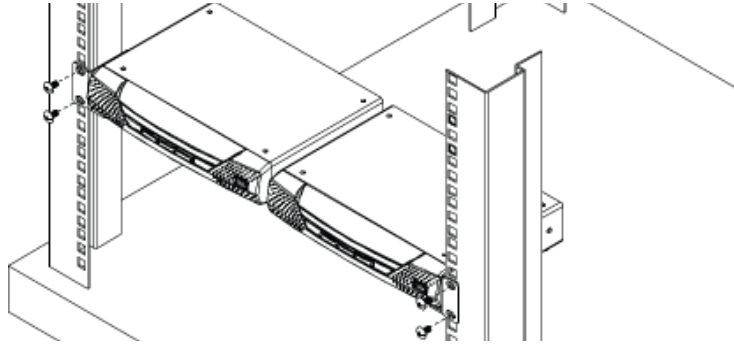
3. Remove the bottom and side screws from each unit.



4. Use the screws in step 3 to install the left and right mounting brackets.



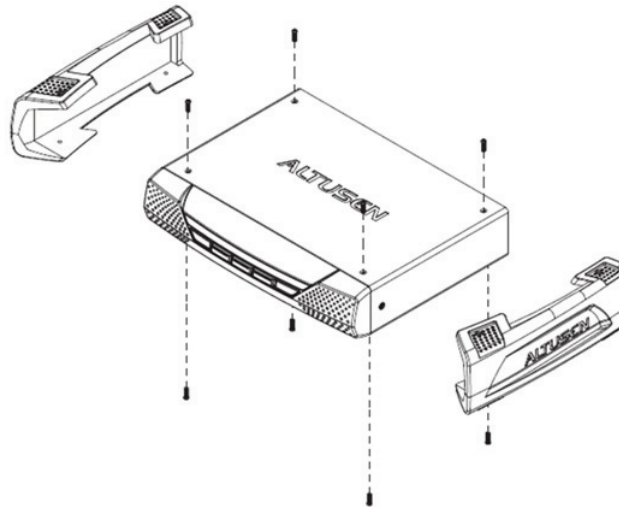
5. Screw the mounting brackets to the rack.



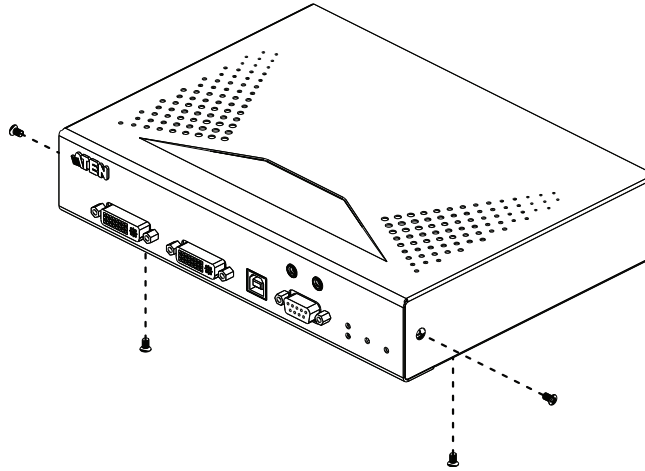
Single Rack Mount

The 2X-031G Single Rack Mounting kit installs one RCMDVI00AT / RCMDVI40AT / RCMDVI00BT / RCMDVI40BT / RCMDVI50T unit in 1U of server rack space.

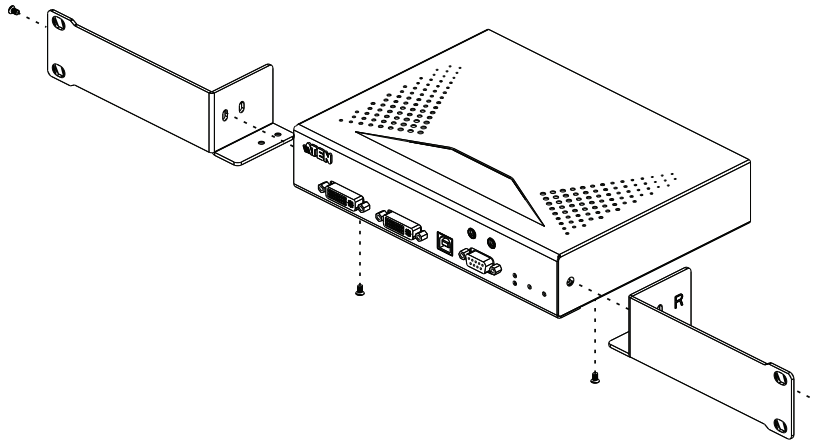
1. Remove the eight screws and plastic guards from the unit (receiver units only).



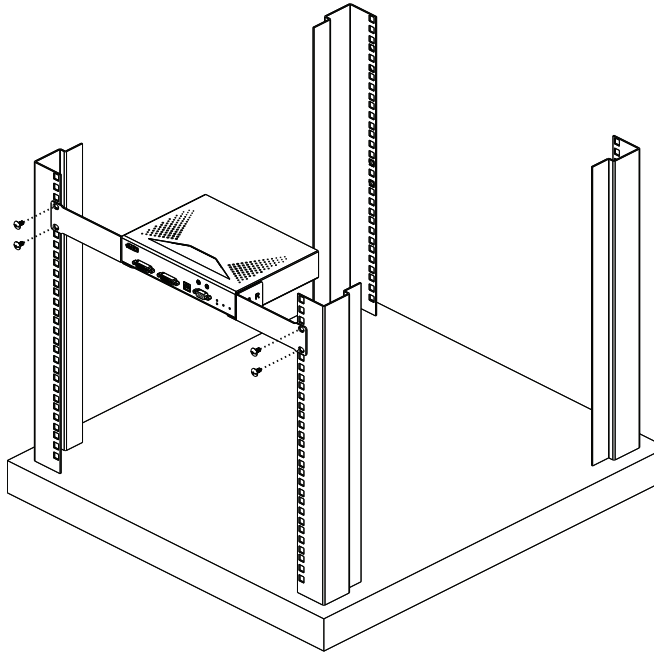
2. Remove the bottom and side screws from the unit.



3. Use the screws in step 2 to install the right and left mounting brackets.



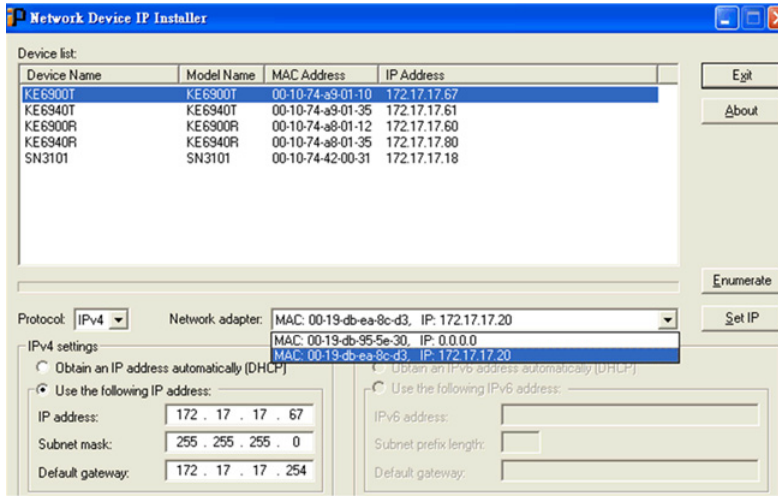
4. Screw the mounting brackets to the rack.



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 or from the product page on the *Software & Driver* tab. 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**.

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
```

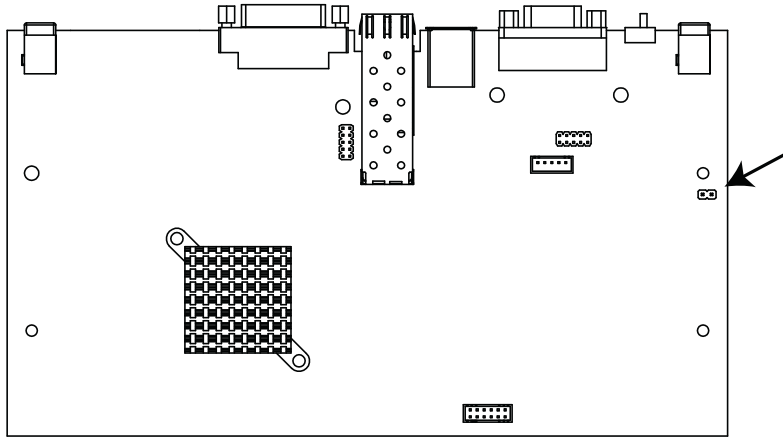
Importing the Files

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.

Reset All Information

To reset all information (including passwords) to their default settings, follow the steps below:

1. Power off the unit and remove its housing.
2. Use a jumper cap to short the mainboard pins labeled **DEFAULT PASSWORD**. An example is shown:



3. Power on the unit.
4. After the unit is turned on, power off the unit.
5. Remove the jumper cap from the **Reset** pins and close the housing.
6. Power on the unit again.

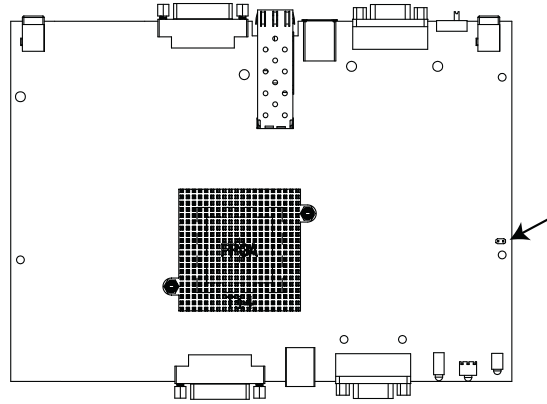
   After powering on the unit, you can use the default administrator Username and Password (see *Logging In*, page 93) to log in.

Default Password Pins

The **Default Password** pins for different models are shown below.

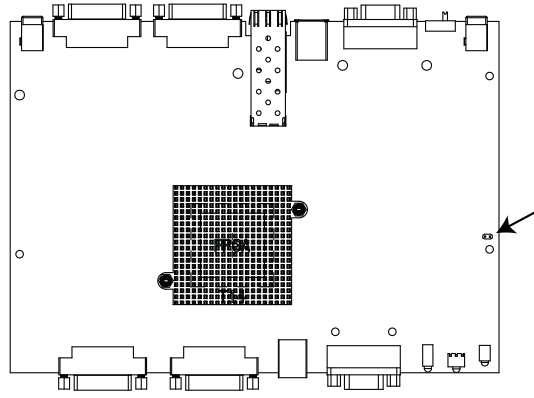
■ RCMDVI00AT / RCMDVI00BT / RCMDVI50T

Note: The unit used in the diagram below is RCMDVI00AT, the default password pin location for the RCMDVI00BT / RCMDVI50T is identical.



■ RCMDVI40AT / RCMDVI40BT

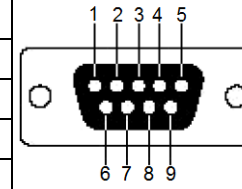
Note: The unit used in the diagram below is RCMDVI40AT, the default password pin location for the RCMDVI40BT is identical.



RS-232 Pin Assignments

Pin assignments for the transmitter and receiver's rear RS-232 port that is used for connecting to a serial terminal are given in the table, below:

Pin	Assignment	
1	N/A	None
2	RXD	Receive Data
3	TXD	Transmit Data
4	DTR	Data Terminal Ready
5	GND	Signal Ground
6	DSR	Data Set Ready
7	RTS	Request to Sent
8	CTS	Clear to Sent
9	N/A	None

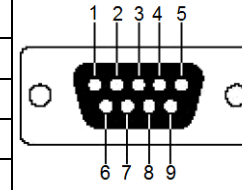


DB9 Male

Transmitter Front RS-232 Port

Pin assignments for the transmitter's front RS-232 port that is used for connecting to a computer for serial control are given in the table, below:

Pin	Assignment	
1	N/A	None
2	TXD	Transmit Data
3	RXD	Receive Data
4	DSR	Data Set Ready
5	GND	Signal Ground
6	DTR	Data Terminal Ready
7	CTS	Clear to Sent
8	RTS	Request to Sent
9	N/A	None



DB9 Female

Multicast IP Address

Multicasting helps to broadcast audio and video data from a transmitter to multiple receivers over a network. To setup up Multicasting on a network switch you must know the Audio and Video Multicast IP address which can be found on the RCM/KE Transmitter. To determinate the default Multicast IP address set by the RCM/KE device use the instructions below. The Multicast IP addresses can be set manually using Telnet.

RCM/KE Multicast Rule

All Audio and Video Multicast IP addresses use the format: 230.X.Y.Z.

X.Y.Z relates to the transmitter's IP address and **230** is always the first octet of a Multicast IP address. You use the transmitter's IP address to find **X** and then use it to calculate the Audio and Video Multicast IP address.

Multicast IP Formula

To calculate the Audio and Video Multicast IP address, use the transmitter's IP address to determine **X** and then use the appropriate table below to calculate the Multicast IP address for each data stream (audio/video).

Example:

Transmitter IP Address: 172.**16**.27.146; (172.**X**.Y.Z)

X =16

If X is between 0 ~ 127

Transmitter IP	X	Video X + 128	Audio X + 192	Multicast Video IP Address	Multicast Audio IP Address
172.**16**.27.146 (example)	16	16 + 128 = **144**	16 + 192 = **208**	230.**144**.27.146	230.**208**.27.146
		___+ 128 =	___+ 192 =	230.___.___.__	230.___.___.__
		___+ 128 =	___+ 192 =	230.___.___.__	230.___.___.__
		___+ 128 =	___+ 192 =	230.___.___.__	230.___.___.__

If X is between 128 ~ 192

Transmitter IP	X - 128 = A	Video A + 128	Audio A + 192	Multicast Video IP Address	Multicast Audio IP Address
172.**168**.27.14 (example)	**168** - 128 = 40	40 + 128 = **168**	40 + 192 = **232**	230.**168**.27.14	230.**232**.27.14
	___ - 128 =	___+ 128 =	___+ 192 =	230.___.___.__	230.___.___.__
	___ - 128 =	___+ 128 =	___+ 192 =	230.___.___.__	230.___.___.__
	___ - 128 =	___+ 128 =	___+ 192 =	230.___.___.__	230.___.___.__

If X is 192 or higher

Transmitter IP	X - 192 = A	Video A + 128	Audio A + 192	Multicast Video IP Address	Multicast Audio IP Address
172.**200**.27.14 (example)	**200** - 192 = 8	8 + 128 = **136**	8 + 192 = **200**	230.**136**.27.14	230.**200**.27.14
	___ - 192 =	___+ 128 =	___+ 192 =	230.___.___.__	230.___.___.__
	___ - 192 =	___+ 128 =	___+ 192 =	230.___.___.__	230.___.___.__
	___ - 192 =	___+ 128 =	___+ 192 =	230.___.___.__	230.___.___.__

Keys to Network Performance

For optimum performance, KE Series devices requires high amounts of data to be transferred across a network; therefore we recommend the following strategies to setup KE Series devices. Using our suggestions will provide better performance and the highest video resolutions possible. Use each of the keys to ensure the best transmission of data and the highest throughput possible.

Build a Network Diagram

To build an effective RCM/KE installation, start by mapping out the layout. Create a diagram with the RCM/KE devices, computers and routers along with how they will be connected across the network. It also helps to write out how the devices will interact. Use this diagram as the frame work as you decide what devices to purchase and how to build the network effectively for the best data throughput.

Considerations:

- If possible, create a private network for the RCM/KE devices
- Use the same switch model throughout
- Use a flat cascaded layout
- Avoid a tree or pyramid structure
- Limit cascades to two levels
- Install network switches near each other
- Minimize the distance of connections
- Install KVM over IP Matrix Manager (CCKM) computer and RCM/KE devices on the same subnet
- Check the 3 Other Factors before installation

Other Factors

■ Choose the Right Cable

Always use Cat 5/6e Ethernet cable or higher installed by a professional between any two devices you are installing. We recommend using ATEN Brand Ethernet cable to ensure the quality. It's best when installing RCM/KE devices to use brand new Ethernet cabling for each part of the installation to ensure the reliability of the data being transmitted. This is a key to getting the best uninterrupted video resolution across the network.

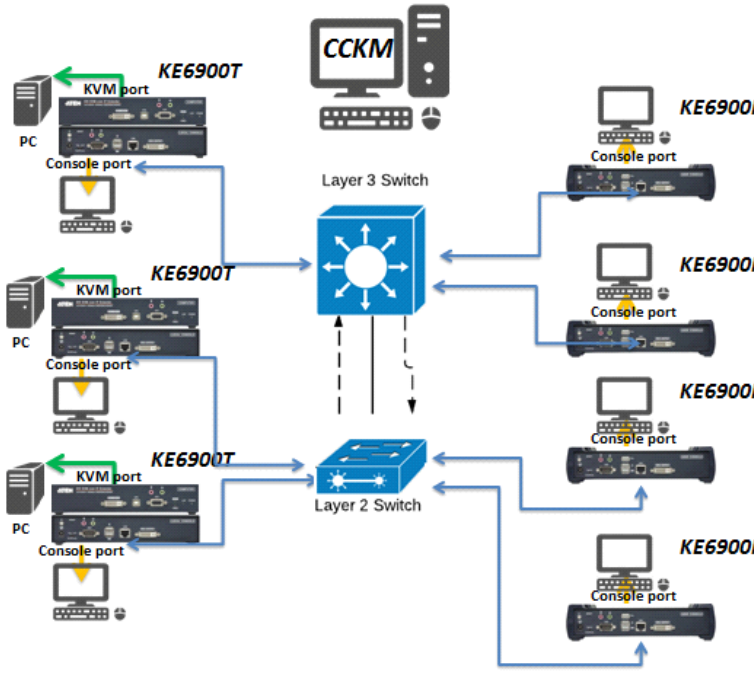
■ Determine the Distance

Distance is an important factor when setting up networks, with a shorter distance and fewer hops through routers, data can be transmitted more efficiently. So whenever possible decrease the distance and direct network traffic effectively between subnets that communicate with each other to increase the data throughput.

■ Ensure the Bandwidth

Ensuring the bandwidth ahead of time will guarantee performance before installing RCM/KE devices on a network. This will eliminate the primary cause of problems related to video quality and transmission of data. If the speed is right at all ends of your network, then the only other causes are derived from device failure or limits caused by a router, switch or device setting.

Sample Network Diagram



Choose a High Performance Switch

A high performance network switch is the means of a successful RCM/KE setup. When choosing a network switch, first select the type:

Layer 2 or Layer 3 Switches

You'll need to determine whether you need a layer 2 or a layer 3 switch for your RCM/KE network. Layer 3 switches cost more than layer 2 switches because they are more complex and handle more network traffic. The best way to calculate which type of switch you need is to first determine if you will have a dedicated network for the RCM/KE devices or if the RCM/KE devices will be on a network that shares throughput with other network equipment such as computers, servers and printers. If they share the network with other devices its best to consider a layer 3 switch and use layer 2 switches exclusively for the RCM/KE device connections. For larger installations we recommend using Layer 3 switches. The major differences are:

Layer 3 Switch: IP addresses in packets are examined and intelligent forwarding decisions are made. On a larger network broken into subnets across long distances, a layer 3 switch becomes the best choice as they can improve network efficiency and provide better traffic flow. They are better at directing more traffic to different locations on a larger more complex network, and with layer two switches working below them.

Layer 2 Switch: Packets are examined and forwarded using only the MAC address. If you have a small central network, a layer 2 switch should do the job. If the network is exclusive and will only transmit the bandwidth of RCM/KE devices, layer 2 switches with the correct settings can get the job done effectively.

Considerations

Number of ports

Choose a switch that has enough ports to match the number of RCM/KE devices you will be installing. Switches typically come in 5, 8, 10, 16, 24, 28, 48, and 52-port configurations. If you are installing 13 RCM/KE transmitters and 13 KE receivers, you will need to purchase a switch with at least 28 ports.

Stackable verse Standalone

Stackable switches allow you to easily manage and configure ports spanning across multiple switches that the RCM/KE devices are connected through. This provides a centralized method to configure and troubleshoot the initial setup of

RCM/KE devices on a network which makes fine tuning the bandwidth, data throughput and video quality easier. Stackable switches can be configured to direct the RCM/KE transmissions between many units more specifically and effectively. Standalone switches provide the same configuration features as Stackable switches but they must be set individually.

Stackable switches provide an easy way to manage multiple switches, as one unit. For example, instead of configuring, managing, and troubleshooting 6 28-port switches individually, you can manage the six as if they are a single unit using Stackable Switches. The six switches (168 ports) function as a single switch and are managed from one web or GUI interface.

What Stackable Switches Can do:

1. Create a link aggregation group with one port in one unit of the stack and another port of that group in another switch in the stack.
2. Select a port on one switch in the stack and mirror the traffic to a switch port on another unit of the stack; thus copy the configuration to direct traffic more effectively between RCM/KE devices.
3. Apply custom ACL security settings to any port on any switch in the stack.
4. Stackable switches can be setup in a ring configuration, so that if a port or cable fails, the stack automatically routes around the failure, at microsecond speeds. Stackable Switches also allow you to add and remove stack “members” which are automatically updated and recognized as such.

Switch Specifications

The following specifications are recommended when choosing a layer 2 or layer 3 switch:

- 1000Mbps Gigabit Ethernet switches (1000Mbps or faster Ethernet ports)
- High bandwidth between switches, if possible using Fibre Channel
- Layer 3 switches that efficiently processes IGMP queries
- IGMP Snooping v2 or v3
- Flow Control Functions
- Throughput of: Full Duplex, 1Gbps up- and down- stream speeds per port
- Performance of their most onerous tasks (e.g. IGMP snooping) with multiple dedicated processors (ASICS)
- Use the same switch make and model throughout each subnet

- The maximum number of simultaneous ‘snoopable groups’ the switch can handle meets or exceeds the number of RCM/KE transmitters that will be used to create Channel groups

Configuring Switches and RCM/KE Devices

Configuring the switch correctly will pass data more efficiently, allowing a better stream across the network to each RCM/KE device. The following settings will help optimize your network traffic through a switch:

- Enable IGMP Snooping on L2 switches
- Enable IGMP Querier on the L3 switch
- Enable IGMP Fast-Leave on all switches where RCM/KE units are directly connected
- Enable Spanning Tree Protocol (STP) on all switches and enable Portfast exclusively on switch ports that have RCM/KE units connected
- Pick an appropriate forwarding mode on all switches. Use Cut-through if available, or Store and Forward (see *Recommended Network Switches* below)

RCM/KE Transmitter Settings:

- Adjust the RCM/KE transmitter settings one at a time, in small intervals, and view the images as you do, so that you can adjust to the positive or negative results and achieve the best quality and bandwidth possible
- If the quality of color is important, set the Color Depth to 24 bits and manually adjust other settings until you are satisfied with the visual appearance
- If moving video images are shown frequently, increase the Video Quality setting to the highest level and reduce the Bandwidth Limit and Color Depth setting.
- When images on the screen are more often static, increase the Background Refresh and/or the Video Quality settings
- Check that all RCM/KE units have been updated with the latest firmware version

Recommended Network Switches

Below are the network switches that have passed ATEN's stress tests using the RCM/KE Series devices. Our tests streamed content over a network with a resolution of 1920 x 1200 @60Hz, 24-bit color depth.

- Cisco Catalyst 2960X / Catalyst 2960XR / Catalyst 3750
- HP Procurve 2920
- H3C S5120
- Huawei S5700
- DLink DGS-1510

Please refer to the FAQ link below on how to select network switches and network switch information collected by ATEN Customer Service Division, where the collected information includes customer's feedback from their actual experience in using and installing the product(s).

https://eservice.aten.com/eServiceCx/Common/FAQ/view.do?id=6276

Additional Mouse Synchronization Procedures

If the mouse synchronization procedures mentioned in the manual fail to resolve mouse pointer problems for particular computers, try the following:

Windows:

Note: In order for the local and remote mouses to synchronize, you must use the generic mouse driver supplied with the MS operating system. If you have a third party driver installed - such as one supplied by the mouse manufacturer - you must remove it.

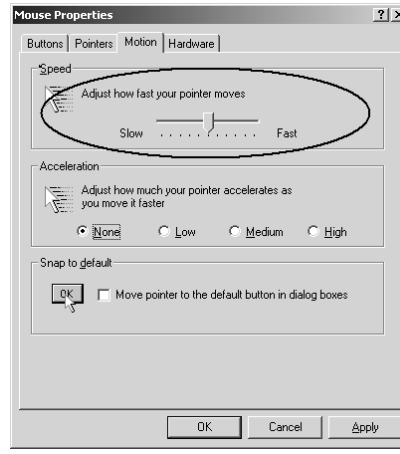
1. Windows 2000:

   a) Open the Mouse Properties dialog box (Control Panel → Mouse → Mouse Properties)

   b) Click the *Motion* tab

   c) Bring the mouse speed to the middle position (6 units in from the left)

   d) Set the mouse acceleration to *None*



2. Windows XP / Windows Server 2003 / Windows 7 / Windows 8 / Windows 10:

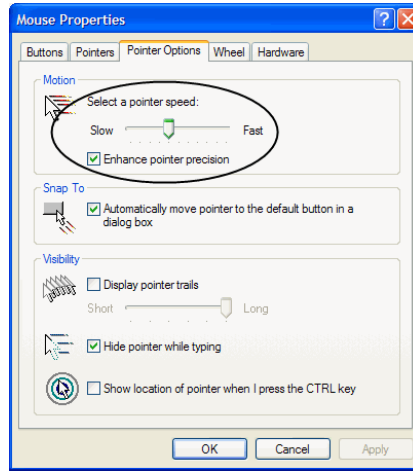
   a) Open the Mouse Properties dialog box (Control Panel → Mouse)

   (For Windows 10, click Start → Devices → Mouse → Additional mouse options)

b) Click the *Pointer Options* tab

c) Bring the mouse speed to the middle position (6 units in from the left)

d) Disable *Enhance Pointer Precision*



3. Windows ME:

   Set the mouse speed to the middle position; disable mouse acceleration (click **Advanced** to get the dialog box for this).

4. Windows NT / Windows 98 / Windows 95:

   Set the mouse speed to the slowest position.

Sun / Linux

Open a terminal session and issue the following command:

Sun: `xset m 1`

Linux: `xset m 0`
`or`
`xset m 1`

(If one does not help, try the other.)

Virtual Media Support

WinClient ActiveX Viewer / WinClient AP

- IDE CDROM/DVD-ROM Drives – Read Only
- IDE Hard Drives – Read Only
- USB CDROM/DVD-ROM Drives – Read Only
- USB Hard Drives – Read/Write*
- USB Flash Drives – Read/Write*
- USB Floppy Drives – Read/Write

* These drives can be mounted either as Drives or Removable Disks (see *Virtual Media*, page 201). Mounting them as removable disks allow booting the remote server if the disk contains a bootable OS. In addition, if the disk contains more than one partition, the remote server can access all the partitions.

- ISO Files – Read Only
- Folders – Read/Write
- Smart Card Readers

Java Applet Viewer / Java Client AP

- ISO Files – Read Only
- Folders – Read/Write

Note: 1. The Java Client supports Virtual Media in the same way as WinClient does – however, the account should have Administrator level privilege.

2. Folder mapping uses a FAT16 file system, so there is a 2G limitation. Virtual Media only supports ISO files less than 4G.

CCKM Server IP address Setup on Windows

1. Select **Network and Sharing Center** and click **Change adapter settings**.
2. Right-click **Local Area Connection** and select **Properties**.
3. In the Local Area Connection Properties window, highlight **Internet Protocol Version 4 (TCP/IPv4)** then click **Properties**.
4. Select **Use the following IP address** and enter in the IP for the CCKM server (e.g. any IP address not in use, and in between 192.168.0.2 and 192.168.0.253)*, Subnet Mask (e.g. 255.255.255.0), and Default Gateway that corresponds with your network setup.
5. Click **OK** to change the CCKM server's IP address.

Note: Make sure the CCKM server's IP address is not a duplicate to prevent IP address conflict.

To connect to the CCKM server via web browser, enter the CCKM IP address and port number (default: 8443). For example, if the CCKM IP address is 192.168.0.10, then enter https://192.168.0.10: 8443.

If you have a 2nd NIC, please follow the following steps.

6. Select **Network and Sharing Center** and click **Change adapter settings**.
7. Right-click **Local Area Connection** for the 2nd NIC and select **Properties**.
8. In the Local Area Connection Properties window, highlight **Internet Protocol Version 4 (TCP/IPv4)** then click **Properties**.
9. Select **Use the following IP address** and enter in the IP of the 2nd subnet for the CCKM server (e.g. any IP address not in use, and in between 192.168.1.2 and 192.168.1.253)*, Subnet Mask (e.g. 255.255.255.0), and Default Gateway that corresponds with your network setup.
10. Click **OK** to change the CCKM server's IP address of the 2nd subnet.

Limited Warranty

ATEN warrants its hardware in the country of purchase against flaws in materials and workmanship for a Warranty Period of two [2] years (warranty period may vary in certain regions/countries) commencing on the date of original purchase. This warranty period includes the LCD panel of ATEN LCD KVM switches. Select products are warranted for an additional year (see *A+ Warranty* for further details). Cables and accessories are not covered by the Standard Warranty.

What is covered by the Limited Hardware Warranty

ATEN will provide a repair service, without charge, during the Warranty Period. If a product is detective, ATEN will, at its discretion, have the option to (1) repair said product with new or repaired components, or (2) replace the entire product with an identical product or with a similar product which fulfills the same function as the defective product. Replaced products assume the warranty of the original product for the remaining period or a period of 90 days, whichever is longer. When the products or components are replaced, the replacing articles shall become customer property and the replaced articles shall become the property of ATEN.

To learn more about our warranty policies, please visit our website:

http://www.aten.com/global/en/legal/policies/warranty-policy/