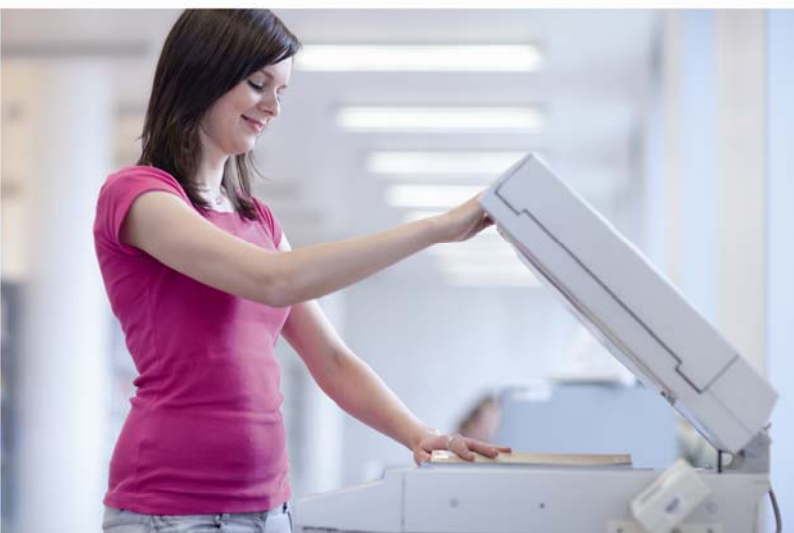


User's Manual



8-Port Combo KVM Over IP Switch

▶ IKVM-8020



Copyright

Copyright © 2013 by PLANET Technology Corp. All rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual or otherwise, without the prior written permission of PLANET.

PLANET makes no representations or warranties, either expressed or implied, with respect to the contents hereof and specifically disclaims any warranties, merchantability or fitness for any particular purpose. Any software described in this manual is sold or licensed "as is". Should the programs prove defective following their purchase, the buyer (and not PLANET, 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. Further, PLANET reserves the right to revise this publication and to make changes from time to time in the contents hereof without obligation to notify any person of such revision or changes.

All brand and product names mentioned in this manual are trademarks and/or registered trademarks of their respective holders.

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and receiver.
3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4. Consult the dealer or an experienced radio technician for help.

FCC Caution

To assure continued compliance. (example-use only shielded interface cables when connecting to computer or peripheral devices). Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This 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.

Federal Communication Commission (FCC) Radiation Exposure Statement

This equipment complies with FCC radiation exposure set forth for an uncontrolled environment. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 20 cm (8 inches) during normal operation.

Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this and of the computer manufacture must therefore be allowed at all times to ensure the safe use of the equipment.

CE Mark Warning

This is a Class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

WEEE Regulation

To avoid the potential effects on the environment and human health as a result of the presence of hazardous substances in electrical and electronic equipment, end users of electrical and electronic equipment should understand the meaning of the crossed-out wheeled bin symbol. Do not dispose of WEEE as unsorted municipal waste and have to collect such WEEE separately.

Revision

User's Manual for PLANET 8-Port Combo KVM over IP switch
Model: IKVM-8020
Rev: 1.00 (January.2013)
Part No. EM-IKVM-8020

Table of Contents

CHAPTER 1 INRODUCTION	5
1.1 Features.....	7
1.2 Package Contents.....	7
1.3 Technical Specifications	8
CHAPTER 2 INSTALLATION.....	9
2.1 System Requirements	9
2.2 Cable Diagrams	9
2.3 Product Details	10
2.4 Hardware Installation.....	11
2.5 Cascade Chain Connection Diagram	13
CHAPTER 3 Operations.....	15
3.1 Manual Key	15
3.2 Hot Key and Mouse Clicking	15
3.3 OSD (On Screen Display)	15
Chapter 4 Remote Usage	24
4.1 Prerequisite	24
4.2 Login and Logout	25
4.2.1 Login.....	25
4.2.2. Logout.....	27
4.3 The Remote Console.....	27
4.3.1 Remote Console Control Bar.....	28
4.3.2 Remote Console Status Line.....	33
Chapter 5 Menu Options	34
5.1 Remote Control.....	34
5.1.1 KVM Console.....	34
5.1.2 Telnet/SSH Console.....	34
5.1.3 Remote Wakeup.....	35
5.2 Virtual Media.....	38
5.2.1 Drive Redirection.....	39
5.2.2 Virtual Drive	40
5.2.3 CD/DVD Image.....	40
5.3 User Management.....	42
5.3.1 Change Password.....	42
5.3.2 Users	42
5.4 KVM Settings.....	44
5.4.1 User Console.....	44
5.4.2 Keyboard/Mouse.....	47
5.4.3 Video.....	48
5.5 Device Settings	49
5.5.1 Network	49
5.5.2 Dynamic DNS.....	52
5.5.3 Security.....	54
5.5.4 Certificate	56
5.5.5 Serial Port	57
5.5.6 Date / Time	57
5.5.7 Event Log	59
5.5.8 Authentication.....	60
5.5.9 USB	61
5.5.10 Config File.....	61
5.6 Maintenance.....	61
5.6.1 Device Information.....	62
5.6.2 Even log.....	63
5.6.3 Unit Reset	63
Appendix A Cable Connectors Specifications	65
Appendix B Troubleshooting & Frequently Asked Questions.....	66

CHAPTER 1 INTRODUCTION

Easily Control Servers with Flexibility

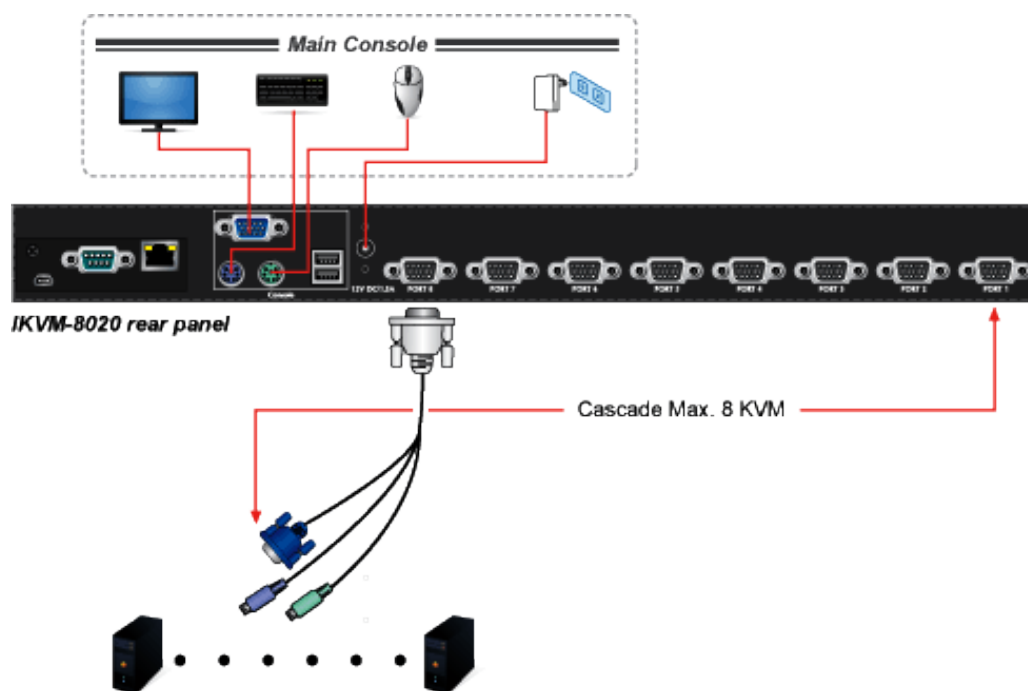
The PLANET 8-Port Combo IP KVM Switch, IKVM-8020 is an enterprise-class, secure, KVM-over-IP switch that provides BIOS-level control of up to 64 servers. Use a dedicated micro-controller and potentially specialized video capture hardware to capture the video, keyboard, and mouse signals, compress and convert them into packets, and send them over an Ethernet link to a remote console application that unpacks and reconstitutes the dynamic graphical image. This IP KVM solution includes standard features such as Powerful Mouse / Keyboard Support such as installing software, transferring files and backing up data.



Powerful VGA / Mouse / Keyboard Support

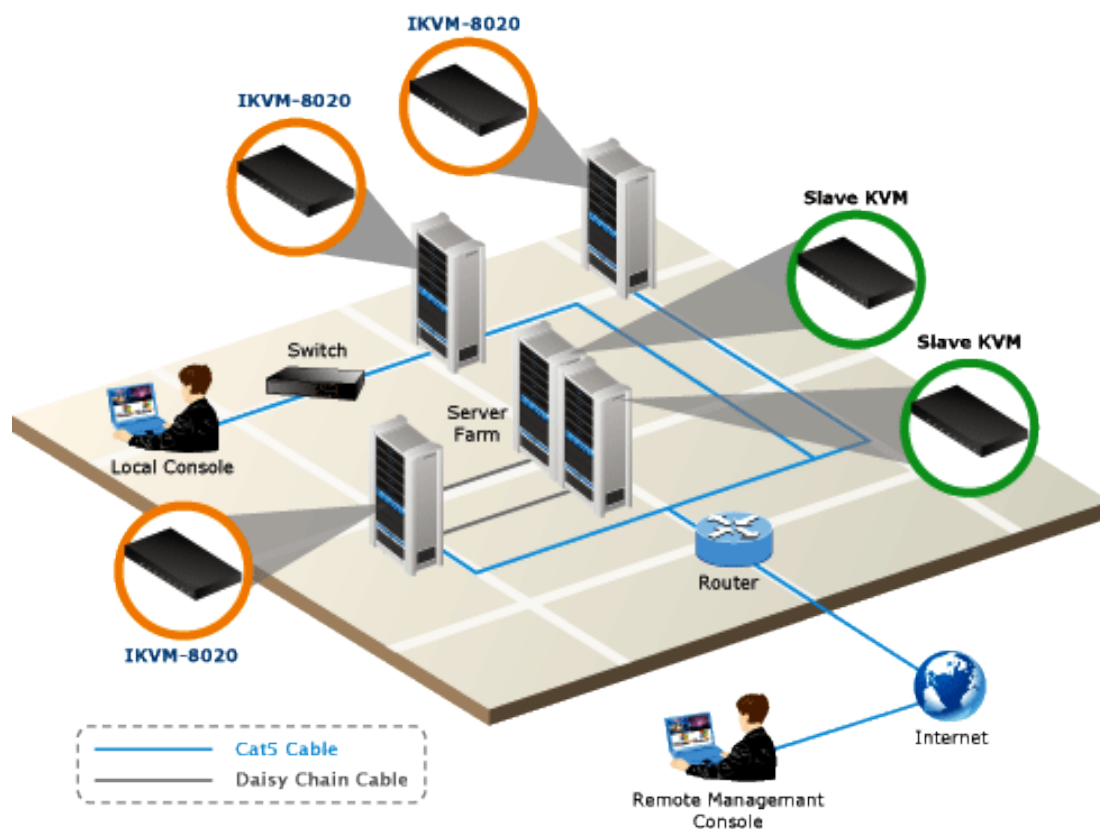
The IKVM-8020 will detect the current video mode of the console automatically; and manual fine-tuning is also available to receive an optimal video quality. The IKVM-8020 will accept video streams with a dot clock rate up to 110MHz, therefore, the remote VGA resolution can up to 1600 x 1200 video resolutions.

User can connect up to 8 PCs to the IKVM-8020. The IKVM-8020 also fully supports various models of PS/2 and USB mice manufactured by Logitech, Microsoft and IBM as well as compatible PS/2 and USB mice of other brands. The KVM supports the PS/2 and USB Keyboard Port of the CODE SET 1/2/3 and further allows you to use the KVM for all kinds of servers and PCs.



Easy Switching , Efficient Management

The IKVM-8020 can fully control the connected PCs of any platform through any at-hand browser or just work as a normal 8-Port KVM Switch in local site. By the support of daisy chain function, users can cascade one IKVM-8020 to multiple KVM-810 or KVM-1610, and manage this KVM chain with one single IP. The IKVM-8020 is the ideal choice for those users who want to maintain their PC system at office or home 24/7.



1.1 Features

Hardware

- 19" rack mount 1U size design
- LED display for easy status monitoring
- Built-in one extra daisy chain port to cascade with KVM-810 and KVM-1610
- High Video Resolution up to 1920 x 1440 (local side) or 1600 x 1200 (remote side)
- Supports hot plug; no need to power off the KVM switch or PCs when adding or removing PCs

System

- Supports SSL protocol for any encrypted network traffic between itself and a connected client
- Automatically senses video resolution for best possible screen capture
- No Software Required : easy PC selection via On Screen Display (OSD) menu, Push Buttons, Hot Keys
- Compliant with DOS, Windows, Netware, Unix, Linux, iMAC, Power MAC and Sun Micro Systems with USB port by connecting with a USB-PS/2 adapter

Installation

- Remote mass storage control
- Supports password protection and PC server name search
- Buzzer sound for switching port confirmation
- Keyboard status restored when switching PCs

1.2 Package Contents

- ◆ 1 x 8-port KVM switch
- ◆ 1 x User's Manual
- ◆ 1 x CD-ROM
- ◆ 1 x Adaptor (for US. EU. UK. AU type)
- ◆ 2 x KVM Cable (3-in-1 KVM Cable for Computer side)
- ◆ 2 x Rack Mount Kit
- ◆ 6 x Rack Mount Screw
- ◆ 4 x Pad



.....
1. If any of the above items are missing, please contact your dealer immediately.

2. Using the power supply that is not the one included in unit packet will cause damage and void the warranty for this product.
.....

1.3 Technical Specifications

Model	IKVM-8020
Hardware Interface	
PC Port	8
Host Connectors (all female type)	HDDB 15-pin x 8
Local Console Connectors (all female type)	USB keyboard port & USB mouse port PS/2 keyboard port & PS/2 mouse port HDDB 15-pin VGA port
Daisy Chain Connectors (all female type)	PS/2 keyboard port PS/2 mouse port HDDB 15-pin VGA port
Remote Console	10/100 Mbps Ethernet, RJ-45
Control Feature	
Max connected PCs	64 (by cascade 8 KVM-810)
Max cascade levels	2
Port Selection Keys	8
PC Selection	On Screen Display Menu / Hot Key / Button
VGA Resolution	Local console: 1920 x 1440 Remote console: 1600 x 1200
Network and Configuration	
Network Standard	IEEE 802.3 10Base-T IEEE 802.3u 100Base-TX
Supported Protocol	TCP, IP, ARP, ICMP, HTTP/HTTPS, Telnet, SSH, DHCP/BOOTP, PPP, SMTP, DNS, NTP, Dynamic DNS
Client Software	Microsoft Java VM, Sun Java VM (Plug in), Netscape Java VM
Remote Access Key	128-bit SSL / 256-bit SSL(Firefox)
Keyboard / mouse Emulation	USB & PS/2
DDC / EDID communication	DDC2
Environment	
Dimension (W x D x H)	160 x 444.5 x 44.3 mm
Weight	2.76kg
Environmental Specification	Operating temperature: 0 ~ 50 Degree C

	Storage temperature: -20 ~ 60 Degree C Relative humidity: 0 ~ 80% (non-condensing)
Power Requirement	12V DC, 1.5A
Electromagnetic Compatibility	FCC, CE

CHAPTER 2 INSTALLATION

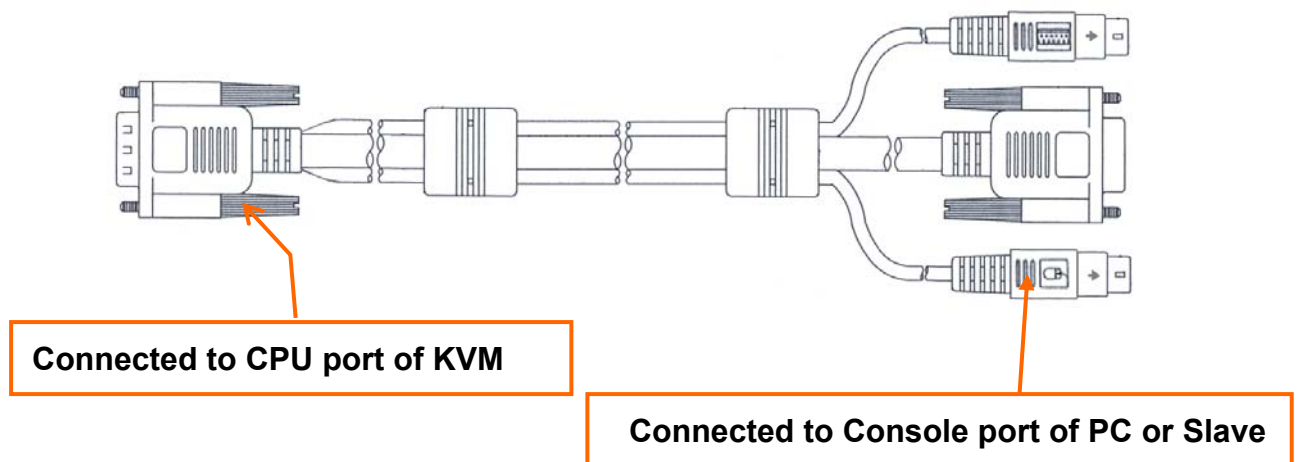
2.1 System Requirements

IKVM-8020

Description	8-Port Combo KVM Switch
Console side	One VGA Monitor One PS/2 Keyboard One PS/2 Mouse One USB Keyboard One USB Mouse
Computer side	8 * 3-in-1 KVM Cable (VGA / Keyboard / Mouse) [Optional]

2.2 Cable Diagrams

3-in-1 KVM Cable is for PS2 Computer or Server; connected USB PC or Server, Please use PS2 to USB Adapter



PS/2 Cable:

Mini Din 6 pin Male to Male



AT to PS/2 keyboard adapter: (Optional)

Din 5 pin Male to Mini Din 6 pin Female



VGA Cable:

HDB15 pin Male to Male



PS2 to DB9 adapter: (Optional)

Mini Din 6 pin Female to DB 9 pin Female



2.3 Product Details

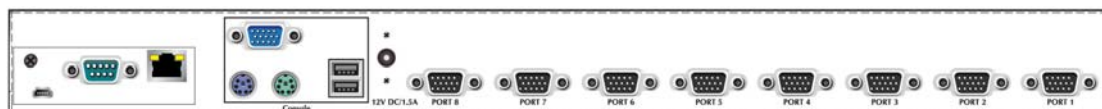
Front panel



LEDs	Color	Description
Power	Blue	A blue light indicates that the KVM is operating.
Port	Green	The PC or KVM connected to the corresponding port is on and operating.
	Red	The situation of being connected to the port.

Button	Description
OSD	OSD Control Mode.
Console-Reconfirmed	The keyboard and mouse will be reconnected, and the EDID in the screen will be read again.

Real panel



Port	Description
CPU	Install the cable connected to a PC here.
Console	<p>◆ In the Master KVM, connect the monitor, keyboard and mouse here.</p> <p>◆ In the Slave KVM, connect the cable come from the Master CPU port here.</p>

2.4 Hardware Installation

Before installation, please make sure all of peripherals and computers have been turned off.

Step 1 Rack Installation

Find a convenient place to put your KVM Switch. Its 19" rack mount form factor makes it ideal stackable on 19" rack. When stacking to a rack, attach the included brackets to the sides of the KVM Switch. Take note of the length of your cables so that your computers, KVM Switch, keyboard, mouse and monitor are distanced properly.

Step 2 Connecting Monitor to the KVM Switch

Connect the monitor to the KVM Switch. Using the attached cable, or the one included with your monitor, connect it to the HDDB-15 female port on the back of the KVM unit labeled with the monitor symbol at the CONSOLE port connector.



Step 3 Connecting Keyboard to the KVM Switch

Connect the keyboard and mouse to the KVM Switch. If you have an AT type keyboard, you will need an AT to PS/2 adapter.



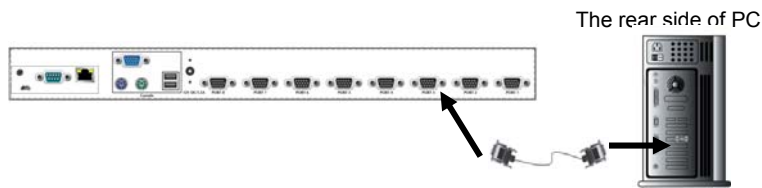
Step 4 Connecting Mouse to the KVM Switch

Connect the mouse to the KVM Switch.



Step 5 Connecting VGA/Mouse/Keyboard port of PC(s) to the KVM Switch

Install the Master KVM to the 3-in-1 cable (same as the cable for connecting the KVM to the PC) in the middle of the Slave KVMs.



Step 6 Check Again

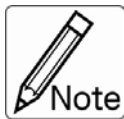
Double-check all of the connections. You can check the color of keyboard and mouse connector to make sure the keyboard and mouse cables go to the correct ports.

Step 7 Connecting Other PCs

Repeat step 5 for the remainder of the computers.

Step 8 Connecting KVM Power

Attach the power supply to the KVM unit and plug the other end into an electrical receptacle. Now you will see the LED for Port 1 light up, and you will hear a beep. Switch on your monitor.



.....
It is not necessary to power down the whole system for install a new PC or KVM thereafter. All you need is to make sure that the new PC or KVM is OFF during the installation. If the KVM powers down due to external Factors (such as power failure or the power of the KVM is turned off), we recommend you to reinstall the whole system.
.....

2.5 Cascade Chain Connection Diagram

Step 1 Rack Installation

Find a convenient place to put your KVM Switch. Its 19" rack mount form factor makes it ideal stackable on 19" rack. When stacking to a rack, attach the included brackets to the sides of the KVM Switch. Take note of the length of your cables so that your computers, KVM Switch, keyboard, mouse and monitor are distanced properly.

Step 2 Connecting Monitor to the KVM Switch

Connect the monitor to the KVM Switch. Using the attached cable, or the one included with your monitor, connect it to the HDDB-15 female port on the back of the KVM unit labeled with the monitor symbol at the CONSOLE port connector.



Step 3 Connecting Keyboard to the KVM Switch

Connect the keyboard and mouse to the KVM Switch. If you have an AT type keyboard, you will need an AT to PS/2 adapter.



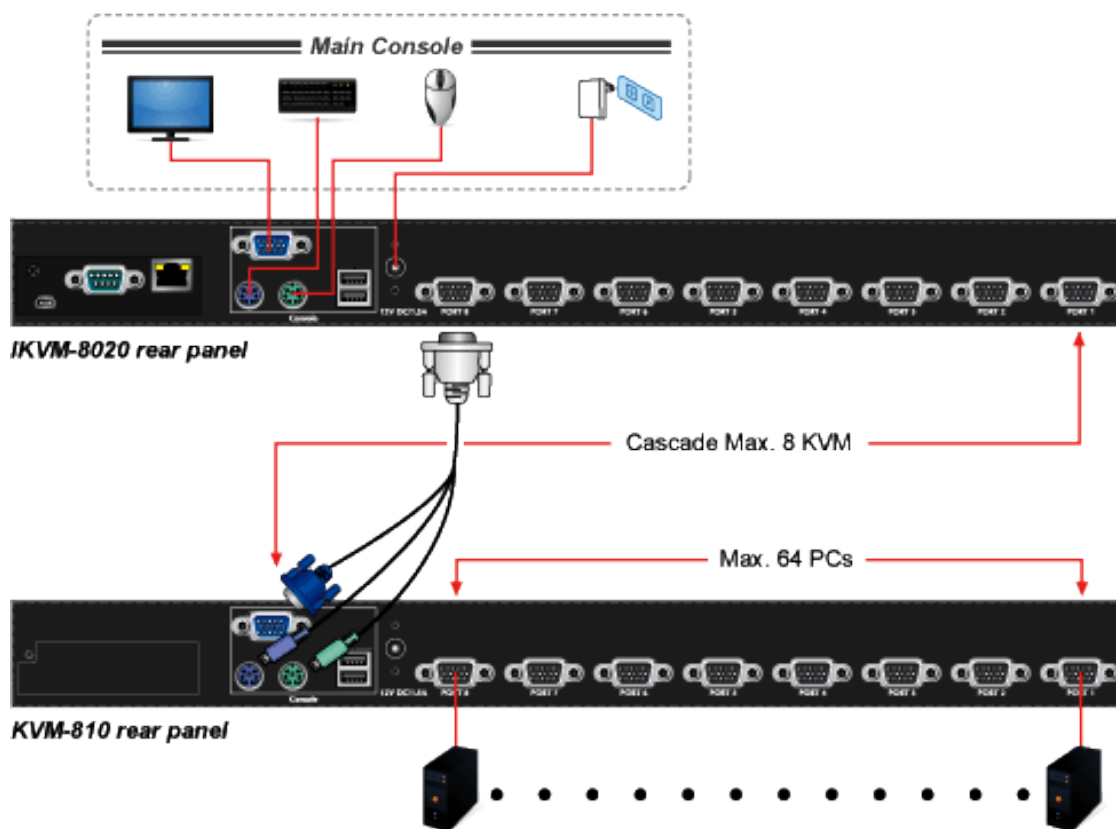
Step 4 Connecting Mouse to the KVM Switch

Connect the mouse to the KVM Switch.



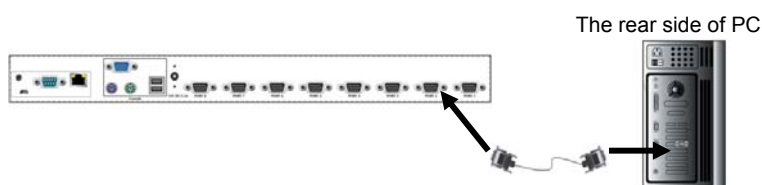
Step 5 Connecting console port of KVM to the KVM Switch

Use the 3-in-1 cable(or with PS2 to USB Adaptor) to connect the CPU port of the master KVM in parallel to the console port of the slave KVM.



Step 6 Connecting VGA/Mouse/Keyboard port of PC(s) to the KVM Switch

Install the Master KVM to the 3-in-1 cable (same as the cable for connecting the KVM to the PC) in the middle of the Slave KVMs.



Step 7 Check Again

Double-check all of the connections. You can check the color of keyboard and mouse connector to make sure the keyboard and mouse cables go to the correct ports.

Step 8 Connecting Other PCs

Repeat step 5 - 6 for the remainder of the computers.

Step 9 Connecting KVM Power

Attach the power supply to the KVM unit and plug the other end into an electrical receptacle. Now you will see the LED for Port 1 light up, and you will hear a beep. Switch on your monitor.

CHAPTER 3 Operations

3.1 Manual Key

It is the simplest switching method. You just need to press the Port Selection Switch on the front panel of the KVM. The Selection LED (**Red**) is on, indicating that you are switching to the corresponding port.



- 1. The Port Selection Switch functions only when connected to a PC.
- 2. If the Offline Skip of the OSD System Setting is Auto, then you cannot make any switch when pressing an offline Port Selection switch.
- 3. For Auto Scan Mode, none of the Port Selection Switches functions

3.2 Hot Key and Mouse Clicking

Hot key and mouse clicking are applicable for switching a small section. You can select the SVS (Smart View Setting) from the OSD of the PC first (for a quick switch of PC) and use the keyboard (press the **Ctrl** key twice) or the mouse (press and hold the middle button while pressing the left or right button) to switch to the previous or next set of PC.



The mouse must have at least 3 keys. As far as you select a PC with the SVS, you can use this method for the switch.

3.3 OSD (On Screen Display)

Press the NumLock on the keyboard twice or simultaneously press the Push Buttons 1 and 2 of the Port Selection Switch on the KVM panel to start the OSD. Use the key Up, Down and Enter keys on the keyboard to switch or directly move the mouse to the target PC, and then double click the left button.

Additionally, you also can use the numeric keys to enter the direct switch. For example, if you want to switch a PC to the Slave KVM port 04 under the Master KVM port 03, then you can start the OSD and then directly enter 0304. If you are using a standalone machine, then just enter the first two digits.

More OSD related information is given in the following OSD sections.

Start

Press the NumLock twice or the Port Selection Switches 1 and 2 on the panel to enter the OSD.



If you have modified the Hot Key for starting the OSD and are unable to enter the OSD by pressing NumLock, and then you can start the OSD by using Port Selection Switch first, and then press F9 to enter into the System Setting to modify the options of the OSD Entry Hot Key.

If you have modified the Hot Key for starting the OSD and are unable to enter the OSD by pressing NumLock, then you can start the OSD by using the Port Selection Switch first, and then press F9 to enter into the System Setting to modify the options of the OSD Entry Hot Key.

Operation

You can operate the options by keyboard or mouse. For the keyboard operation, besides the common Up and Down keys, there are special function keys such as Enter, Space Bar, Function Key (F1, F4...) under the OSD remark field. For the mouse operation, the left key refers to Enter and the right key refers to Exit. For example, move the mouse point to your desired PC, and click the left key. The selection bar will move to that position and then click the left key again for the execution.



You must use the keyboard to complete the two functions: Name Edit and Password.

Switch Menu

Master List

1	{	03-04:Mail Ser 4	
2	{	LIST: MASTER	
		PWR C# KVM NAME SVS	
		• 01 Admin ⊕	
		• 02 ⊖	
3	{	• 03 04 Mail Group O	Press Enter
		• 04 ⊖	
		• 05 Peter ⊕	
		• 06 08 Web Group O	
		• 07 16 Data Group O	
		• 08 ⊖	
4	{	⬅️ ⬆️ ⬇️ ⬆️ ⬆️: Move Space: Edit Esc: Exit	
		F1: Smart View Enter: Switching	
		F4: Auto Scan F9: System Setting	
		F5: Clear Name List	

Slave List

03-04:Mail Ser 4
LIST: Mail Group
PWR C# KVM NAME SVS
• 01 Mail Ser 1 ⊖
• 02 Mail Ser 2 ⊖
• 03 Mail Ser 3 ⊕
• 04 Mail Ser 4 ⊕
⬅️ ⬆️ ⬇️ ⬆️ ⬆️: Move Space: Edit Esc: Exit
F1: Smart View Enter: Switching
F4: Auto Scan F9: System Setting
F5: Clear Name List

1. This field provides the information of the currently connected PC. As shown in the figure above, 03 refer to the Port Number of the Master; 04 refer the Port Number of the Slave; and Mail Ser 4 is the name of this PC defined by Users. If a PC connects to the Master, then the number consists of the first two digits. If a User has not given a name for the PC, the name field will be blank.

2. This field shows the list of the Master KVM or a certain set of Slave KVM currently displayed on the OSD. We recommend you to give a name to the Slave KVM, or else the display after LIST: will be blank.
3. This field shows the list of connections to the KVM, and the fields are described below: PWR: It shows the status of power supply and indicates a normal power supply for the equipment (PC or KVM) connected to the CPU port.

C#: It shows the channel number; the KVM-810 will display 01~08 and the KVM-1610 will display 01~08; 09~16 (Since the screen cannot display all at a time, therefore you can use PgUp / PgDn to switch the pages).

KVM: It shows the KVM model. If there is a number in this field, it shows that a set of KVM connects to this port. The number 04 indicates Port 4 and 08 indicates Port 8 and 16 indicates Port 16 and so on.



If the connected KVM is not on, there will have no number in this field.

NAME: It shows the name of the equipment, and users can name the Slave KVM or PC on their own. There are a total of 12 characters selected from the group of "A~Z", "a~z", "0~9", "+", "-", "*", "/", "=", "[", "]", ",", ".", ":".



Please use the CapsLock to toggle the upper and lower cases.

SVS: It shows the Smart View Setting; use ⊕ to open and ⊖ to close. The SVS is blank and not clickable if the KVM is connected in parallel. If this option is set to open, then you can make the switch by operating the Hot Key Switch or Mouse Clicking or selecting the option by Auto Scan. You also can use mouse to click this field.

Selection BAR: It shows the selection bar (**Green**); you can use the ↑↓ keys on the board to move the selection bar, and the situated position indicates the selected target for giving instructions. For example, if the selection bar points at C#05 and you press Enter, then the system will switch to that particular PC or press the “Space BAR” to start editing the name. Press F4 to enable/disable the SVS option.

4 、 Instruction Hint Field:

↑↓: Use the ↑↓ keys on the keyboard or the mouse to move the selection bar
(Move)

SPACE: The “Space BAR” on the keyboard is used to start editing the name of the PC or KVM.
(Edit)

ESC: Use the “Esc” key on the keyboard to exit the current option or exit OSD.
(Exit)

F4: Use the F4 key to run Auto Scan, and you can set the residing time, channel display time and mode of the Auto Scan from System Setting.
(Auto Scan)

F9: Use the F9 key to enter into the System Setting Menu.
(System Setting)

F5: Use the F5 key to clear the values of all Name fields. If you clear the name list under the Master screen, then you will also clear the name lists under all slaves. If you clear the name list under a certain slave, then you only clear the name list under that particular Slave KVM.
(Clear Name List)

F1: It switches the Smart View Setting.
(Smart View)

System Setting Menu

System Setting

Channel Display Mode	Full
Channel Display Tim	5 Sec
Auto Scan Time	5 Sec
OSD Entry Hot Key	Number Lock
Hot Key Switching	OFF
Mouse Clicking	OFF
Beeper Sound	ON
Offline Skip	Manual
OSD Language	English
Security Level	None
Console Lock Time	5 Min
↑↓	Move
Space	Change
Esc	Exit
F1	Information
F4	OSD Position
F8	Restore Default Setting

Item	Description	Default	Other Selection
Channel Display Mode	For Port Switching, Auto Scan and OSD Close, the Monitor will show the Channel information and mode selection.	Full	Number, Name
Channel Display Time	It shows the time for displaying channel information.	5 Sec	10Sec, Always, None
Auto Scan Time	For Auto Scan, it shows the residing time for each port.	5 Sec	10Sec, 20Sec, 30Sec, 60Sec
OSD Entry Hot Key	Select to turn on the hot keys of the OSD control screen.	NumLock	Scroll Lock, Shift, None
Hot Key Switching	Turn on/off the "Ctrl" hot keys on the keyboard for switching computer functions.	OFF	ON
Mouse Clicking	Turn on/off the keys of the mouse for switching computer functions.	OFF	ON
Beeper Sound	Turn on/off the beeper sound function.	ON	OFF
Offline Skip	Set the offline skip function to auto or manual.	Manual	Auto
OSD Language	Select the language for the OSD.	English	Francis, Deutsch, Italian, Espino
Security Level	Select the security mode and level.	None	Low, High
Console Lock Time *1	The lock time of console port.	5 Min	1Min, 3Min, 10Min, 30Min, 60Min

*1: You can select this option only if the Security Level is not "None".

F1: Information; It provides the model name and F/W version information, which is helpful for users to understand the updated version.

F4: OSD Position; you can enter the OSD position to make adjustments; we recommend you to unify the resolution for all computer display mode, and use this function again to adjust the OSD position. You can use the Up, Down, Left or Right keys on the keyboard or a mouse to move the OSD position.

F8: Restore Default Setting; Restore the factory default settings. Please note that all name lists will be cleared and the system settings are set to the default settings as shown in the table above.

Esc: Exit; Exit the system setting and close the OSD. If you have made changes in this option, the system will ask whether or not you want to save the setting before the selected option is effective.

Auto Scan Mode: You can start the OSD first and press “F4” to enter the Auto Scan Mode. If you want to scan the PC, you must use the Smart View Setting to select the Auto Scan Time in the System Setting for the residing time, which includes 5 sec, 10 sec, 20 sec, 30 sec and 60 sec. You can adjust the Channel Display Mode and Channel Display Time from the Channel Display mode. By then, all keys on the panel, keyboard and mouse are not operable. You can only use the ESC key to exit the Auto Scan Mode.

Security Mode: Switch the Security Level from “None” to “Low” in the System Setting, and enter your Password (“A~Z”, “0~9”, a maximum of 12 characters), and the security will be effective after you confirm the Password. The use of the Console Lock Time is to set the time to enter a security mode after the keyboard and mouse has idled for a predetermined time. Once you enter into the security mode, you need to enter the correct password before you can move the mouse or enter any key from the keyboard. You need a correct password to operate the whole system normally.

Important Note: What should I do if I forgot my Password?

After you enter a wrong password for 5 consecutive times, a time delay bar will appear, and a set of “Magic Numbers” will show up at the bottom.

Record the magic numbers and contact with your distributor.

Console - Reconfirmed: Simultaneously press the largest two numbered Port Selection Switches on the panel to start the Console- Reconfirmed. If you change the Console equipment, please use this function to let KVM reconfirm the equipment at the Console end once.

EDID & DDC: A vast majority of computer monitors supports the Extended Display Identification Data (EDID) and allows data access by Display Data Channel (DDC). The KVM also supports these two specifications, but the KVM only reads the EDID of the Monitor when the KVM is on. If it is necessary to change monitors during an operation, please use the Console Reconfirmed function to read the EDID again.

Chapter 4 Remote Usage

4.1 Prerequisite

The IKVM-8020 feature an embedded operating system and applications offering a variety of standardized interfaces. This chapter will describe both these interfaces, and the way to use them in a more detailed manner. The interfaces are accessed using the TCP/IP protocol family, thus they can be accessed using the built-in Ethernet port.

The following interfaces are supported:

HTTP/HTTPS

The IKVM-8020 can be entirely managed using a standard web browser. You can access the IKVM-8020 using the insecure HTTP protocol, or using the encrypted HTTPS protocol. Whenever possible, use HTTPS.

Telnet

A standard Telnet client can be used to access an arbitrary device connected to the IKVM-8020 port via a terminal mode.

The primary interface of the IKVM-8020 is the HTTP interface. This is covered extensively in this chapter. Other interfaces are addressed in subtopics.

In order to use the Remote Console window of your managed host system, the browser has to come with a Java Runtime Environment version 1.1 or higher. If the browser has no Java support (such as on a small handheld device), you are still able to maintain your remote host system using the administration forms displayed by the browser itself.

Important: We recommend installing a Sun JVM 1.5 or above.

For an insecure connection to the IKVM-8020, we can recommend the following browsers:

- Microsoft Internet Explorer version 8.0 or higher on Windows 2000, Windows XP, Windows Server 2003 and Win7.
- Mozilla Firefox 14 on Windows 2000, Windows XP, Windows Server 2003, Win7 and Linux and other UNIX-like Operating Systems

In order to access the remote host system using a securely encrypted connection, you need a browser that supports the HTTPS protocol. Strong security is only assured by using a key length of 128 Bit. Some of the old browsers do not have a strong 128 Bit encryption algorithm.

Using the Internet Explorer, open the menu entry “?” and “Info” to read about the key length that is currently activated. The dialog box contains a link that leads you to information on how to upgrade your browser to a state of the art encryption scheme. The picture below shows the dialog box presented by the Internet Explorer 8.0.



Newer web browsers do support strong encryption on default.

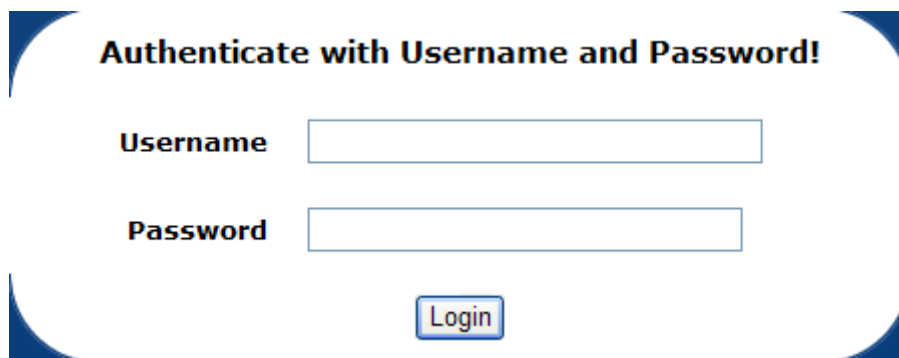
4.2 Login and Logout

4.2.1 Login

Note:	Your web browser has to accept cookies, or else login is not possible.
--------------	--

Launch your web browser. Direct it to the address of your IKVM-8020, which you configured during the initial configuration. The address used might be a plain IP address or a host and domain name, in the case where you have given your IKVM-8020 a symbolic name in the DNS. For instance, type the following in the address line of your browser when establishing an unsecured connection: `http://<IP address of IKVM-8020 >`

When using a secure connection, type in: `https://<IP address of IKVM-8020 >`
This will lead you to the IKVM-8020 login page.

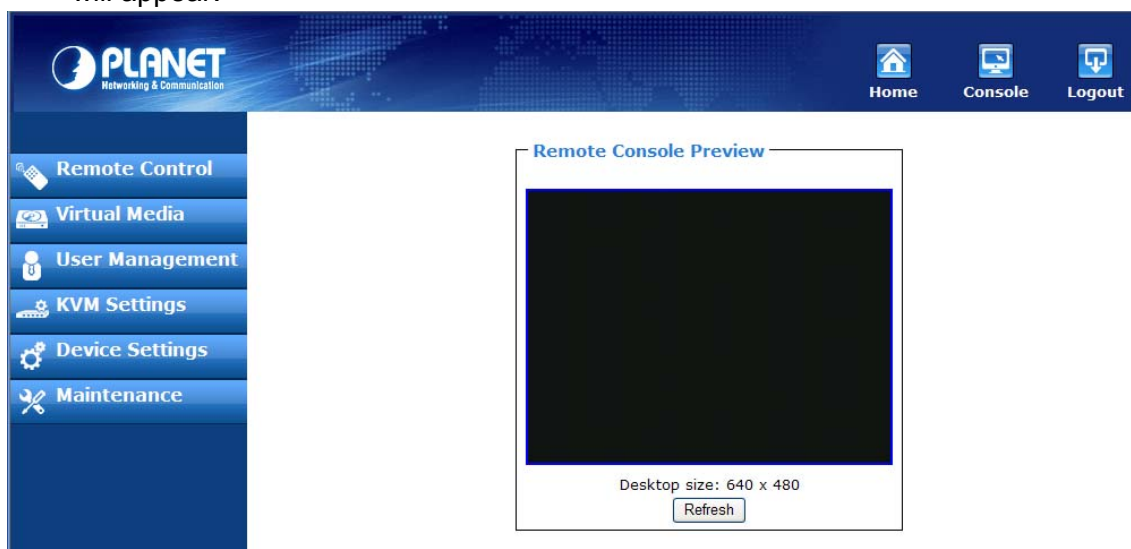


The IKVM-8020 has a built-in super user that has all permissions to administrate the device:




Login name	super (in default)
Password	pass (in default)

Note: Please change the super user password immediately after the first time login successfully. Not changing the pass phrase for the super user is a severe security risk and might result in unauthorized access to the IKVM-8020 and to the host system including all possible consequences!

Having logged into the IKVM-8020 successfully, the main page of the IKVM-8020 will appear.



This page consists of three parts; each of them contains specific information. The buttons on the upper side allow you to navigate within the front end.

 Home	Return to the main page of the IKVM-8020.
 Console	Open the IKVM-8020 remote console.
 Logout	Exit from the IKVM-8020 front end.

The lower left frame contains a navigation bar and allows you to switch between the different sections of the IKVM-8020. Within the right frame, task-specific information is displayed that depends on the section you have chosen before.

Warning: If there is no activity for half an hour, the IKVM-8020 will log you out, automatically. A click on one of the links will bring you back to the login screen.

4.2.2. Logout



This button logs out the current user and presents a new login screen.

Please note that an automatic logout will be performed in case there is no activity for half an hour.

4.3 The Remote Console



Clicking on the icon opens an additional Remote Console window. The Remote Console window is a Java Applet that tries to establish its own TCP connection to the IKVM-8020. The protocol that is run over this connection is neither HTTP nor HTTPS, but RFB (Remote Frame Buffer Protocol). Currently, RFB tries to establish a connection to port number 443. Your local network environment has to allow this connection to be made, i.e. your firewall end, in case you have a private internal network, your NAT (Network Address Translation) settings have to be configured accordingly.

In case the IKVM-8020 are connected to your local network environment and your connection to the Internet is available using a proxy server only without NAT being configured, the Remote Console is very unlikely to be able to establish the according connection. This is because today's web proxies are not capable of relaying the RFB protocol.

In case of problems, please consult your network administrator in order to provide an appropriate network environment.

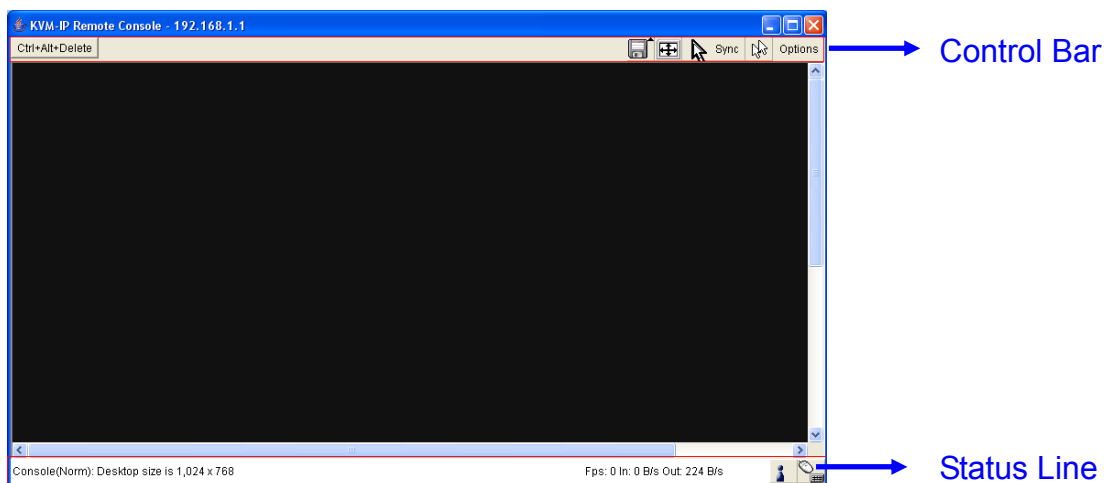
Once the Remote Console is connected, it displays the screen content of your host system. The Remote Console will behave exactly in the same way as if you were sitting directly in front of the screen of your remote system. That means keyboard and mouse can be used in the usual way. However, be aware of the fact that the remote system will react to keyboard and mouse actions with a slight delay. The delay depends on the bandwidth of the network which you use to connect to the IKVM-8020.





With respect to the keyboard, the very exact remote representation might lead to some confusion as your local keyboard changes its keyboard layout according to the remote host system. If you use a German administration system, and your host system uses a US English keyboard layout, for instance, special keys on the German keyboard will not work as expected. Instead, the keys will result in their US English counterpart. You can circumvent such problems by adjusting the keyboard of your remote system to the same mapping as your local one.

The Remote Console window always tries to show the remote screen with its optimal size. That means it will adapt its size to the size of the remote screen initially and after the screen resolution of the remote screen has been changed. However, you can always resize the Remote Console window in your local window system as usual.

4.3.1 Remote Console Control Bar

The upper part of the Remote Console window contains a control bar. Using its elements you can see the state of the Remote Console and influence the local Remote Console settings. A description for each control follows.

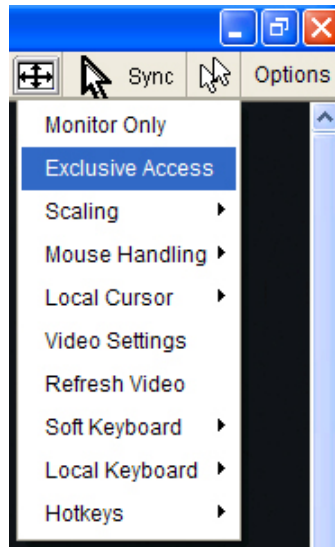


Controls	Description
	Special button to send the "Control+Alt+Delete" key combination to the remote system.
 Auto Adjust Button	If the video display is of bad quality or distorted in some way, press this button and wait a few seconds while the IKVM-8020 tries to adjust itself for the best possible video quality.
 Mouse Synchronize Button	Pressing this button to activate the mouse synchronization process. Choose this option in order to synchronize the local with the remote mouse cursor. This is especially necessary when using accelerated mouse settings on the host system. In general, there is no need to change mouse settings on the host.
 Single/Double Mouse	Switches between the Single Mouse Mode (where only the remote mouse pointer is visible) and the Double Mouse Mode

Mode (where remote and local mouse pointers are visible and need to be synchronized). Single mouse mode is only available if using SUN JVM 1.5 or higher.

Options

Click on this button, an Options menu will appear:



A short description of the options follows.

Monitor Only

Toggles the Monitor only filter on or off. If the filter is switched on, no remote console interaction is possible, and monitoring is possible.

Exclusive Access

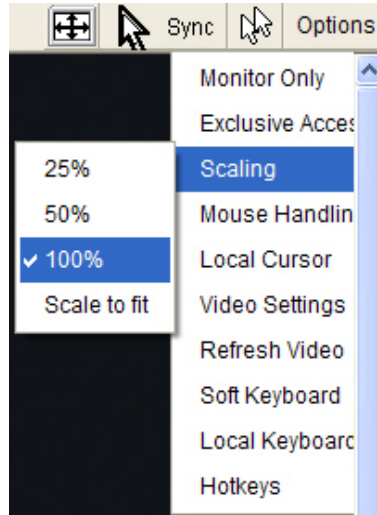
If a user has the appropriate permission, he can force the Remote Consoles of all other users to close. No one can open the Remote Console at the same time again until this user disables the exclusive access, or logs off.

A change in the access mode is also visible in the status line.



Scaling

Allow you to scale down the Remote Console. You can still use both mouse and keyboard; however the scaling algorithm will not preserve all display details.



Mouse Handling

The submenu for mouse handling offers two options for synchronizing the local and the remote mouse pointer.

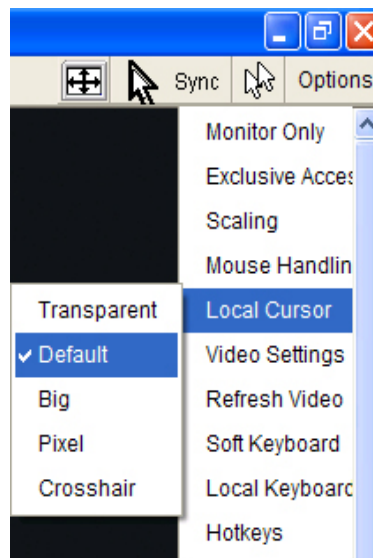
Fast Sync--The fast synchronization is used to correct a temporary, but fixed skew.

Intelligent Sync--Use this option if the fast sync does not work or the mouse settings have been changed on the host system.

This method takes more time than the fast one and requires a correctly adjusted picture. Use the auto adjustment function or the manual correction in the Video Settings panel to setup the picture.

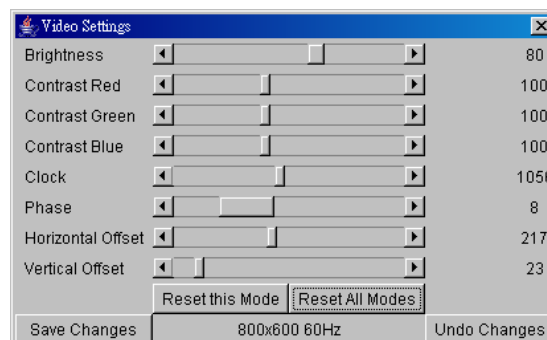
Local Cursor

Offers a list of different cursor shapes to choose from for the local mouse pointer. The selected shape will be saved for the current user and activated the next time this user opens the Remote Console. The number of available shapes depends on the Java Virtual Machine; a version of 1.2 or higher offers the full list.



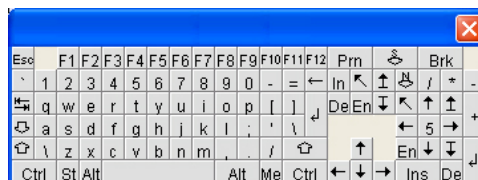
Video Settings

Opens a panel for changing the IKVM-8020 video settings.



Controls	Description
Brightness	Controls the brightness of the picture.
Contrast	Controls the contrast of the picture.
Clock	Defines the horizontal frequency for a video line and depends on the video mode. Different video card types may require different values here. The default settings in conjunction with the auto adjustment procedure should be adequate for all common configurations. If the picture quality is still bad after auto adjustment, you may try to change this setting together with the sampling phase to achieve a better quality.
Phase	Defines the phase for video sampling, used to control the display quality together with the setting for sampling clock.
Horizontal Position	Use the left and right buttons to move the picture in horizontal direction while this option is selected.
Vertical Position	Use the left and right buttons to move the picture in vertical direction while this option is selected.
Reset this Mode	Reset mode specific settings to the factory-made defaults.
Reset all Modes	Reset all settings to the factory-made defaults
Save Changes	Save changes permanently.
Undo Changes	Restore last settings.

Soft Keyboard



Opens up the Menu for the Soft-Keyboards.

Controls	Description
Show	Pops up the Soft-Keyboards. The Soft-Keyboards is necessary in case your host system runs a completely different language and country mapping than your administration machine.
Mapping	Used for choosing the according language and country mapping of the Soft-Keyboards.

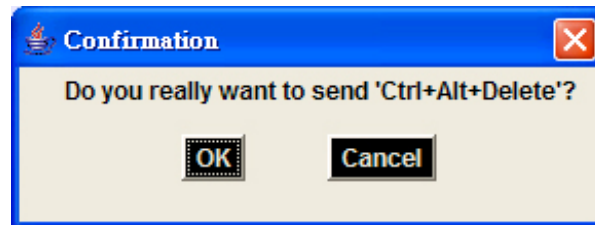
Local Keyboard

Used to change the language mapping of your browser machine running the Remote Console Applet. Normally, the applet determines the correct value automatically. However, depending on your particular JVM and your browser settings this is not always possible. A typical example is a German localized system that uses an US-English keyboard mapping. In this case you have to change the Local Keyboard setting to the right language, manually.

Hotkeys

Opens a list of hotkeys defined previously. Choose one entry, the command will be sent to the host system.

A confirmation dialog can be added that will be displayed before sending the selected command to the remote host. Select “OK” to perform the command on the remote host.

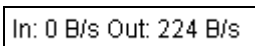


4.3.2 Remote Console Status Line

The Remote Console Status Bar shows both console and the connection state. The size of the remote screen is displayed. The value in brackets describes the connection to the Remote Console. “Norm” means a standard connection without encryption; “SSL” indicates a secure connection.



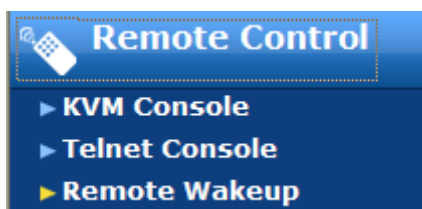
Furthermore, both the incoming (“In:”) and the outgoing (“Out:”) network traffic are visible (in B/s). If compressed encoding is enabled, a value in brackets displays the compressed transfer rate.



Chapter 5 Menu Options

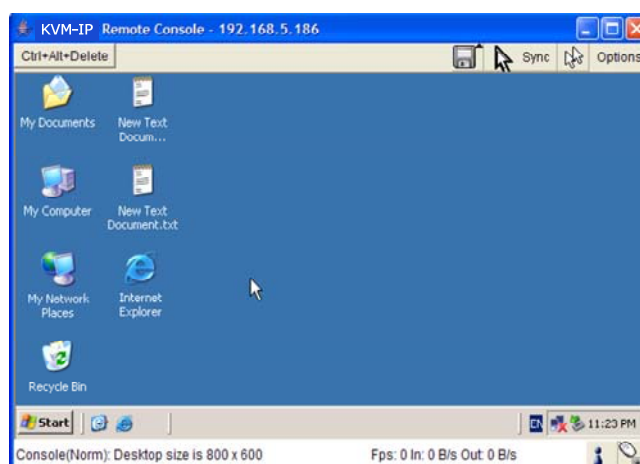
5.1 Remote Control

The Remote Console is the redirected screen, keyboard and mouse of the remote host system that IP-KVM controls. The Remote Console window is a Java Applet that tries to establish its own TCP connection to the IKVM-8020.



Starting the Remote Console opens a new window displays screen movement of host system, with its size automatically adjusted to optimum. Keyboard and mouse are redirected to control the host system simultaneously. A slight delay may present depending on the bandwidth of network.

5.1.1 KVM Console



To open the KVM console either click on the icon **Console** or **Remote Control > KVM Console** of the menu entry on the left or **Click to open** of the console picture on the right.

5.1.2 Telnet/SSH Console

In general, the Telnet or SSH interface supports two operation modes: the **command** line mode and the **terminal** mode. The command line mode is used to control or display some parameters. In terminal mode the pass-through access to serial port is activated (if the serial settings were configured accordingly). All inputs are redirected to the device on serial port and its answers are displayed on the Telnet interface.

In order to log in with Telnet or SSH, you have to enable the access settings from **Device Settings > Network**.

Network Miscellaneous Settings

Remote Console & HTTPS port	<input type="text" value="443"/>	*
HTTP port	<input type="text" value="80"/>	*
TELNET port	<input type="text" value="23"/>	*
SSH port	<input type="text" value="22"/>	*
Bandwidth Limit	<input type="text"/>	kbit/s *

☐ Enable TELNET access *
☐ Enable SSH access *
☐ Disable Setup Protocol *

* Stored value is equal to the default.

5.1.3 Remote Wakeup

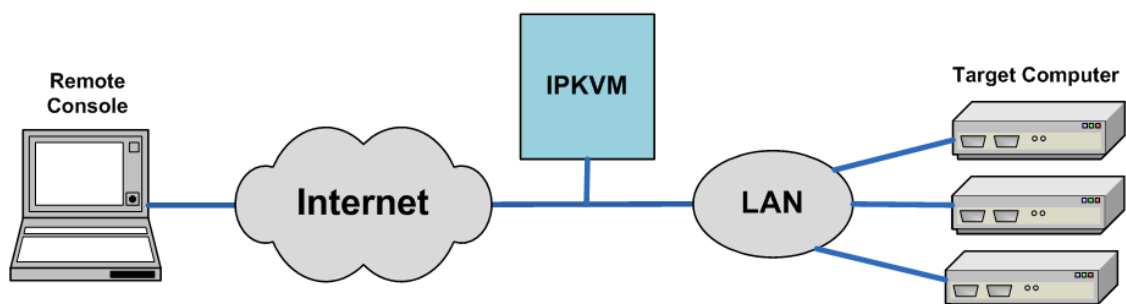
Remote Wakeup Server List

	Wake Up	Server Description	Server IP	Server MAC
Server 1	<input type="checkbox"/>	Example	192.168.123.1	00:00:00:00:00:01

Remote Wakeup Server Settings

	Server Description	Server IP	Server MAC
Server 1	<input type="text" value="Example"/>	<input type="text" value="192.168.123.1"/>	<input type="text" value="00:00:00:00:00:01"/>

The IKVM-8020 provides the remote power wakeup function, which can remotely wake up the sleeping computer. With this feature, the computers that are not in use for now can be shut down and remotely wake up the computer when want to use it, and thus save the power energy.



Settings on target computer:

In order to be waked up, some settings have to be done on the target computer:

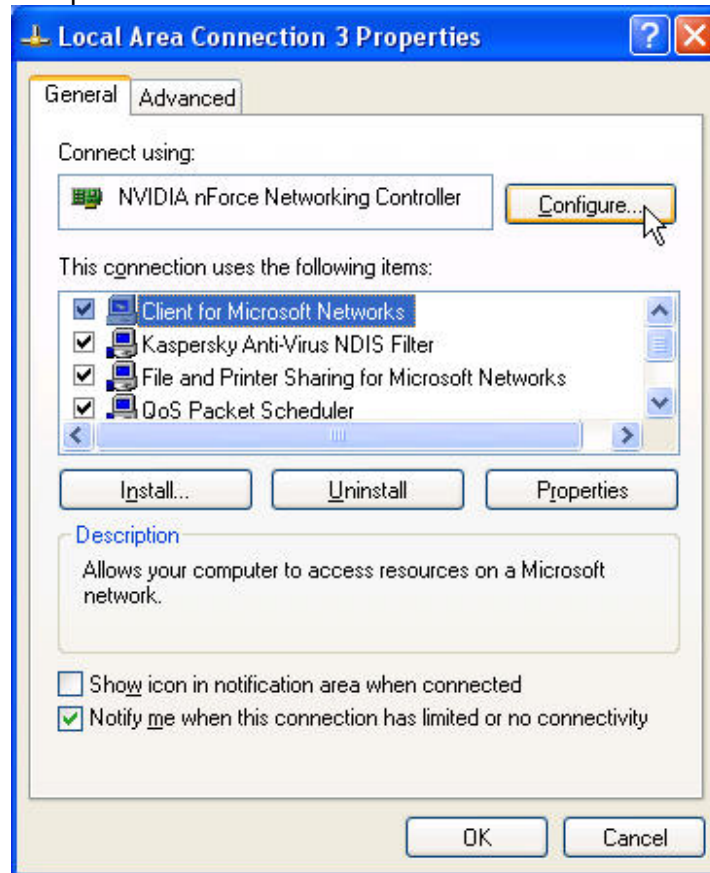
1. BIOS setting:

Have the wake up function in BIOS **Enabled**

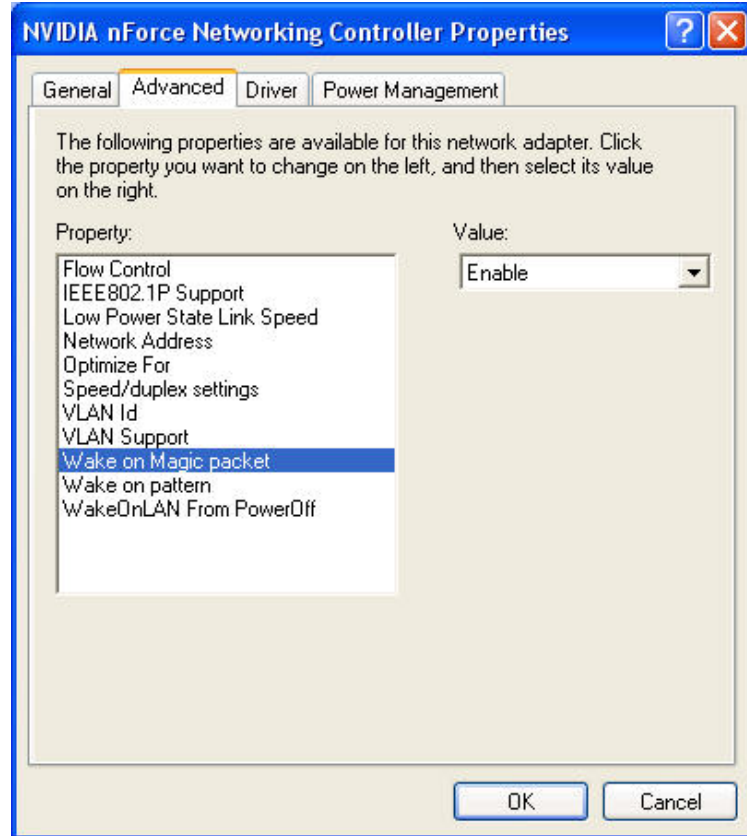
Note: the naming in BIOS varies depending on the BIOS type; it may be **Wake On LAN/PME, PME Event Wake Up, or Power On By PCI Device**.

2. Windows Settings:

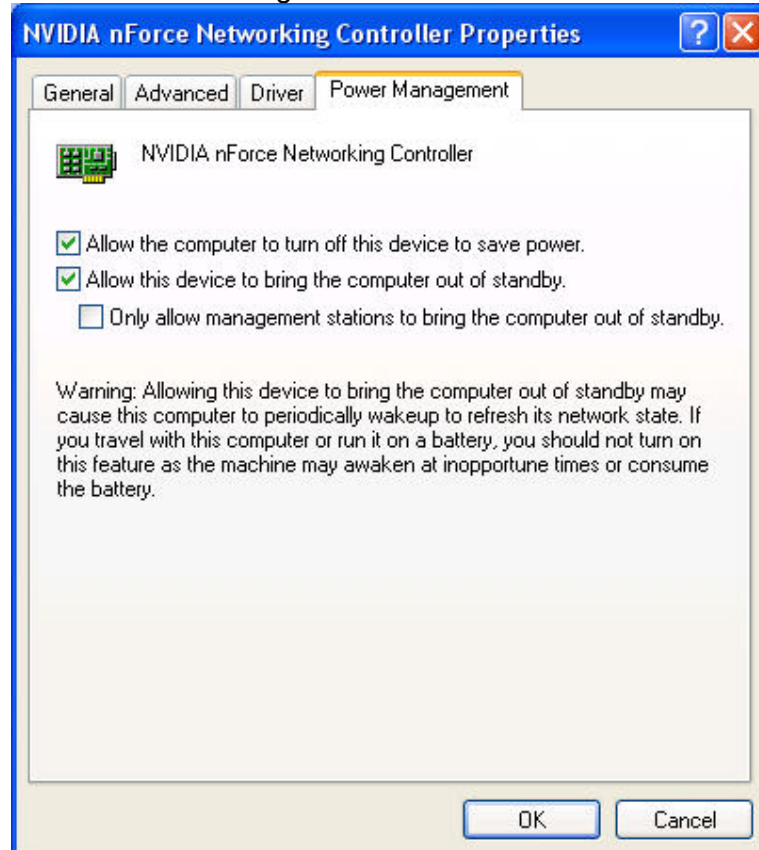
Enter the Properties of Local Area Connection.



Make sure Wake on Magic packet is **Enable**.



Make sure the following two items are selected.



Settings on IP-KVM:

The control can be easily set up from the web page.

1. Click on **Remote Control > Remote Wakeup** to bring up the configuration page.
2. Click on **More entries** to add additional controlled target
3. Key in the server description and the server's IP address
4. Click on **Get MAC** to get the corresponding MAC address of the server
5. Click on **Apply** to save the entry

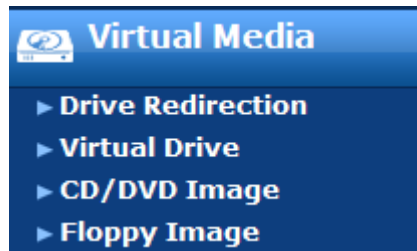
Click on **Reset to defaults** if want to clear all entries

5.2 Virtual Media

The IKVM-8020 provides a powerful capability called Virtual Media (or Virtual Disk). Using the USB port, the IKVM-8020 can present either a local floppy disk image or a redirected remote CD/DVD-ROM image to the target computer.

This can allow system recovery in conditions as bad as having local disks down and no primary network connection. With Floppy Disk Image, the user can upload an image to the IP-KVM's memory, which then emulates a locally attached floppy drive. With CD/DVD-ROM Image, a Windows or other SAMBA share can emulate a locally attached CD/DVD-ROM, for instance to update software.

Drive Redirection allows you to share (redirect) your local drive (floppy drives, hard disks, CD ROMs and other removable devices like USB sticks) with the remote system over a TCP network connection. Thus, with Drive Redirection, you can use a virtual disk drive on the remote computer instead of an image file. It is also possible to enable a remote machine to write data to your local disc.



Before go ahead with this setup, both remote user computer and local computer (the one connected with the IKVM-8020 unit) would have to have Operating System Win2000, XP or above. This function would not work on other platforms at this moment.

Before using Virtual Media, please connect the USB cable from IKVM-8020 to host computer. After connecting the USB cable, you can see a "Removable Disk" on the host computer. Below is the host computer screen (the computer which connected with IKVM-8020).

5.2.1 Drive Redirection

The Drive Redirection is another possibility to use a virtual disc drive on the remote computer. With Drive Redirection you do not have to use an image file but may work with a drive from your local computer on the remote machine. The drive is hereby shared over a TCP network connection. Devices such as floppy drives, hard discs, CD-ROMs and other removable devices like USB sticks can be redirected. It is even possible to enable a write support so that for the remote machine it is possible to write data to your local disc.

Active Image
No disk emulation set.

Drive Redirection
Drive Redirection allows you to share your local drive (floppy, CD/DVD, removable disks and haddisks) with the remote system.

☐ Disable Drive Redirection *
☒ Force read-only connections *

* Stored value is equal to the default.

Please note that Drive Redirection works on a level which is far below the operating system. That means that neither the local nor the remote operating system is aware that the drive is currently redirected, actually. This may lead to inconsistent data as soon as one of the operating systems (either from the local machine, or from the remote host) is writing data on the device. If write support is enabled the remote computer might damage the data and the file system on the redirected device. On the other hand, if the local operating system writes data to the redirected device the drive cache of the operating system of the remote host might contain older data. This may confuse the remote host's operating system. We recommend using the Drive Redirection with care, especially the write support.

Disable Drive Redirection

To disable the function of Drive Redirection.

Force read-only connections

If enabled the Write Support for the Drive Redirection is switched off. It is not possible to write on a redirected device.

Click **Apply** to submit your changes.

5.2.2 Virtual Drive

Virtual Drive Options

☐ Disable USB Mass Storage if no image is loaded *

Apply

Reset to defaults

* Stored value is equal to the default.

Set this option to disable the mass storage emulation (and hide the virtual drive) if not mounting an image file or drive to the host system. To set this option, press the button "Apply".

Note: If unset, and no file image will be found it may happen that the host system will hang on boot due to changes in the boot order, or the boot manager (LILO, GRUB). This case was reported for some Windows versions (2000, XP), other OS might not be fully excluded. This behavior depends on the BIOS version used in that machine.

5.2.3 CD/DVD Image

Use Image on Windows Share (via SAMBA)

To include an image from a Windows share, select "CD/DVD Image" from the submenu.

Active Image

No disk emulation set.

Image on Windows Share

This option allows you to share a CD/DVD image over a Windows Share.
This image will be emulated to the host as USB device.

Share host

Share folder name

Image file name

User (optional)

Password (optional)

Set

40

System Setting	
Share host	The server name or its IP address (the PC that shares out the image file). On Windows 95, 98 and Windows ME do not specify the IP address but the server name ("NetBIOS Name").
Share folder name	The name of the share to be used
Image file name	The image file name on the share folder.
User (optional)	If necessary, specify the user name for the share named before. If unspecified and a guest account is activated, this guest account information will be used as your login.
Password (optional)	If necessary, specify the password for the given user name.

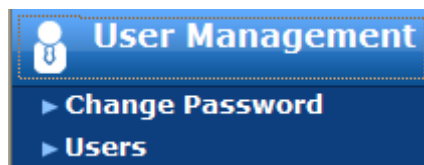
Notes:

1. The output image extension file name has to be 'iso', e.g. CD-Rom_vir.iso.
2. You may create an ISO image size up to 650Mb (for CD-ROM). This drive would be in read-only mode and would not allow you to write any information on this drive but copying only. This drive would be bootable under DOS mode if the motherboard / BIOS on the host computer support USB BOOTABLE function. For emulating DVD Drive, please use **Drive Redirection** function.
3. The above information has to be given from the point of view of IP-KVM with correct IP address and device name. Administrative permission is required as regular user may not have the right to access. Please login as a system administrator (or as "root" on UNIX systems).
4. The specified image file is supposed to be accessible from the IP-KVM. The information above has to be given from the point of view of the IP-KVM. It is important to specify correct IP addresses, and device names. Otherwise, IP-KVM may not be able to access the referenced image file properly; leave the given file unmounted and will display an according error message, instead. So, we recommend to state correct values and repeat this steps if necessary.

Furthermore, the specified share has to be configured correctly. Therefore, administrative permissions are required. As a regular user you may not have these permissions. You should either login as a system administrator (or as "root" on UNIX systems), or ask your system administrator for help to complete this task.

5.3 User Management

On an IP-KVM, each user name has settings and permissions associated with it. Settings affect how the user interfaces with the Remote Console. Permissions allow or forbid the user from performing various actions on the IP-KVM's web pages. A newly assigned user has permissions inherited from an assigned group, if any, or individual permissions if no group is assigned.



5.3.1 Change Password

Change Password

Old Password

New Password

Confirm New Password

- 1) Change password of currently logged in user:
- 2) Old Password: type in current password
- 3) New Password: type in new password
- 4) Confirm New Password: re-type new password for verification
- 5) Click "Apply" to submit your changes.

5.3.2 Users

User Management

Existing users

New user name

Full user name

Password

Confirm Password

Email address

Mobile number

Role

☐ Enforce user to change password on next login *

The IKVM-8020 comes with 1 pre-configured user account that has fixed permissions. The account “super” has all possible rights to configure the device and to use all functions IP-KVM offers.

Upon delivery, the account “super” has the password “pass”. Make sure to change password immediately after you have installed and on initial access of your IP-KVM.

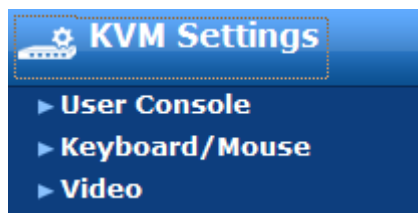
System Setting	
New User name	The new user name for the selected account.
Password	The password for the login name. It must be at least three characters long.
Confirm password	Confirmation of the password above.
Email address	This is optional.
Mobile number	This information may be optionally provided.

Select an existing user for modification. Once a user has been selected, click the lookup button to see the user information.

To create a user presses the button **Create**. The **Modify** button changes the displayed user settings. To delete a user press the button **Delete**.

Note:	The IKVM-8020 is equipped with a host-independent processor and memory unit who both have a limitation in terms of the processing instructions and memory space. To guarantee an acceptable response time we recommend not exceeding the number of 15 users connected to the IP-KVM at the same time. The memory space that is available onto the IP-KVM mainly depends on the configuration and the usage of the IP-KVM (log file entries etc.). That's why we recommend not storing more than 150 user profiles.
--------------	--

5.4 KVM Settings



5.4.1 User Console

The following settings are user specific. That means, the super user can customize these settings for every users separately. Changing the settings for one user does not affect the settings for the other users.

Remote Console Settings for User

The settings on this page are user specific. Changes you make here will affect the selected user only.

super

Transmission Encoding

☒ Automatic Detection *

☐ Pre-configured

Network speed *

☐ Manually

Compression *

Color depth *

Remote Console Type

☐ Default Java VM

☒ Sun Microsystems Java Browser Plugin *

If you do not have the Java Browser Plugin already installed on your system, this option will cause downloading of around 11 MByte Plugin code. The Plugin will enable extended Remote Console functionality.

Miscellaneous Remote Console Settings

☐ Start in Monitor Mode *

☐ Start in Exclusive Access Mode *

Mouse Hotkey

Hotkey
*

Used for fast mouse synchronization (in Double Mouse mode) and to free the grabbed mouse (in Single Mouse mode).

Remote Console Button Keys

	Key Definition	Name
Button Key 1	<input type="text" value="confirm Ctrl+Alt+Delete"/>	<input type="text" value=""/>

* Stored value is equal to the default.

User select box

This selection box displays the user ID for which the values are shown and for which the changes will take effect. You may change the settings of other users if you have the required privileges.

Transmission Encoding

The Transmission Encoding setting allows changing the image-encoding algorithm that is used to transmit the video data to the Remote Console window. It is possible to optimize the speed of the remote screen processing depending on the number of users working at the same time and the network bandwidth of the connection line (Modem, ISDN, DSL, LAN, etc.).

Automatic detection

The encoding and the compression level are determined automatically from the available bandwidth and the current content of the video image.

Pre-configured

The pre-configured settings deliver the best result because of optimized adjustment of compression and color depth for the indicated network speed.

Manually

Allows adjusting both compression rate and the color depth individually. Depending on the selected compression rate the data stream between the IP-KVM and the Remote Console will be compressed in order to save bandwidth. Since high compression rates consume more computing power of IP-KVM, they should not be used while several users are accessing the IP-KVM simultaneously.

The standard color depth is 16 Bit (65536 colors). The other color depths are intended for slower network connections in order to allow a faster transmission of data. Therefore compression level 0 (no compression) uses only 16 Bit color depth. At lower bandwidths only 4 Bit (16 colors) and 2 Bit (4 gray scales) are recommended for typical desktop interfaces. Photo-like pictures have best results with 4 Bit (16 gray scales). 1 Bit color depth (black/white) should only be used for extremely slow network connections.

Remote Console Type

Specifies, which Remote Console Viewer to use.

Default Java-VM

Uses the default Java Virtual Machine of your Browser. This may be the Microsoft JVM for the Internet Explorer, or the Sun JVM if it is configured this way. Use of the Sun JVM may also be forced (see below).

Sun Microsystems Java Browser Plug-in

Instructs the web browser of your administration system to use the JVM of Sun Microsystems. The JVM in the browser is used to run the code for the Remote Console window, which is actually a Java Applet. If you check this box for the first time on your administration system and the appropriate Java plug-in is not already installed on your system, it will be downloaded and installed automatically. However, in order to make the installation possible, you still need to answer the according dialogs with "yes".

The download volume is around 11 Mbytes. The advantage of downloading Sun's JVM lays in providing a stable and identical Java Virtual Machine across different platforms. The Remote Console software is optimized for these JVM versions and offers wider range of functionality when run in SUN's JVM. Please make sure that you are installing Sun JVM v1.5 or above to your client system.

Miscellaneous Remote Console Settings

Start in Monitor Mode

Sets the initial value for the monitor mode. By default the monitor mode is off. In case you switch it on, the Remote Console window will be started in a read only mode.

Start in Exclusive Access Mode

Enables the exclusive access mode immediately at Remote Console startup. This forces the Remote Consoles of all other users to close. No one can open the Remote Console at the same time again until this user disables the exclusive access or logs off.

Mouse hotkey

Allows specifying a hotkey combination which starts either the mouse synchronization process if pressed in the Remote Console, or is used to leave the single mouse mode.

Remote Console Button Keys

Button Keys allow simulating keystrokes on the remote system that cannot be generated locally. The reason for this might be a missing key or the fact, that the local operating system of the Remote Console is unconditionally catching this keystroke already. Typical examples are "Control+Alt+Delete" on Windows and DOS, what is always caught, or "Control+Backspace" on Unix or Unix-like OS for terminating the X-Server. The syntax to define a new Button Key is as follows:

[confirm] <keycode>[+|-[*]<keycode>]* "confirm" requests confirmation by a dialog box before the key strokes will be sent to the remote host.

"keycode" is the key to be sent. Multiple key codes can be concatenated with a plus, or a minus sign. The plus sign builds key combinations, all keys will be pressed until a minus sign or the end of the combination is encountered. In this case all pressed keys should be released in reversed sequence. The minus sign builds single, separate key presses and releases. The star inserts a pause with duration of 100 milliseconds.

5.4.2 Keyboard/Mouse

Keyboard/Mouse Settings

Keyboard Model

Generic 101/104-Key PC ▾ *

Key release timeout

☐ enabled *

Timeout after

25 ▾ msec *

Enable key release timeout if you experience duplicated keystrokes during poor network performance.

Mouse speed

☒ Auto

☐ Fixed scaling : 0.25 ▾ *

☐ Absolute mouse scaling for MAC server

Apply

Reset to defaults

* Stored value is equal to the default.

PS/2 Keyboard Model

Enables a certain keyboard layout. You can choose between “Generic 101-Key PC” for a standard keyboard layout, “Generic 104-Key PC” for a standard keyboard layout extended by three additional windows keys, “Generic 106-Key PC” for a Japanese keyboard, and “Apple Macintosh” for the Apple Macintosh.

Keyboard timeout

Recommended as “enable” for keyboard timeout when host is UNIX or UNIX-like OS.

Mouse Speed

Auto mouse speed

Use this option if the mouse settings on host use an additional acceleration setting. The IP-KVM tries to detect the acceleration and speed of the mouse during the mouse sync process.

Fixed mouse speed

Use a direct translation of mouse movements between the local and the remote pointer. You may also set a fixed scaling which determines the pixel-amount of the remote mouse pointer movement when the local mouse pointer is moved by one pixel. This option is used to manually control the remote mouse speed and only works when the mouse settings on the host are linear. This means mouse acceleration of OS should be disabled, and the intelligent mouse synchronization of IP-KVM is not functioning under this setting.

Absolute mouse scaling for MAC server

Use this option for MAC server. To set the options, click on the button **Apply**.

5.4.3 Video

Miscellaneous Video Settings

Noise filter *

☒ Force Composite Sync (Required for Sun Computers) *

* Stored value is equal to the default.

Miscellaneous Video Settings

Noise filter

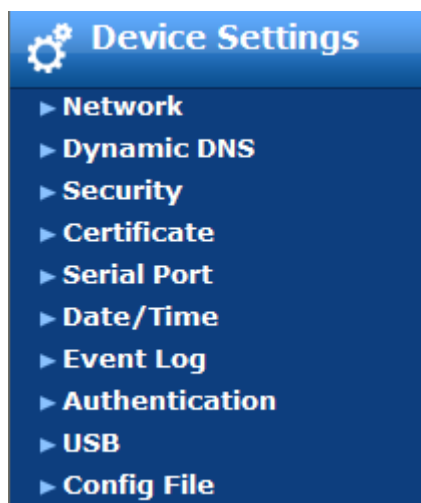
This option defines how the IP-KVM reacts to small changes in the video input signal. Turning on the noise filter can help reduce video flickering that is often caused by distortions, as well as lowering unnecessary bandwidth consumption. A large filter setting needs less network traffic and leads to a faster video display, but small changes in some display regions may not be recognized immediately. A small filter displays all changes instantly but may lead to a constant amount of network traffic even if the display content is not really changing (depending on the quality of the video input signal). All in all the default setting should be suitable for most situations.

Force Composite Sync (Required for Sun Computers)

When connecting the device directly to legacy Sun computer (with composite sync as the video output, it may be possible that IP-KVM don't recognize the composite sync automatically. To support signal transmission from a Sun machine, enable this option. If not enabled the picture of the remote console will not be visible.

To set the options, click on the button **Apply**.

5.5 Device Settings



5.5.1 Network

The Network Settings panel allows changing network related parameters. Each parameter will be explained below. Once applied the new network settings will immediately come into effect.

Network Basic Settings

IP auto configuration	None	*
Preferred host name (DHCP only)		*
IP address	10.1.1.222	
Subnet mask	255.255.255.0	*
Gateway IP address	10.1.1.1	
Primary DNS server IP address		*
Secondary DNS server IP address		*
Server Name	KVM Server	*

Network Miscellaneous Settings

Remote Console & HTTPS port *

HTTP port *

TELNET port *

SSH port *

Bandwidth Limit kbit/s *

☐ Enable TELNET access *

☐ Enable SSH access *

☐ Disable Setup Protocol *

* Stored value is equal to the default.

Note: Changing the network settings of the IP-KVM might result in losing connection to it. In case you change the settings remotely make sure that all the values are correct and you still have an option to access the IP-KVM.

System Setting

IP auto configuration

With this option you can control if the IP-KVM should fetch its network settings from a DHCP or BOOTP server. For DHCP, select "dhcp", and for BOOTP select "bootp" accordingly. If you choose "none" then IP auto configuration is disabled.

Preferred host name

Preferred host name to request from DHCP server. Whether the DHCP server takes the IP-KVM suggestion into account or not depends on the server configuration.

IP address

IP address in the usual dot notation.

Subnet Mask

The net mask of the local network.

Gateway IP address

In case the IP-KVM should be accessible from networks other than the local one, this IP address must be set to the local network router's IP address.

Primary DNS Server IP Address	IP address of the primary Domain Name Server in dot notation. This option may be left empty; however the IP-KVM will not be able to perform name resolution.
Secondary DNS Server IP Address	IP address of the secondary Domain Name Server in dot notation. It will be used in case the Primary DNS Server cannot be contacted.
Remote Console And HTTPS port	Port number at which the IP-KVM's Remote Console server and HTTPS server are listening. If left empty the default value will be used.
HTTP port	Port number at which the IP-KVM's HTTP server is listening. If left empty the default value will be used.
Telnet port	Port number at which the IP-KVM's Telnet server is listening. If left empty the default value will be used.
SSH port	Port number at which the IP-KVM SSH (Secure SHell) server is listening to. If left empty the default value (port 22) will be used.
Bandwidth limitation	The maximum network traffic generated through the IP-KVM Ethernet device. Value in Kbit/s.
Enable Telnet access	This enables the Telnet function.
Enable SSH access	This enables the SSH (Secure SHell) function.
Disable Setup Protocol	Enable this option to exclude the IP-KVM from the setup protocol. Setup protocol is a proprietary layer-2 MAC-based protocol to allow some configuration software to detect IP-KVM devices in the network, even without IP address, and then config network related settings to IP-KVM.

5.5.2 Dynamic DNS

Dynamic DNS Settings

☐ Enable Dynamic DNS *

Dynamic DNS server

DNS System Dynamic

Hostname (eg. yourhost.dyndns.com)

Username

Password

Check time (HH:MM) *

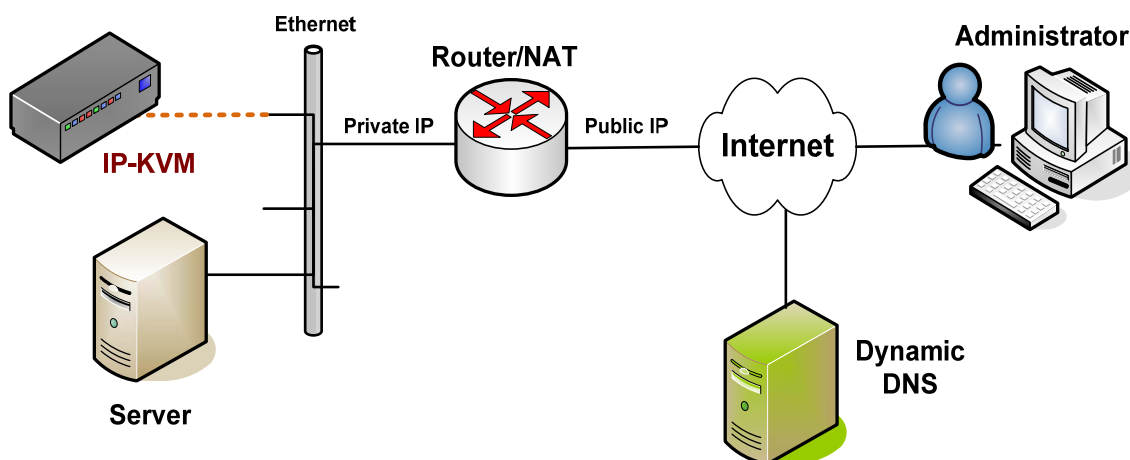
Check interval 24h *

Delete saved external IP Delete

Apply
Reset to defaults

* Stored value is equal to the default.

A freely available Dynamic DNS service (www.dyndns.org) can be used in the following scenario.



The IP-KVM is reachable via the IP address of the DSL router, which is dynamically assigned by the provider. Since the administrator does not know the IP address assigned by the provider, the IP-KVM connects to a special dynamic DNS server in regular intervals and registers its IP address there. The administrator may contact this server as well and pick up the same IP address relating to his IP-KVM unit.

The administrator has to register an IP-KVM that is supposed to take part in the service with the Dynamic DNS Server and assign a certain hostname to it. He will get a nickname and a password in return to the registration process. This account

information together with the hostname is needed in order to determine the IP address of the registered IP-KVM.

You have to perform the following steps in order to enable Dynamic DNS:

- Make sure that the LAN interface of the IP-KVM is properly configured.
- Enter the Dynamic DNS Settings configuration dialog as shown in Figure.
- Enable Dynamic DNS and change the settings according to your needs (see below).

Enable Dynamic DNS

This enables the Dynamic DNS service. This requires a configured DNS server IP address.

Dynamic DNS server

This is the server name where IP-KVM registers itself in regular intervals. Currently, this is a fixed setting since only dyndns.org is supported for now.

DNS System

Choose Dynamic for free DNS service. Custom for your own domain.

Hostname

This is the hostname of the IP-KVM that is provided by the Dynamic DNS Server. (use the whole name including the domain, e.g. testserver.dyndns.org , not just the actual hostname).

Username

You have registered this username during your manual registration with the Dynamic DNS Server. Spaces are not allowed in the Nickname.

Password

You have used this password during your manual registration with the Dynamic DNS Server.

Check time

The IP-KVM registers itself for initiating the IP address of IP-KVM stored in the Dynamic DNS server at this time.

Check interval

This is the interval for reporting again to the Dynamic DNS server for updating the IP address associated with the Domain Name of the IP-KVM.

Note:	The IP-KVM has its own independent real time clock. Make sure the time setting of the IP-KVM is correct. (see the Section Date And Time)
--------------	---

5.5.3 Security

HTTP Encryption
☐ Force HTTPS for Web access *

KVM Encryption
 KVM Encryption ☒ Off * ☐ Try ☐ Force

Group based System Access Control

Please note: 'Apply' is required, or changes will be lost.

☐ Enable Group based System Access Control *

Default Action *

Rule #	Starting IP	Ending IP	Group	Action
1	0.0.0.0	255.255.255.255	All	ACCEPT
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text" value="super"/>	<input type="text" value="ACCEPT"/>

* Stored value is equal to the default.

Force HTTPS

If this option is enabled access to the web front-end is only possible using an HTTPS connection. The IP-KVM will not listen on the HTTP port for incoming connections.

In case you want to create your own SSL certificate that is used to identify the IP-KVM refer to the Section called *Certificate*.

KVM encryption

This option controls the encryption of the RFB protocol. RFB is used by the Remote Console to transmit both the screen data to the administrator machine and keyboard and mouse data back to the host. If set to "Off" no encryption will be used. If set to "Try" the applet tries to make an encrypted connection. In case connection establishment fails for any reason an unencrypted connection will be used.

If set to "Force" the applet tries to make an encrypted connection with certificate. An error will be reported in case connection establishment fails.

Group-based System Access Control

This is the IP filtering function, it keeps unauthorized hosts from accessing to the IP-KVM by specifying IP filtering rules. It is important to fully understand what an IP filter is. If you don't fully understand this, you will get unexpected results against your original plan.

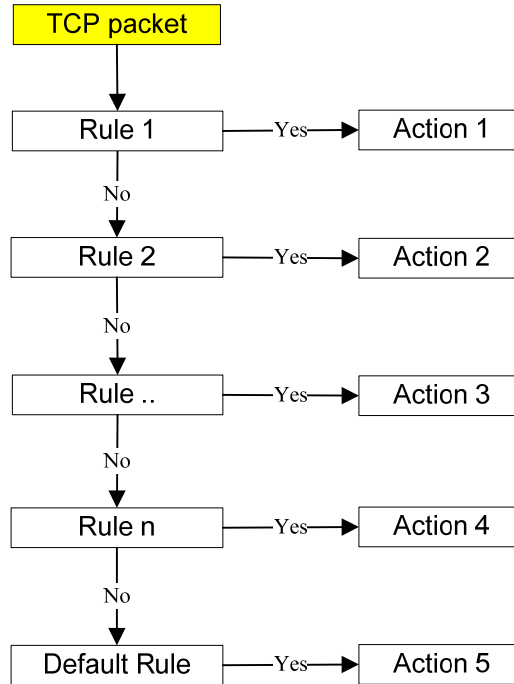
Chain rule

The **Chain rule** determines whether the access from the hosts is allowed or not. It can be one of these two values:

- ACCEPT : access allowed
- DROP : access not allowed

The rule can be configured to apply to a particular Group level (All, User, Super, Administrator).

When the IP-KVM receives a TCP packet, it will process the packet with the chain rule depicted below. The process ordering is important; The packet will enter the chain rule 1 first, if meet the rule then take action directly, otherwise go to chain rule 2.



Check the “Enable Group based System Access Control” to edit the rules

Users can add a new IP filtering rule by setting the properties at adding line by **Append** or **Insert**. User can remove a rule by **Remove** or **Delete**

Group based System Access Control

Please note: 'Apply' is required, or changes will be lost.

☒ Enable Group based System Access Control *

Default Action: ACCEPT *

Rule #	Starting IP	Ending IP	Group	Action
1	0.0.0.0	255.255.255.255	All	ACCEPT
	192.168.123.199	192.168.123.230	super	ACCEPT

Append Insert Replace Delete

Apply Reset to defaults

* Stored value is equal to the default.

5.5.4 Certificate

Certificate Signing Request (CSR)

Common name

Organizational unit

Organization

Locality/City

State/Province

Country (ISO code)

Email

Challenge password

Confirm Challenge password

Key length (bits)

1024

*

Create

* Stored value is equal to the default.

The IP-KVM uses the Secure Socket Layer (SSL) protocol for any encrypted network traffic between itself and a connected client. During the connection establishment the IP-KVM has to expose its identity to a client using a cryptographic certificate.

The default certificate comes with IP-KVM device upon delivery is for testing purpose only. System administrator should not rely on this default certificate as the secured global access mechanism through Internet.

However, it is possible to generate and install a new base64 X.509 certificate that is unique for a particular IP-KVM. In order to do that, the IP-KVM is able to generate a new cryptographic key and the associated Certificate Signing Request (CSR) that needs to be certified by a certification authority (CA). A certification authority verifies that you are the person who you claim you are, and signs and issues a SSL certificate to you.

5.5.5 Serial Port

Serial Port Settings

☒ Configuration login *
☐ Modem

Serial line speed bits/s *
 Modem init string *
 Modem server IP address *
 Modem client IP address *

☐ Passthrough access to serial port 1 via Telnet/SSH

Speed	Data bits	Parity	Stop Bits	Handshake
<input type="text" value="115200"/>	<input type="text" value="8"/>	<input type="text" value="none"/>	<input type="text" value="1"/>	<input type="text" value="None"/>

Serial Port Log

Key Word 1

The IP-KVM Serial Settings allows you to specify what device is connected to the serial port and how to use it.

5.5.6 Date / Time

Date/Time Settings

UTC Offset *

☒ User specified time *
 Date / / (mm/dd/yyyy)
 Time : : (hh:mm:ss)

☐ Synchronize with NTP Server

Primary Time server *
 Secondary Time server *

* Stored value is equal to the default.

This link refers to a page, where the internal real-time clock of the IP-KVM can be set up. You have the possibility to adjust the clock manually, or to use a NTP timeserver.

Without a timeserver, your time setting will not be persistent, so you have to adjust it again, after IP-KVM loses power for more than a few minutes.

To avoid this, you can use a NTP timeserver, which sets up the internal clock automatically to the current UTC time. Because NTP server time is always UTC, there is a setting that allows you to set up a static offset to get your local time.

Note:	There is currently no way to adjust the daylight saving time automatically. So you have to set up the UTC offset twice a year properly to the local rules of your country.
--------------	--

5.5.7 Event Log

Event Log Targets

☒ List Logging Enabled *

Entries shown per page *

Clear internal log

☒ NFS Logging Enabled *

NFS Server *

NFS Share *

NFS Log File *

☐ SMTP Logging Enabled *

SMTP Server *

Receiver Email Address *

Sender Email Address *

☐ SNMP Logging Enabled *

Destination IP *

☐ SNMP Logging Enabled *

Destination IP *

Community *

Event Log Assignments

Event	List	NFS
Board Message	<input checked="" type="checkbox"/> *	<input checked="" type="checkbox"/> *
Security	<input checked="" type="checkbox"/> *	<input checked="" type="checkbox"/> *
Remote Console	<input checked="" type="checkbox"/> *	<input checked="" type="checkbox"/> *
Host Control	<input checked="" type="checkbox"/> *	<input checked="" type="checkbox"/> *
Authentication	<input checked="" type="checkbox"/> *	<input checked="" type="checkbox"/> *
Serial Port	<input checked="" type="checkbox"/> *	<input checked="" type="checkbox"/> *

* Stored value is equal to the default.

Important events like a login failure or a firmware update are logged to a selection of logging destinations. Each of those events belongs to an event group, which can be activated separately.

The common way to log events is to use the internal log list of the IP-KVM. To show the log list, click on "Event Log" on the "Maintenance" page. In the Event Log Settings you can choose how many log entries are shown on each page. Furthermore, you can clear the log file here.

5.5.8 Authentication

Authentication Settings

☒ Local Authentication *

☐ LDAP

User LDAP Server

*

Base DN of User LDAP Server

*

Type of external LDAP Server

*

Name of login-name attribute

*

Name of user-entry objectclass

*

User search subfilter

*

Active Directory Domain

*

☐ RADIUS

	Server	Shared Secret	Auth. Port	Acc. Port	Timeout	Retries
1.	<input type="text"/>	<input type="text"/>	<input type="text" value="1812"/>	<input type="text" value="1813"/>	<input type="text" value="1"/>	<input type="text" value="3"/>
<input type="button" value="More Entries"/>						

On this screen you can specify where the IP-KVM will look in order to authenticate the users. You can use "Local Authentication"; this means you need to have created the user account on the IP-KVM and the user/group information residing on the IP-KVM for authentication.

The other options allow you to specify an LDAP or a RADIUS Server to use for the login authentication. These methods are very useful when you want to map users into specific groups which have certain privileges. It is usually far easier and simpler to refer to already existing groups, rather than having to re-enter everything into the IP-KVM.

Note: Whatever you configure, you can always login over the network as the superuser "super". The superuser is always authenticated and authorized locally, so you always have a "back door" to the IP-KVM.

5.5.9 USB

USB Device Settings

☐ Force using USB 1.1 *

USB 2.0 is the default setting, if the operating system of the managed computer does not support USB 2.0, please force it to USB 1.1.

Apply Reset to defaults

* Stored value is equal to the default.

USB 2.0 is the default setting, if the operating system of the managed computer does not support USB 2.0, please force it to USB 1.1.

5.5.10 Config File

Device Configuration

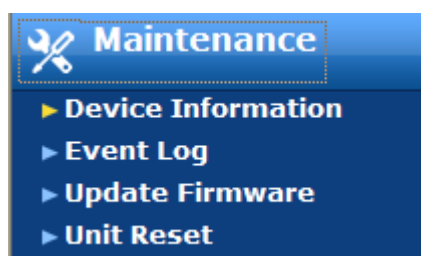
Configuration Restore 瀏覽... Restore

Configuration Backup Backup

With this function, the configuration settings can be saved (Backup) in a file (config.gz), or reloaded (Restore) from a previously saved configuration file.

5.6 Maintenance

The administrator performs various maintenance activities on the IP-KVM. These include viewing its status, update firmware, view the event log and reset the unit



5.6.1 Device Information

The Device Status page contains a table with information about the IP-KVM's hardware and firmware. This information is useful if technical support is required.

Device Information	
Product Name:	IP-KVM
Server Name:	KVM Server
Serial Number:	08051111150053
Board ID:	0a33a201e84968fb
Device IP Address:	10.1.1.222
Device MAC Address:	00:30:4F:00:49:08
Firmware Version:	04.30.06
Firmware Build Number:	49097
Firmware Description:	2011-12-07 22:53 IPKM03STD
Hardware Revision:	0x15
<hr/>	
Connected Users	
	super (10.1.1.169) active

The Data file for support allows you to download the IP-KVM data file with specific support information. This is an XML file with certain customized support information like the serial number etc. You may send us this information together with a support request. It will help us to locate and solve your reported problem.

5.6.2 Even log

The figure below displays the log list including the events that are logged by the IP-KVM

Event Log [Prev] []

Date	Event	Description
01/06/2000 01:27:09	Authentication	User 'super' logged in from IP address 10.1.1.169
01/05/2000 23:43:45	Authentication	User 'super' logged in from IP address 10.1.1.169
01/05/2000 22:34:16	Authentication	User 'super' logged in from IP address 10.1.1.169
01/05/2000 07:07:40	Authentication	User 'super' logged in from IP address 10.1.1.169
01/05/2000 03:44:19	Authentication	User 'super' logged in from IP address 10.1.1.169
01/05/2000 03:23:37	Authentication	User 'super' logged in from IP address 10.1.1.169
01/04/2000 06:34:28	Authentication	User 'super' logged in from IP address 10.1.1.169
01/04/2000 06:08:00	Authentication	User 'super' logged in from IP address 10.1.1.169
01/04/2000 05:30:50	Authentication	User 'super' logged in from IP address 10.1.1.169
01/04/2000 05:02:48	Remote Console	Connection to client 10.1.1.169 closed.
01/04/2000 05:02:48	Remote Console	Connection to client 10.1.1.169 established.
01/04/2000 05:00:31	Remote Console	Connection to client 10.1.1.169 closed.
01/04/2000 05:00:20	Remote Console	Connection to client 10.1.1.169 established.
01/04/2000 04:59:55	Remote Console	Connection to client 10.1.1.169 closed.
01/04/2000 04:55:50	Remote Console	Connection to client 10.1.1.169 established.
01/04/2000 04:55:10	Authentication	User 'super' logged in from IP address 10.1.1.169

5.6.3 Unit Reset

This section allows you to reset specific parts of the device. This involves resetting keyboard/mouse, USB, video engine, or the IP-KVM device itself. In general, the IP-KVM requires a reset when implementing a firmware update. In the event of an abnormal operation, a number of subsystems may be reset without resetting the entire IP-KVM.

Click **Maintenance > Unit Reset**, the following window displays.

Reset Keyboard/Mouse (PS/2)	<input type="button" value="Reset"/>
Reset USB	<input type="button" value="Reset"/>
Reset Video Engine	<input type="button" value="Reset"/>
Reset Device	<input type="button" value="Reset"/> This may take up to a minute.

To reset a certain IP-KVM functionality click on the **Reset** button as displayed in figure below.

Clicking on **Reset** of **Reset Device** will reboot the IP-KVM system. It will close all current connections to the administration console and to the Remote Console. The whole process will take about one minute. Resetting “subdevices” (e.g. video engine) will take few seconds only and does not result in closing connections.

Note: Only the **super** user is allowed to reset the IP-KVM.

Appendix A Cable Connectors Specifications

Cable Connectors

1. 3-in-1 VGA Cable

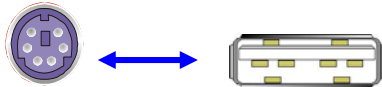
HDDDB15 male to one HDDDB15 male plus two minis din 6-pin PS/2 connectors.



3-in-1 VGA Cable Connectors

2. PS/2 keyboard to USB Changer

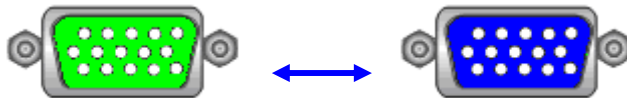
PS/2 (keyboard) to USB (keyboard and mouse) changer.



PS/2 keyboard to USB Changer

3. Daisy Chain Cable

VGA Cable: HDDDB15 Male to Male



Daisy Chain Cable

Note:	Daisy chain needs the cable 15 lines fully connected. This is a special VGA cable, normal VGA cable have unconnected lines. Please contact your dealer for Daisy chain cable.
--------------	---

Appendix B Troubleshooting & Frequently Asked Questions

Q:	The remote mouse doesn't work or is not synchronous
A:	Make sure the mouse settings in IKVM-8020 match the mouse model. There are some circumstances where the mouse synchronization process could behave incorrectly, refer to Section 3.4.3 for further explanation.
Q:	The video quality is bad or the picture is grainy
A:	Try to correct the brightness and contrast settings (see section 4.3.1) until they are out of a range where the picture looks grainy. Use the auto adjustment feature to correct a flickering video.
Q:	Login on IKVM-8020 fails.
A:	Was the correct combination of user and password given? On delivery, the user "super" has the password "pass". Moreover your browser must be configured to accept cookies.
Q:	The Remote Console window can't connect to IKVM-8020.
A:	Possibly a firewall prevents access to the Remote Console. Make sure the TCP port numbers 443 or 80 are open for incoming TCP connection establishments.
Q:	No connection can be established to IKVM-8020.
A:	Check whether the network connection is working in general (ping the IP address of IKVM-8020). If not, check network hardware. Is IKVM-8020 powered on? Check whether the IP address of IKVM-8020 and all other IP related settings are correct! Also verify that all the IP infrastructure of your LAN, like routers etc., is correctly configured. Without a ping functioning, IKVM-8020 can't work either.
Q:	Special key combinations, e.g. ALT+F2, ALT+F3 are intercepted by the console system and not transmitted to the host.
A:	You have to define a so-called 'Button Key'. This can be done in the Remote Console settings.
Q:	In the browser the IKVM-8020 pages are inconsistent or chaotic.
A:	Make sure your browser cache settings are feasible. Especially make sure the cache settings are not set to something like "never check for newer pages". Otherwise IKVM-8020 pages may be loaded from your browser cache and not from the card.
Q:	Windows XP doesn't awake from standby mode

A:	This is possibly a Windows XP problem. Try not to move the mouse while XP goes in standby mode.																												
Q:	Can't upload the signed certificate in MacOS X																												
A:	If an 'internal error' occurs while uploading the signed certificate, either change the extension of the file to .txt or add a file helper using the Internet Explorer preferences for this type of file. Make sure that the encoding is plain text and the checkbox 'use for outgoing' is checked. Another possibility is to use a Mozilla based browser.																												
Q:	Every time I open a dialog box with some buttons the mouse pointers are not synchronous anymore																												
A:	Please check, if you have an option like "Automatically move mouse pointer to the default button of dialog boxes" enabled in the mouse settings of the operating system. This option needs to be disabled.																												
Q:	What resolution support in remote side.																												
A:	<p>Please check below lists the user role permissions granted for three user role groups (<i>Super, Administrator and User</i>).</p> <table border="1"> <thead> <tr> <th>Resolution (x, y)</th><th>Refresh Rates (Hz)</th></tr> </thead> <tbody> <tr><td>640 x 350</td><td>70, 85</td></tr> <tr><td>640 x 400</td><td>56, 70, 85</td></tr> <tr><td>640 x 480</td><td>60, 72, 75, 85, 90, 100, 120</td></tr> <tr><td>720 x 400</td><td>70, 85</td></tr> <tr><td>800 x 600</td><td>56, 60, 70, 72, 75, 85, 90, 100</td></tr> <tr><td>832 x 624</td><td>75</td></tr> <tr><td>1024 x 768</td><td>60, 70, 72, 75, 85, 90, 100</td></tr> <tr><td>1152 x 864</td><td>75</td></tr> <tr><td>1152 x 870</td><td>75</td></tr> <tr><td>1152 x 900</td><td>66</td></tr> <tr><td>1280 x 960</td><td>60</td></tr> <tr><td>1280 x 1024</td><td>60, 75</td></tr> <tr><td>1600 x 1200</td><td>60</td></tr> </tbody> </table>	Resolution (x, y)	Refresh Rates (Hz)	640 x 350	70, 85	640 x 400	56, 70, 85	640 x 480	60, 72, 75, 85, 90, 100, 120	720 x 400	70, 85	800 x 600	56, 60, 70, 72, 75, 85, 90, 100	832 x 624	75	1024 x 768	60, 70, 72, 75, 85, 90, 100	1152 x 864	75	1152 x 870	75	1152 x 900	66	1280 x 960	60	1280 x 1024	60, 75	1600 x 1200	60
Resolution (x, y)	Refresh Rates (Hz)																												
640 x 350	70, 85																												
640 x 400	56, 70, 85																												
640 x 480	60, 72, 75, 85, 90, 100, 120																												
720 x 400	70, 85																												
800 x 600	56, 60, 70, 72, 75, 85, 90, 100																												
832 x 624	75																												
1024 x 768	60, 70, 72, 75, 85, 90, 100																												
1152 x 864	75																												
1152 x 870	75																												
1152 x 900	66																												
1280 x 960	60																												
1280 x 1024	60, 75																												
1600 x 1200	60																												