

USER MANUAL

IP-KVM 1001
KVM over IP Switch

User Manual

Rev: 1.0

April 30th, 2009

Copyright & Disclaimers

©Opengear Inc. 2009. All Rights Reserved.

Information in this document is subject to change without notice and does not represent a commitment on the part of Opengear. Opengear provides this document “as is,” without warranty of any kind, expressed or implied, including, but not limited to, the implied warranties of fitness or merchantability for a particular purpose.

Opengear may make improvements and/or changes in this manual or in the product(s) and/or the program(s) described in this manual at any time. This product might include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes may be incorporated in new editions of the publication.

For Warranty & Support information please refer Appendix G

Notice to Users

Proper back-up systems and necessary safety devices should be utilized to protect against injury, death or property damage due to system failure. Such protection is the responsibility of the user.

This device is not approved for use as a life-support or medical system.

Any changes or modifications made to this device without the explicit approval or consent of Opengear will void Opengear of any liability or responsibility of injury or loss caused by any malfunction.

This equipment is for indoor use and all the communication wirings are limited to inside of the building.

Manual Conventions

This manual uses different fonts and typefaces to show specific actions:

Note Text presented like this indicates issues to take note of



Text presented like this highlights important issues and it is essential you read and take heed of these warnings

- Text presented with an arrow head indent indicates an action you should take as part of the procedure

Publishing history

Date	Revision	Update details
April 2009	1.0	Initial release document

INDEX

1.	Product Overview	6
1.1	Introduction	6
1.2	Main features	6
2.	Installation and Start Up	8
2.1	Package checklist	8
2.2	Product Views	8
2.3	LED indicators and Reset button	10
2.4	System requirements	10
2.5	Hardware installation	11
2.6	Cabling the connection to stand-alone computers	11
2.6.1	Stand alone PS/2	12
2.6.2	Stand alone USB	14
2.6.3	Cascaded connection	16
2.7	Cabling the connection to a multi-port KVM switch	17
2.8	When the server is up and running	19
2.9	When the server is dead	19
3.	Configuration	20
3.1	Initial IP configuration using <i>psetup</i>	20
3.1.1	Reset the Super User password	20
3.1.2	Set up a fixed IP	21
3.1.3	Enable DHCP	21
3.2	Initial IP configuration using a web browser	23
3.3	Initial IP configuration using the serial console	24
3.4	Keyboard, mouse and video configuration	25
3.4.1	IP-KVM keyboard settings	25
3.4.2	Remote Mouse Settings	25
3.4.3	Automatic mouse speed and mouse synchronization	26
3.4.4	Host system mouse settings	26
3.4.5	Single and Double Mouse Mode	27
3.4.6	Recommended Mouse Settings	27
3.4.7	Video Modes	27
4.	Usage	28
4.1	Prerequisites	28
4.1.1	Browser	28
4.2	Logging in and out	29
4.2.1	Log in to the IP-KVM	29
4.2.2	Log out from the IP-KVM	31
4.3	The Remote Console	32
4.3.1	Main Window of Remote Console	32
4.3.2	Control Bar of Remote Console	33
4.3.3	Status Line of Remote Console	43
5.	Menu Options	44
5.1	Remote Control	44
5.1.1	KVM Console	45
5.1.2	Telnet/SSH Console	45
5.2	Virtual Media	48
5.2.1	Drive Redirection	49
5.2.2	Virtual Drive	50
5.2.3	CD/DVD Image	51
5.2.4	Floppy Disk	56
5.2.5	Creating an Image	58
5.2.5.1	Creating a Floppy Image	58
5.2.5.2	Creating a CD/DVD ISO Image	59

5.2.6	Making a Drive Redirection.....	60
5.3	User Management.....	64
5.3.1	Change Password.....	64
5.3.2	Users and Groups.....	65
5.4	KVM Settings.....	66
5.4.1	User Console.....	66
5.4.2	Keyboard/Mouse.....	70
5.4.3	Video.....	71
5.5	Device Settings.....	72
5.5.1	Network.....	72
5.5.2	Dynamic DNS.....	75
5.5.3	Security.....	77
5.5.4	Certificate.....	79
5.5.5	Serial Port.....	82
5.5.6	Date / Time.....	84
5.5.7	Event Log.....	86
5.5.8	Authentication.....	88
5.5.9	USB.....	91
5.5.10	Config File.....	91
5.5.11	Authentication.....	92
5.6	Maintenance.....	94
5.6.1	Device Information.....	94
5.6.2	Event log.....	95
5.6.3	Update Firmware.....	96
5.6.4	Unit Reset.....	98
5.6.5	Reset to Factory Defaults.....	99
6.	Addendum.....	102
A.	Key Codes.....	102
B.	Video Modes.....	103
C.	User Role Permissions.....	103
D.	Bandwidth Consumption.....	104
E.	Pin-outs of RJ45-DB9F Cable.....	104
F.	TCP/UDP Port Numbers.....	105
G.	Protocol Glossary.....	105
H.	Regulation Information.....	106
I.	Service and warranty.....	107

Figures

Figure 2-1	Product View	9
Figure 2-2	Panel View	10
Figure 2-3	3-in-1 Integrated Adapting Local Cable	10
Figure 2-4	Serial Cable.....	10
Figure 2-5	Cable Connections (stand-alone, PS/2)	13
Figure 2-6	Cable Connections (stand-alone, USB)	15
Figure 2-7	Cable Connections (stand-alone, PS/2)	16
Figure 2-8	Cable Connections (with a Multi-port KVM Switch).....	18
Figure 4-1	The Internet Explorer displaying the encryption key length	29
Figure 4-2	Remote Console Control Bar.....	33
Figure 4-3	Remote Console Options Menu	34
Figure 4-4	Remote Console Exclusive Mode	35
Figure 4-5	Remote Console Options Menu:Scaling	36
Figure 4-6	Remote Console Options Menu:Cursor.....	37
Figure 4-7	Video Settings Panel	38
Figure 4-8	Soft Keyboard.....	39
Figure 4-9	Soft Keyboard Mapping	39
Figure 4-10	Remote Console Confirmation Dialog	40
Figure 4-11	Encoding Compression	41
Figure 4-12	Predefined Compression.....	42
Figure 4-13	Lossy Compression	42
Figure 4-14	Encoding Color depth	43
Figure 4-15	Status line.....	43
Figure 4-16	Status line transfer rate	43
Figure 5-1	KVM Console	45
Figure 5-2	Telnet Console	47
Figure 5-3	Options of Drive Redirection.....	50
Figure 5-4	USB mass storage option	51
Figure 5-5	Virtual Media - CD-ROM Image.....	51
Figure 5-6	Explorer Context Menu.....	53
Figure 5-7	Share Configuration Dialog	54
Figure 5-8	Virtual Media - Floppy Disk.....	56
Figure 5-9	RawWrite for Windows selection dialog	58
Figure 5-10	Nero selection dialog.....	59
Figure 5-11	Built-in Java Drive Redirection	60
Figure 5-12	Setting Password	64
Figure 5-13	User Console Setting.....	68
Figure 5-14	Keyboard and Mouse Settings	70
Figure 5-15	Video Settings.....	71
Figure 5-16	Network Settings	73
Figure 5-17	Dynamic DNS.....	75
Figure 5-18	Dynamic DNS Scenario.....	76
Figure 5-19	Device Security	77
Figure 5-20	Chain Rules of IP Filtering	78
Figure 5-21	IP Filter Settings.....	79
Figure 5-22	Certificate Settings	80
Figure 5-23	SSL Certificate Upload.....	82
Figure 5-24	CSR string	82
Figure 5-25	Serial Port.....	83
Figure 5-26	Date / Time.....	85
Figure 5-27	Event Log.....	86
Figure 5-28	Device Information	94
Figure 5-29	Connected Users.....	95
Figure 5-30	Event Log List.....	95
Figure 5-31	Update Firmware.....	96
Figure 5-32	Unit Reset.....	99

1. Product Overview

1.1 Introduction

Opengear's KVM-over-IP switch (referred to generically in this manual as the **IP-KVM**) redirects local keyboard, mouse and video data to a remote administration console. It allows you to control one or many computers locally at the server site or remotely via the Internet using a standard browser. You can securely gain BIOS level access to systems for maintenance, support, or failure recovery over the Internet. Communication is secured via SSL authentication and encryption. The IP-KVM can also be used in conjunction with a KVM switch for multiple-server access.

The IP-KVM provides convenient remote KVM access and control via LAN or Internet. It captures, digitizes and compresses video signal and transmits it with keyboard and mouse signals to and from a remote computer. IP-KVM provides a non-intrusive solution for remote access and control. Remote access and control software runs on its embedded processor only but not on mission-critical servers, so that there is no interference with server operation or impact on network performance.

1.2 Main features

- Manage servers around the world
- Remote KVM (keyboard, video, and mouse) access over IP network or over a modem link
- Local console port for direct analogous access to KVM switch
- Combo (PS2 + USB) Local Console interfaces
- Dual LAN port for Remote Console and easy cascaded wiring
- Dual USB port for Local Console
- Full control under any OS at BIOS level, during boot, or at Blue Screens
- No additional software necessary on client console side
- Remote mass storage control and redirection
- Remote control over Java-enabled browsers
- SSL Secure access through certificate authentication and data encryption
- SSL 256-bit encryption of all transmitted data
- RSA 2048-bit encryption
- Auto-optimize the frame rate and video quality according to the bandwidth availability
- Automatically senses video resolution for best possible screen capture
- High-performance mouse tracking and synchronization
- Interwork with most of KVM switches

- Firmware update via web interface
- Rack mountable

Feature	Description
Target Server Side	1x Attached 3-in-1 integrated cable and K/V/M connectors (HDDDB15 male plus two mini din 6-pin PS/2 connectors)
	1x USB 2.0 mini receptacle
	1x RJ-45 Serial Port
Local Console Side	1x 3-in-1 VGA connector (HDDDB15 female)
	2x USB type-A connectors
Remote Console Side	2x Standard RJ-45 Connectors (LAN ports)
LED Indicators	2x LEDs: Power (red), Ready (green)
Push Button	1x Reset push button
Video Resolution	up to 2048 x 1536 @60Hz (Local Console)
	up to 1600 x 1200 @60Hz (Remote Console)
Protocols	TCP, IP, ARP, ICMP, HTTP/HTTPS, SSL, Telnet, DHCP, PPP, SMTP, NTP, DDNS
Security	AES 256-bit encryption for all transmitted data
	RSA 2048-bit encryption for authentication
	SSHv2
Authentication	SSL / Certificate, RADIUS, LDAP
Virtual Media	Floppy/CD/DVD/USB/HD drive redirection
	Floppy/CD/DVD/ISO Image redirection
DC Power	12VDC, 1A
Operation Temperature	0 ~ 50 °C (32 ~ 122 °F)
Humidity	0~80% RH
Housing	Metal
Dimension (mm)	103 x 87 x 28.5
Weight	1000g

2. Installation and Start Up

Introduction

This chapter overviews the general installation and configuration of your IP-KVM and steps through in detail the physical installation and connection to controlled devices

2.1 General installation and configuration steps

- Step 1 Check kit contents (refer *Chapter 2.2*)
- Step 2 IP-KVM installation and connection to the target server and network (refer *Chapter 2.5 - 2.7*)
- Step 3 Configure the IP-KVM network settings (refer *Chapter 3.1 - 3.3*)
- Step 4 Configuring the KVM settings for the Target Server and IP-KVM (refer *Chapter 3.4*)

2.2 Package checklist

The IP-KVM package consists of the followings items:

- ✓ The IP-KVM unit
- ✓ CD-ROM (software utilities and user manual)
- ✓ Quick Start Guide
- ✓ DC power supply adapter
- ✓ 3-in-1 Integrated Adapting Local Cable
- ✓ USB A-mini cable
- ✓ Serial cable (RJ45 to DB9F)
- ✓ Rack mounting kit (with brackets and screws)
- ✓ Footpads set

2.3 Product Views

The IP-KVM has an attached 3-in-1 Integrated Host Cable to simplify cable connection. Similarly the dual LAN ports provides flexibility of cascaded wiring and the palm size form factor enables flexible installation.



Figure 2-1 Product View

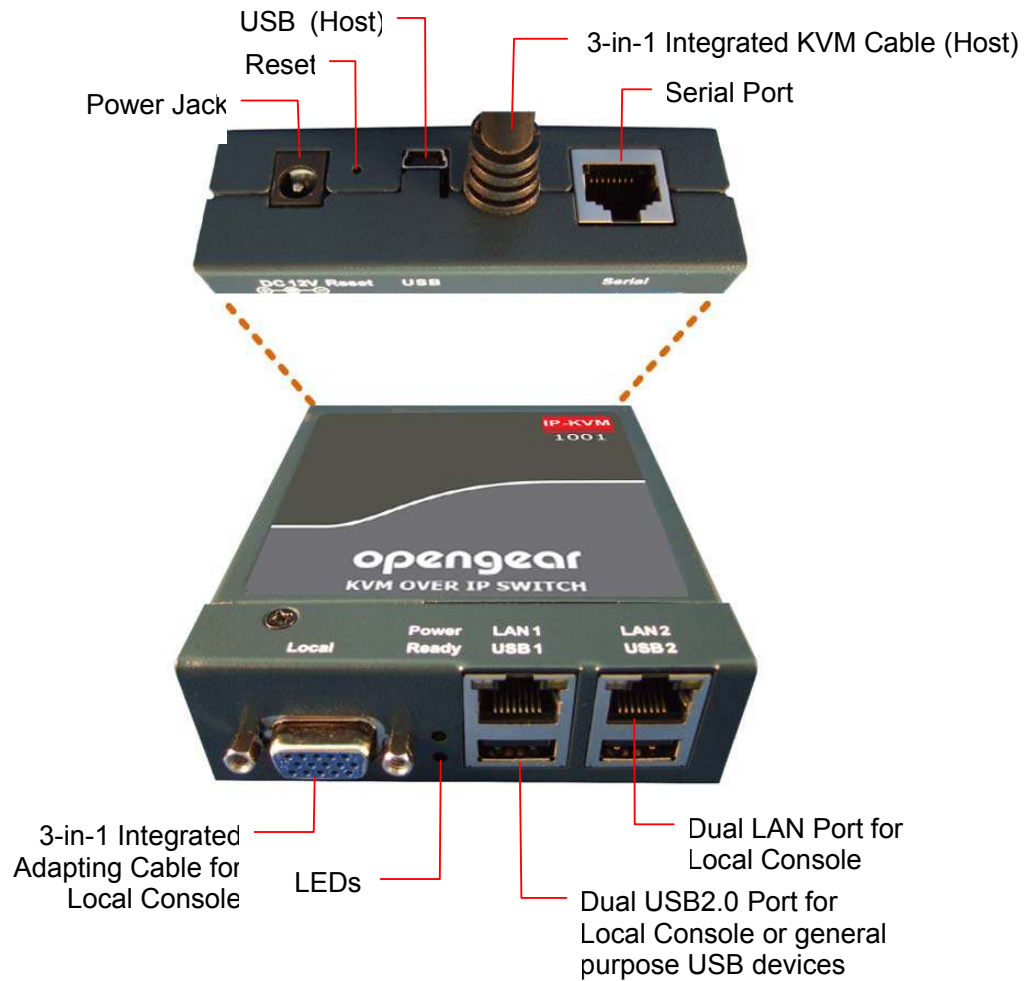


Figure 2-2 Panel View



Figure 2-3 3-in-1 Integrated Adapting Local Cable



Figure 2-4 Serial Cable

2.4 LED indicators and Reset button

LED	Indication
Power	RED – on when power applied
Ready	Green -- blinking per second when system is ready
<Ethernet>	Ethernet Link/Act/10/100Mbps: Orange -- 10BaseT Ethernet connection established Green -- 100BaseT Ethernet connection established Blinking: data in activity ON: no data in activity and link connected

A recessed **RESET** button is located on the rear panel. Press the button to reboot the IP-KVM unit

2.5 System requirements

Hardware

Item	Description
Local Host side	One Computer or Server or the console port of the KVM switch

Local console side	One PS/2 or USB Keyboard and Mouse, and one Monitor
Remote Console side	One Computer or Multiple Computers are linked into the network

Software

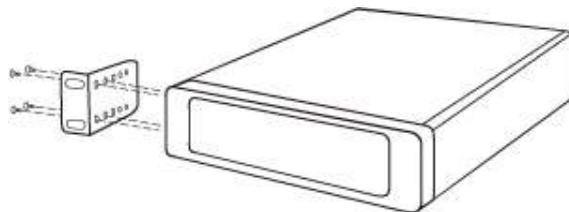
Item	Description
Local Host side	<No additional software necessary>
Remote Console side	(1) Java Runtime Environment (see Note) (2) Browser: Microsoft Internet Explorer (v6.0 or above), Netscape, Mozilla, Safari, Firefox, Avant, World, Opera, and others.

Note The Remote Console browser needs to JRE (Java Runtime Environment) v5.0 (version 1.5) or above. You can get the Java Software from the website <http://www.java.com/en/download/>. It's recommended to install newer Java version (e.g. version 6 update 11 or above) for better performance.

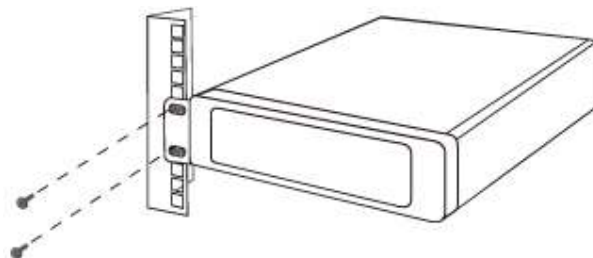
2.6 Hardware installation

The IP-KVM can be placed on the desktop or rack mounted on a 19"/1U rack:

- Screw the mounting brackets into the side of the unit at the front, as shown below



- Slide the unit into the rack and secure it to the rack



2.7 Cabling the connection to stand-alone computers



When connecting cables ensure the IP-KVM and host computer are powered off

2.6.1 Stand alone PS/2

To cable connect to a stand-alone host computer with PS/2 style keyboard and mouse:

- Connect the VGA and PS/2 connectors of the attached 3-in-1 Integrated Host Cable to the **Host** computer
- Connect the 3-in-1 Integrated Adapting Cable to the **Local** DB-15 connector of IP-KVM
- Connect the monitor to the Adapting Cable
- Connect the keyboard to the Adapting Cable
- Connect the mouse to the Adapting Cable
- Connect one end of Ethernet cable to LAN1 or LAN 2 jack of IP-KVM, and the other end to the Remote Console computer

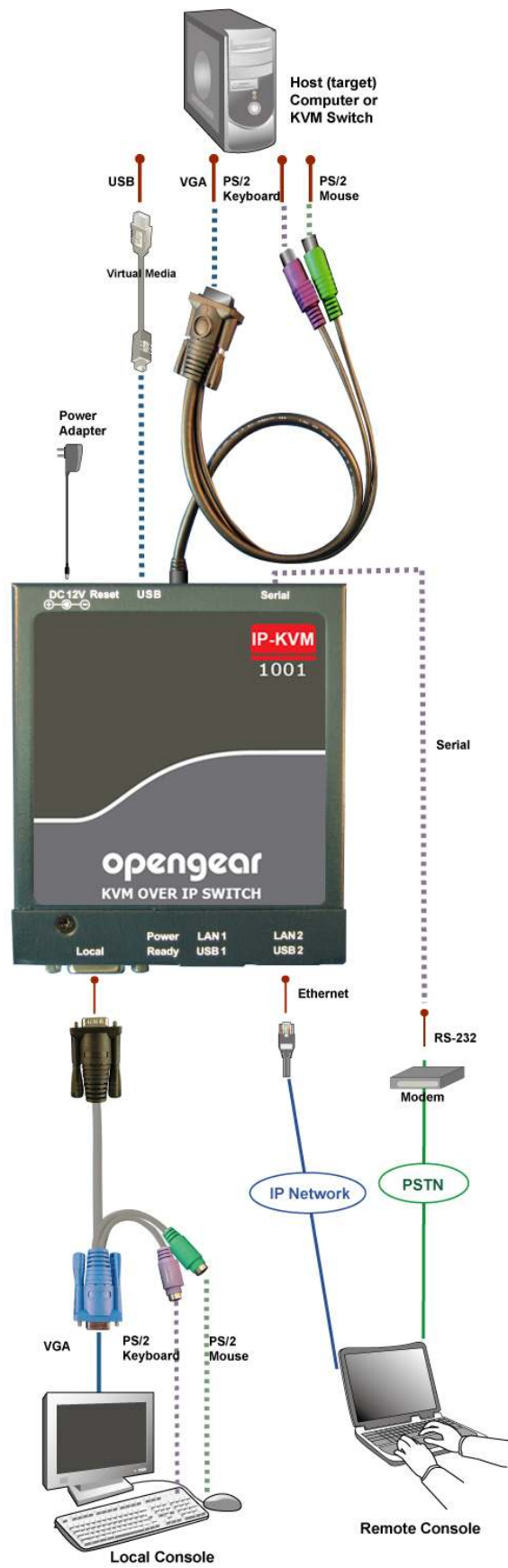


Figure 2-5 Cable Connections (stand-alone, PS/2)

The IP-KVM cabling should now be connected to the Host and Console devices as shown in Figure 2.5 above. Leave the Serial interface open for now. Optionally connect the USB connectors of USB A-mini cable to the Host computer and the IP-KVM (for remote mass storage control).

- Apply power to the Host and IP-KVM. It will take about 60 seconds to complete its startup processes and enter normal running state

2.6.2 Stand alone USB

To cable connect to a stand-alone host computer with USB keyboard /mouse:

- Connect the VGA of the attached 3-in-1 Integrated Host Cable to the **Host** computer
- Connect the USB connectors of USB A-mini cable to the host computer and the IP-KVM module while for remote mass storage control
- Connect the 3-in-1 Integrated Adapting Cable to the **Local** DB-15 connector of IP-KVM
- Connect the monitor to the Adapting Cable
- Connect the USB keyboard to the USB2 or USB1 connector
- Connect the USB mouse to the USB1 or USB2 connector
- Connect one end of Ethernet cable to LAN1 or LAN 2 jack of IP-KVM, and the other end to the Remote Console computer (over your IP network)

Figure 2.6 below depicts the installation cable connections:

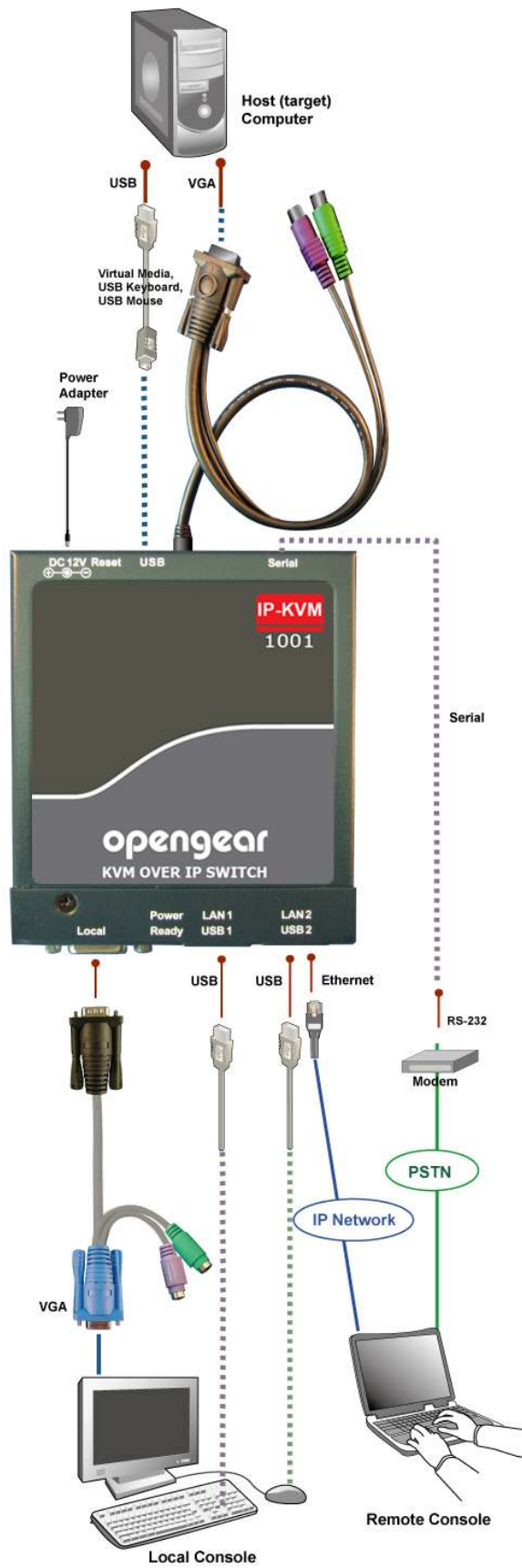


Figure 2-6 Cable Connections (stand-alone, USB)

2.6.3 Cascaded connection

The IP-KVM has a built-in Ethernet hub so it is simple to cascade multiple IP-KVM devices to control multiple host computers:

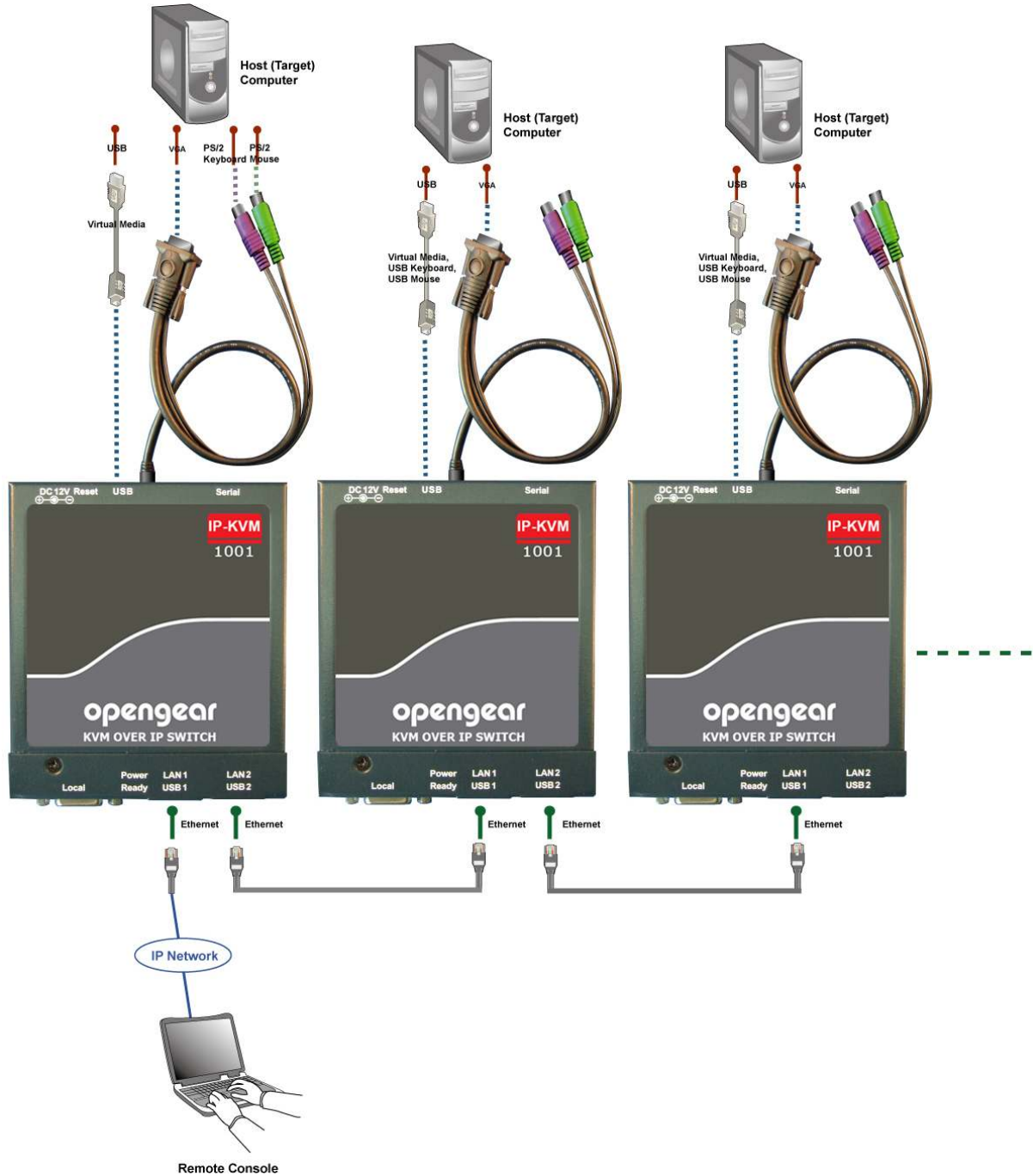


Figure 2-7 Cable Connections (stand-alone, PS/2)

- Install cable connections between each stand-alone IP-KVM and Host computer (as described in 2.6.1 and 2.6.2)

- With straight or cross-over Ethernet cables interconnect the IP-KVM devices using LAN1 or LAN2 sockets
- Connect one end of the Ethernet cable to LAN1 or LAN 2 jack of one of the IP-KVM devices and the other end to the Remote Console computer

2.8 Cabling the connection to a multi-port KVM switch

As well as connecting to a standalone computer the IP-KVM host side can alternately be connected to a multi-port KVM switch.

The installation procedures are as for stand-alone computer, except that the host signals are connected to the **PS/2 Local Console** of the KVM Switch.

Figure 2.8 below depicts the cable connections:

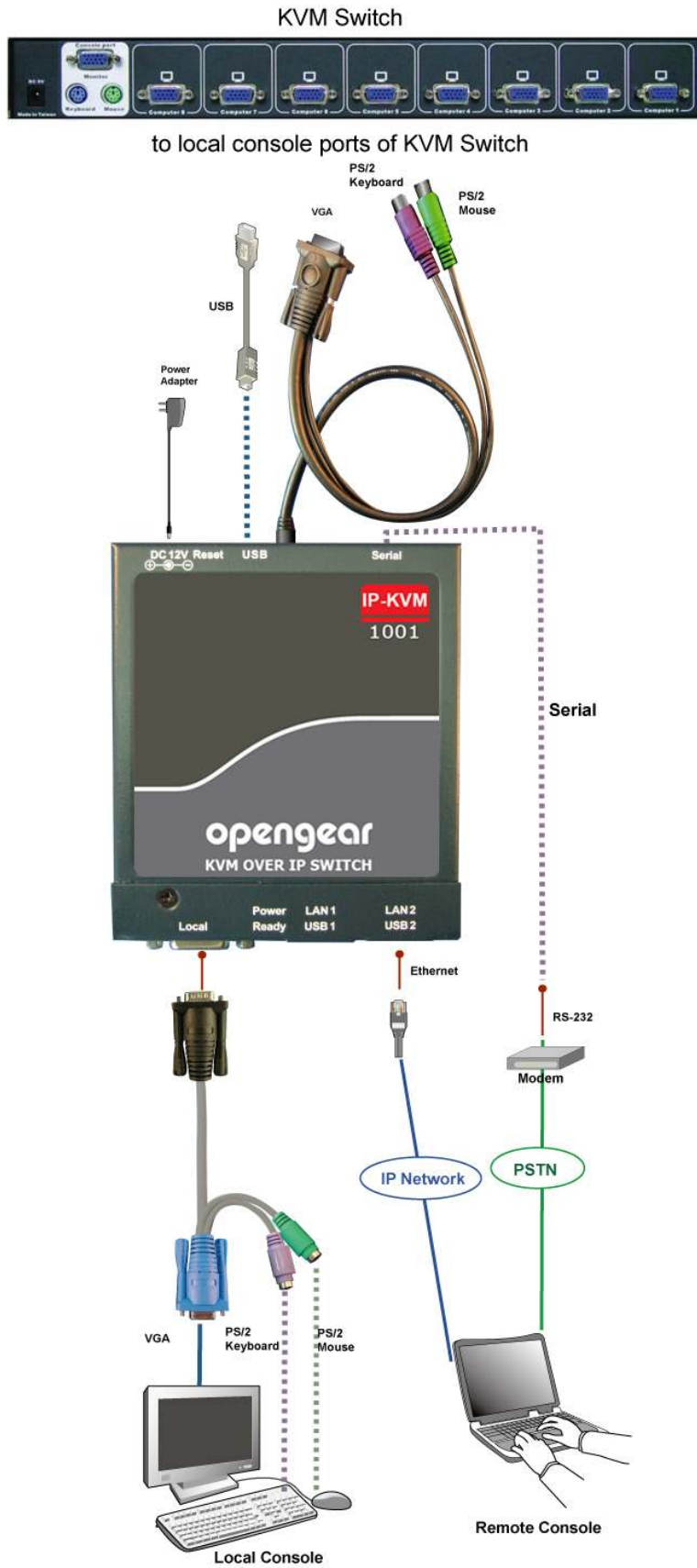


Figure 2-8 Cable Connections (with a Multi-port KVM Switch)

2.9 When the server is up and running

The IP-KVM gives you a full control over the remote server. The Management Console allows you to access the remote server's graphics, keyboard and mouse and to send special commands to the server. You can also perform periodic maintenance of the server. Using the Console Redirection Service, you are able to do the following:

- Reboot the system
- Watch the boot process.
- Boot the system from a separate partition to load the diagnostic environment.
- Run special diagnostic programs

2.10 When the server is dead

Obviously fixing hardware defects is not possible through a remote management device. Nevertheless IP-KVM gives the administrator valuable information about the type of a hardware failure that has occurred so they can initiate appropriate recovery action:

Type of failure	Detected by
Hard disk failure	Console screen, CMOS set-up information
Power cable detached, power supply failure	Server remains in power off state after power on command has been given.
CPU Controller, main board failure.	Power supply is on, but there is no video output.
CPU fan failure	By server specific management software
RAM failure	Boot-Sequence on boot console

3. Configuration

Introduction

This chapter provides step-by-step instructions for the initial network configuration and the keyboard, video and mouse communications settings. The IP-KVM can be set up:

- Over the network using the *psetup* tool
- Over the network using a web browser
- Over a serial connection using a terminal (emulator)

3.1 Initial IP configuration using *psetup*

The factory default settings for the IP-KVM unit are:

DHCP: Disable

Default IP address: 192.168.0.70

Default Net Mask: 255.255.255.0

If this initial configuration does not meet your local requirements you can use the *psetup* setup tool to change the configuration to suit your needs. You can be find *psetup* on your IP-KVM CD-ROM. The *psetup* tool can locate all the IP-KVM units on your IP network and set their network configuration (IP address, subnet mask, DHCP etc).

3.1.1 Reset the Super User password

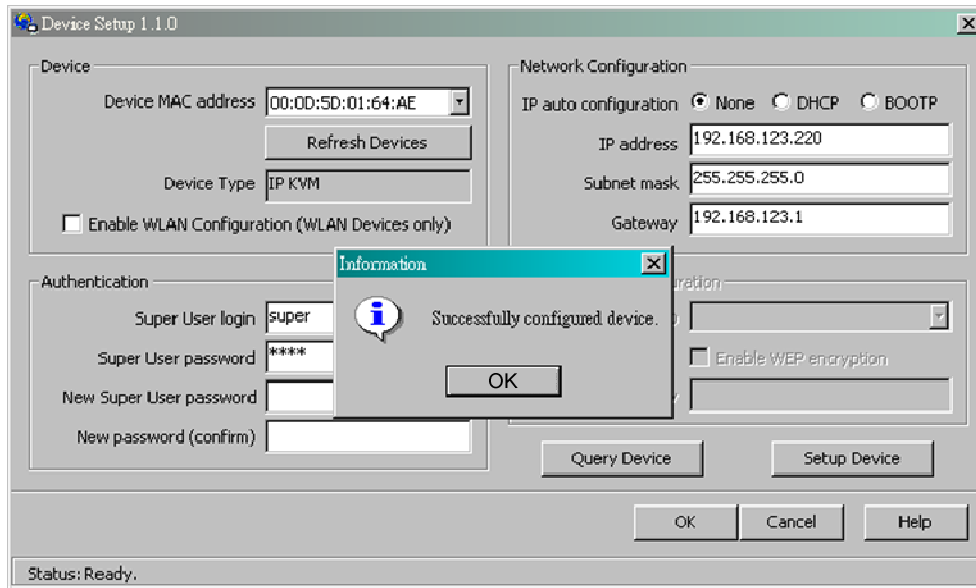


Make sure to change the super user password immediately after you have installed and accessed your IP-KVM for the first time. Not changing this password for the super user is a severe security risk and might result in unauthorized access to the IP-KVM and to the host system

- Click **Refresh Devices** and *psetup* will detect any network connected IP-KVM devices and display them by their MAC addresses
- You can click **Query Device** and it will show the current IP configuration of the selected MAC address device (i.e. IP address 192.168.0.70)
- Enter the *Super User login* name. The initial name is **super** with all lower case characters
- Enter the current *Super User password*. This initial value is **pass** again all lower case
- Enter a *New Super User password* and re-type the *New password* confirmation

Note The IP-KVM accepts 32 letters of username and password

- Press the OK button to accept these changes. This will close the window and you will need to reload *psetup*



3.1.2 Set up a fixed IP

The *psetup* tool can configure the IP-KVM with a fixed IP address:

- Click **Refresh Devices** and *psetup* will detect any network connected IP-KVM devices and display them by their MAC addresses
- For *Authentication* enter the *Super User login* name (*super*) and the new *Super User password*
- Set *IP auto configuration* as “None” and enter the new *IP address* and *Subnet mask* (and optionally enter the IP address of the *Gateway* for the network segment)
- Click **Setup Device**. If super login was authenticated, it'll show *Successfully configured device*. Otherwise it'll show *Permission Denied*

3.1.3 Enable DHCP

Alternately you can use *psetup* to set the IP-KVM in DHCP mode:

- Click **Refresh Devices** and log as the *Super User*
- Set *IP auto configuration* as **DHCP**

- Click **Setup Device**. Once enabled, the IP-KVM will try to contact a DHCP server in the subnet to which it is physically connected. If a DHCP server is found, it may provide a valid IP address, gateway address and net mask
- Before you connect the device to your local subnet, be sure to complete the corresponding configuration of your DHCP server. It is recommended to configure a fixed IP assignment to the MAC address of the IP-KVM. You can find the MAC address labeled on the bottom side of the metal housing

If you have installed the IP-KVM on a network with DHCP enabled when you plug the Ethernet cable to IP-KVM it will be assigned an IP address via DHCP. You can use *psetup* to find out this IP:

- Click **Refresh Devices** button to detect connected IP-KVM devices and select MAC address of the IP-KVM in *Device MAC address* box. You can find the MAC address labeled on the bottom side of the IP-KVM unit. MAC address is detected as connection from computer and IP-KVM is valid through USB or network
- Click **Query Device** to find the IP configuration of the selected IP-KVM unit

Note You can nominate IP addresses to be assigned by BOOTP or DHCP. BOOTP is a static configuration protocol that uses a table to maps IP addresses to physical addresses. DHCP is an extension to BOOTP that dynamically assigns configuration information.

3.2 Initial IP configuration using a web browser

The factory default settings for the IP-KVM unit are:

DHCP: Disable

Default IP address: 192.168.0.70

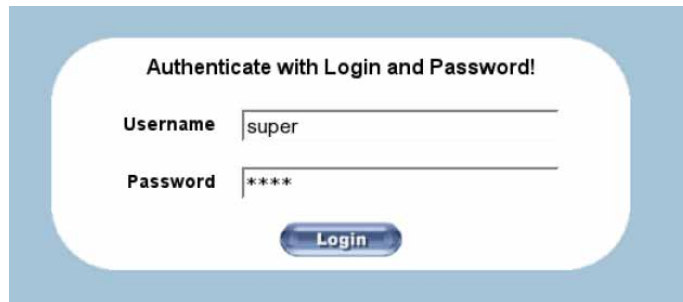
Default Net Mask: 255.255.255.0

Using your favorite web browser you can access the IP-KVM from the Remote Console computer that you have IP connected to LAN1 (or LAN2):

- Enter **https://192.168.0.70** (for a secure SSL connection) or **http://192.168.0.70** (for an insecure connection)

Note Your web browser must be enabled to accept cookies, or else login is not possible

- This will lead you to the IP-KVM login page as shown below:



- Log in using the default system user name **super** and the default password **pass**

When connecting to the IPK-KVM unit, the IPK-KVM system (web server, Telnet server or SSH server) will prompt user to enter the user name and password in order to access to the system. If this is the first time logging in, log in with the factory default username and password, you will be prompted to change the default password.



Make sure to change the super user password immediately after you have installed and accessed your IP-KVM for the first time. Not changing this password for the super user is a severe security risk and might result in unauthorized access to the IP-KVM and to the host system

- The IP-KVM home page will display
- Select **Device Settings: Network** and under **Network Basic Settings** you can set new IP address or enable DHCP/BOOTP

Network Basic Settings

IP auto configuration *

Preferred host name (DHCP only) *

IP address

Subnet mask *

Gateway IP address

Primary DNS server IP address *

Secondary DNS server IP address *

- Click **Apply**

Note: To configure using the web browser, the Remote Console computer must have an IP address in the same network range as the IP-KVM (i.e. it must have an address 192.168.0.0 - 192.168.0.255). If setting up the Remote Console computer in this range is not convenient you can as an alternate set the IP-KVM IP address using the *psetup* program or using a serial console

3.3 Initial IP configuration using the serial console

The IP-KVM has a serial line interface (host side) which can be accessed using a serial terminal (or terminal emulator). This connector is compliant with the RS-232 serial line standard and is configured as shown below:

Parameter	Value
Bits/second	115200
Data bits	8
Parity	No
Stop bits	1
Flow Control	None

When configuring the IP with a serial terminal (such as Hyper Terminal):

- Reset the IP-KVM and immediately press the *ESC* key. You will see some device information, and a => prompt
- Enter **config** then press *Enter* key and wait for a few seconds for the configuration questions to appear
- As you proceed the following questions will appear on the screen. To accept the default values shown in square brackets below, press *Enter* key:

IP auto configuration: None
IP address: [192.168.0.70]
Net mask: [255.255.255.0]
Gateway: [0.0.0.0] -- (0.0.0.0 for none)

IP auto-configuration: With this option you can specify whether the IP-KVM should get its network settings from a DHCP or BOOTP server. For DHCP, enter **dhcp** and for BOOTP enter **bootp**. If you do not specify any of these, the IP auto-configuration is disabled and subsequently you will be asked for the following network settings

IP address: The IP address the IP-KVM. This option is only available if IP auto-configuration is disabled

Net mask: The net mask of the connected IP subnet. This option is only available if IP auto-configuration is disabled

Gateway address: The IP address of the default router for the connected IP subnet. If you do not have a default router, enter 0.0.0.0. This option is only available if IP auto-configuration is disabled

3.4 Keyboard, mouse and video configuration

Between the IP-KVM and the Host there are two interfaces available for transmitting keyboard and mouse data (USB and PS/2). The correct operation of the remote mouse depends on several settings which will be discussed in the following subsections.

3.4.1 IP-KVM keyboard settings

The IP-KVM settings for the host's keyboard type have to be corrected in order to make the remote keyboard work properly. Check the settings in the IP-KVM Web front-end for details.

3.4.2 Remote Mouse Settings

A common seen problem with KVM devices is the synchronization between the local and remote mouse cursors. The IP-KVM addresses this situation with an intelligent synchronization algorithm. There are two mouse modes available on the IP-KVM:

- **Auto mouse speed** The automatic mouse speed mode tries to detect the speed and acceleration settings of the host system automatically. See the section below for a more detailed explanation.
- **Fixed mouse speed** This mode just translates the mouse movements from the Remote Console in a way that one pixel move will result in n-pixel moves on the remote system.

This parameter *n* is adjustable with the scaling. Please note that this works only when mouse acceleration is turned off on the remote system.

3.4.3 Automatic mouse speed and mouse synchronization

The automatic mouse speed mode performs the speed detection during mouse synchronization. Whenever the local and remote mouse cursors move synchronously or not, there are two ways for re-synchronizing local and remote mouse cursors:

- **Fast Sync** The fast synchronization is used to correct a temporary, but fixed skew. Choose the option using the Remote Console options menu or press the mouse synchronization hotkey sequence in case you defined one
- **Intelligent Sync** If the fast sync does not work or the mouse settings have been changed on the host system, use the intelligent resynchronization. This method takes more time than the fast one and can be accessed with the appropriate item in the Remote Console option menu. The intelligent synchronization requires a correctly adjusted picture. Use the auto adjustment function to setup the picture, and make sure that there are no window at the top left corner of the remote desktop that are able to change the mouse cursor shape from the normal state. The Sync mouse button on top of the Remote Console can behave differently, depending on the current state of mouse synchronization. Usually pressing this button leads to a fast sync, except in situations where the KVM port or the video mode changed recently

Note: At first start, if the local mouse pointer is not synchronized with the remote mouse pointer, press the Auto Adjust Button once

3.4.4 Host system mouse settings

The host's operating system knows various settings from the mouse driver.

Note: The following limitations do not apply in case of USB and Mouse Type *Windows >= 2000, MacOSX*

While the IP-KVM works with accelerated mice and is able to synchronize the local with the remote mouse pointer, there are the following limitations, which may prevent this synchronization from working properly:

- **Special Mouse Driver** There are mouse drivers that influence the synchronization process and lead to desynchronized mouse pointers. If this happens, make sure you do not use a special vendor-specific mouse driver on your host system
- **Windows XP Mouse Settings** Windows XP knows a setting named “improve mouse acceleration”, which has to be deactivated

- **Active Desktop** If the Active Desktop feature of Microsoft Windows is enabled do not use a plain background. Instead, use some kind of wallpaper. As an alternative, you could also disable the Active Desktop completely.

Navigate your mouse pointer into the upper-left corner of the applet screen and move it slightly forth and back. Thus the mouse will be resynchronized. If re-synchronizing fails, disable the mouse acceleration and repeat the procedure.

3.4.5 Single and Double Mouse Mode

The information above applies to the Double Mouse Mode, where remote and local mouse pointers are visible and need to be synchronized. The IP-KVM also features a Single Mouse Mode where only the remote mouse pointer is visible. Activate this mode in the open Remote Console and click into the window area. The local mouse pointer will be hidden and the remote one can be controlled directly. To leave this mode, it is necessary to define a mouse hotkey in the Remote Console Settings Panel. Press this key to free the captured local mouse pointer.

3.4.6 Recommended Mouse Settings

For the different operating systems we recommend:

- **MS Windows** In general, we recommend the usage of a mouse via USB. Choose USB without Mouse Sync. For a PS/2 mouse choose Auto Mouse Speed. For XP disable the option “enhance pointer precision” in the Control Panel
- **SUN Solaris** Adjust the mouse settings either via *xset m 1* or use the CDE Control Panel to set the mouse to *1:1, no acceleration*. As an alternative you may also use the Single Mouse Mode
- **MAC OS** We recommend using the Single Mouse Mode.

3.4.7 Video Modes

The IP-KVM recognizes a limited number of common video modes. When running X11 on the host system, please do not use any custom mode lines with special video modes. If you do, the IP-KVM may not be able to detect them. We recommend using any of the standard VESA video modes, instead.

4. Usage

Introduction

The IP-KVM features an embedded operating system and applications offering a variety of standardized interfaces. This chapter describes using these interfaces.

4.1 Prerequisites

The interfaces are accessed using the TCP/IP protocol family, thus they can be accessed using either LAN port on the device. The following interfaces are supported:

- **HTTP/HTTPS** This provides full access to the embedded web server so the IP-KVM environment can be managed using a standard web browser. You can access the IP-KVM using the insecure HTTP protocol, or using the encrypted HTTPS protocol. It is recommended whenever possible to use HTTPS. HTTP/HTTPS is the primary interface of the IP-KVM and it is covered extensively in this chapter
- **Telnet** A standard Telnet client can also be used to access an arbitrary device connected to the IP-KVM's serial port via a terminal mode. However this is not the primary interface and is addressed in subtopics

4.1.1 Browser

In order to use the Remote Console window of your managed host system, the browser has to come with a Java Runtime Environment version 1.5 or above. If the browser has no Java support (such as on a small handheld device), you are still able to maintain your IP-KVM using the administration forms displayed by the browser itself.

Your web browser also must be configured to accept cookies or else login is not possible.

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 and some of the old browsers do not have a strong 128 bit encryption algorithm. You should check your browser (e.g. for Internet Explorer select *Help:About*)



Figure 4-1 The Internet Explorer displaying the encryption key length

For secure connection to the IP-KVM, we recommend using Microsoft Internet Explorer version 6.0 (or higher), Netscape Navigator 7.0 (or higher) or Mozilla 1.6 (or higher). Newer web browsers generally support strong encryption on default.

4.2 Logging in and out

4.2.1 Log in to the IP-KVM

There are three user levels of users who can access the IP-KVM:

User Name	Default Password	Access Privileges
super (factory default)	pass (factory default)	Full access
administrator	(user define)	Has partial rights to change configuration of critical parts
user	(user define)	Has permission to access basic function of open Remote Console

These users are created (and removed) by the *super* user (refer *Chapter 5.3 User Management*) and the permission items for each user level are detailed in Appendix C.

To log in:

- Launch your web browser and direct it to the address of your IP-KVM. This address used can be an IP address or a domain name (in the case where you have given your IP-KVM a symbolic name in the DNS):
 - Type in **http://<IP address of IP-KVM>** for a insecure connection, or
 - type in **https://<IP address of IP-KVM>** for a secure connection
- This will lead you to the IP-KVM login page as shown below:



- Log in using the default system user name **super** and the default password **pass**

When connecting to the IPK-KVM unit, the IPK-KVM system (web server, Telnet server or SSH server) will prompt user to enter the user name and password in order to access to the system. If this is the first time logging in, log in with the factory default username and password, you will be prompted to change the default password.



Make sure to change the super user password immediately after you have installed and accessed your IP-KVM for the first time. Not changing this password for the super user is a severe security risk and might result in unauthorized access to the IP-KVM and to the host system

Having logged into the IP-KVM successfully, the main page of the IP-KVM appears. This page consists of three parts:

- The buttons on the left hand side which allow you to navigate within the front end



- The buttons of the front end are in the upper right:



Home

Return to main page of IP-KVM access page



Console

Open the IP-KVM remote console

Note: If there is no activity for 30 minutes, the IP-KVM will log you out, automatically. A click on one of the links will bring you back to the login screen

- Within the right frame the task-specific information is displayed that depends on the section you have chosen before
 - Click on **Click to open** to start the remote console redirection
 - Click on **Refresh** to refresh the picture



4.2.2 Log out from the IP-KVM



Logout

This link 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 30 minutes.

4.3 The Remote Console

The Remote Console is the redirected screen, keyboard and mouse of the remote host system that IP-KVM controls.

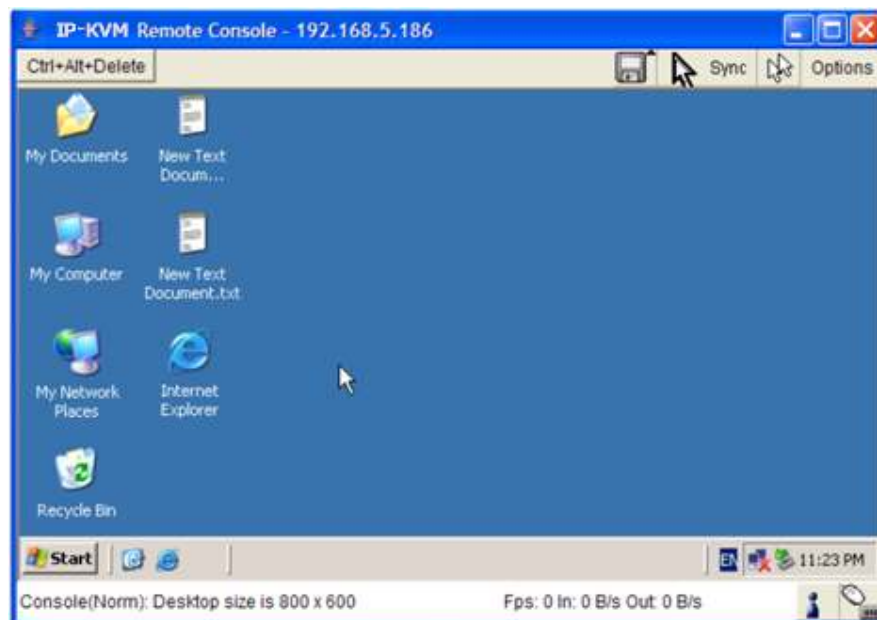
The Remote Console window is a Java Applet that tries to establish its own TCP connection to the IP-KVM. The protocol that is running over this connection is neither HTTP nor HTTPS, but RFB (Remote Frame Buffer Protocol). As default, RFB tries to establish a connection to TCP port number 443. Your local network environment has to allow this connection to be made, i.e. your firewall and, in case you have a private internal network, your NAT (Network Address Translation) settings have to be configured accordingly.

In case the IP-KVM is 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 desired 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 networking environment.

4.3.1 Main Window of Remote 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



Starting the Remote Console opens an additional window. It displays the screen content of your host system. The Remote Console will behave exactly in the same way as if you were sitting locally 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 link to which you use to connect to the IP-KVM.

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.

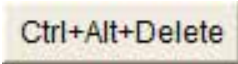

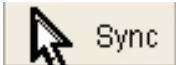
Note: The Remote Console window on your local window system is just one window among others. In order to make keyboard and mouse work, your Remote Console window must have the local input focus

4.3.2 Control Bar of Remote Console

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 adjust the local Remote Console settings:



Figure 4-2 Remote Console Control Bar

- **Ctrl+Alt+Delete**  Special button key to send the “Control Alt Delete” key combination to the remote system (see also section 5.4.1 for defining new button keys)
- **Auto Adjust Video**  If the video display is of bad quality or distorted in some way, press this button and wait a few seconds while the IP-KVM tries to detect the video mode of VGA port to the controlled host and adjust itself for the best possible video quality
- **Synchronize Mouse**  Activates 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


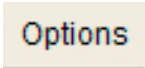
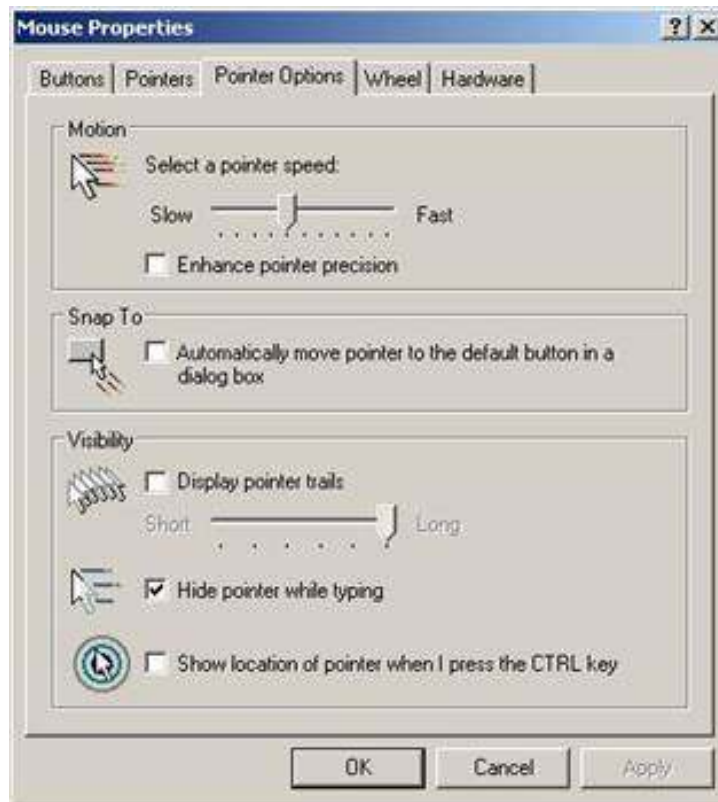
- **Single/Double mouse mode**  Switches between the Single Mouse Mode (where only the remote mouse pointer is visible) and the Double Mouse Mode (where remote and local mouse pointers are visible and need to be synchronized). Single mouse mode is only available if using SUN JVM 1.5 or higher
- **Options**  To open the Options menu, click on the button *Options*



Figure 4-3 Remote Console Options Menu

Note: If your IP-KVM connects to PS/2 target computer and enable Double Mouse mode, in order to keep remote and local mouse pointers in sync, please take the following actions:

1. **Disable** the “Enhance pointer precision” and “Automatically move mouse pointer to the default button in a dialog box” in the mouse settings of host (target) computer OS.



2. If mouse pointers are not in sync, click on **Sync** button or **Options > Mouse Handling > Intelligent Sync**

A short description of these options as 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 or she 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.



Figure 4-4 Remote Console Exclusive Mode

- **Scaling** Allow you to scale down the Remote Console. You can still use both mouse and the keyboard, however the scaling algorithm will not preserve all display details. When you designate 25%, 50%, or 100% scaling, the size of Remote Console window is

calculated according to the remote host video setting with scaling algorithm execution. When you designate “Scale to fit”, the remote video displaying is scaled to fit the size of Remote Console window.

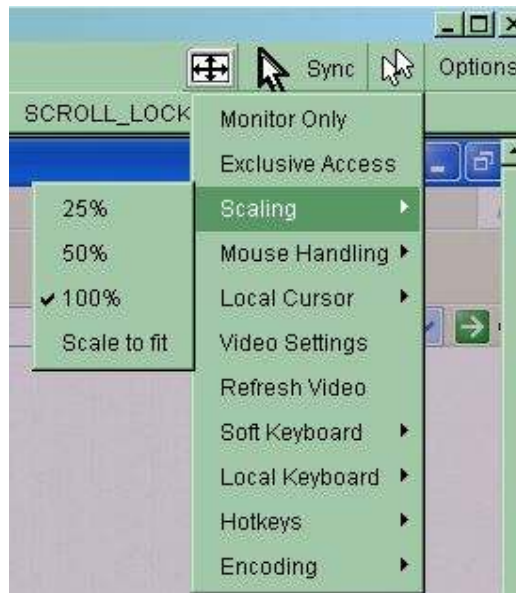
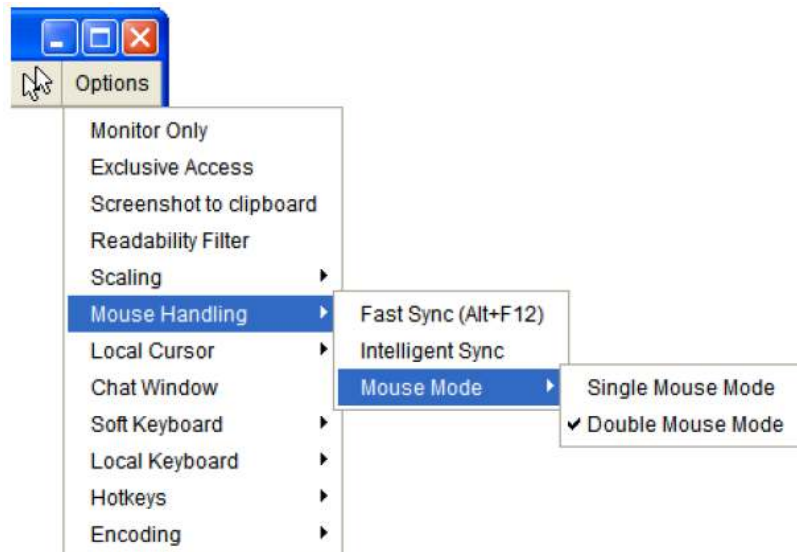


Figure 4-5 Remote Console Options Menu:Scaling

- **Mouse Handling** The submenu for mouse handling offers two options for synchronizing the local and the remote mouse cursors:



- 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 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 (version of 1.5 or above offers the full list)



Figure 4-6 Remote Console Options Menu:Cursor

- **Video Settings** Opens a panel for changing the IP-KVM video settings. IP-KVM features two different dialogs, which for adjusting the video settings:

- Video Settings through the HTML-Frontend* To enable local video port, select this option. This option decides if the local video output of IP-KVM is active and passing through the incoming signal from the host system.

The option Noise Filter defines how 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 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.

ii. *Video Settings through the remote console*

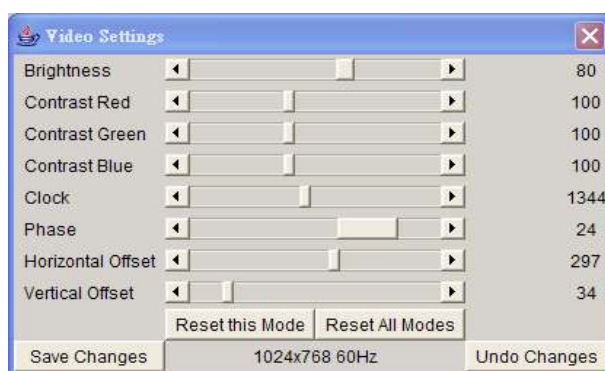


Figure 4-7 Video Settings Panel

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 (Clock , Phase and Position) 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

- **Refresh Video** Click to run this menu item for retrieving the whole video again from the controlled host and displayed on Remote Console. In normal situation, only changed

parts of video will be packed and sent from IP-KVM, for saving network bandwidth. This function is mainly used for troubleshooting purpose where some old video fragments are displayed as not updated in time for some reason; for example, noise filter for VGA is setting too large

- **Soft Keyboard** Opens up the Menu for the Soft-Keyboard



Figure 4-8 Soft Keyboard

Show Pops up the Soft-Keyboard. The Soft-Keyboard is necessary in case your host system runs a completely different language and country mapping than your administration machine.

Mapping Used for choosing the specific language and country mapping of the Soft-Keyboard.

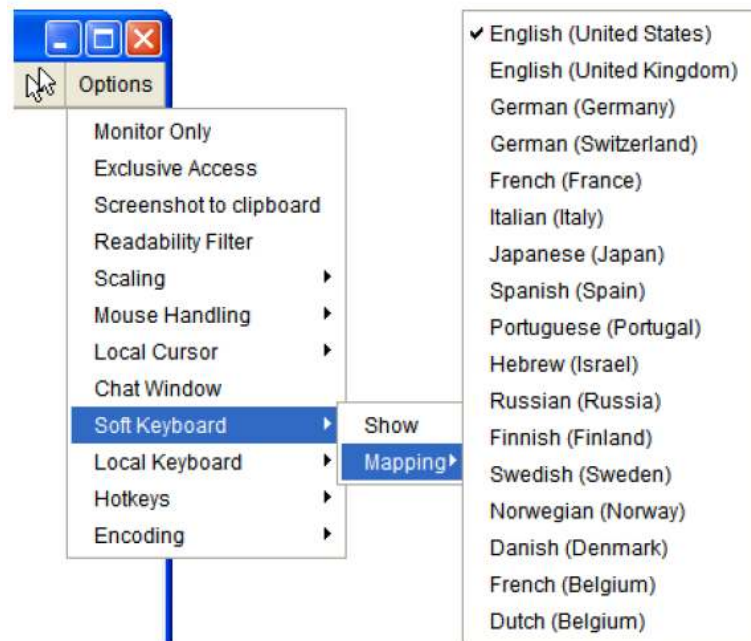


Figure 4-9 Soft Keyboard Mapping

- **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 before. 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 execute the command on the remote host

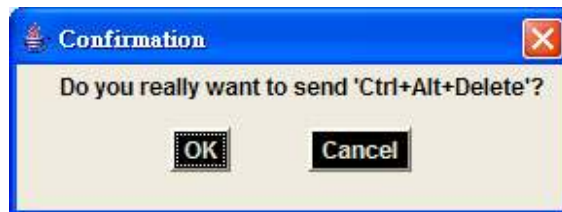
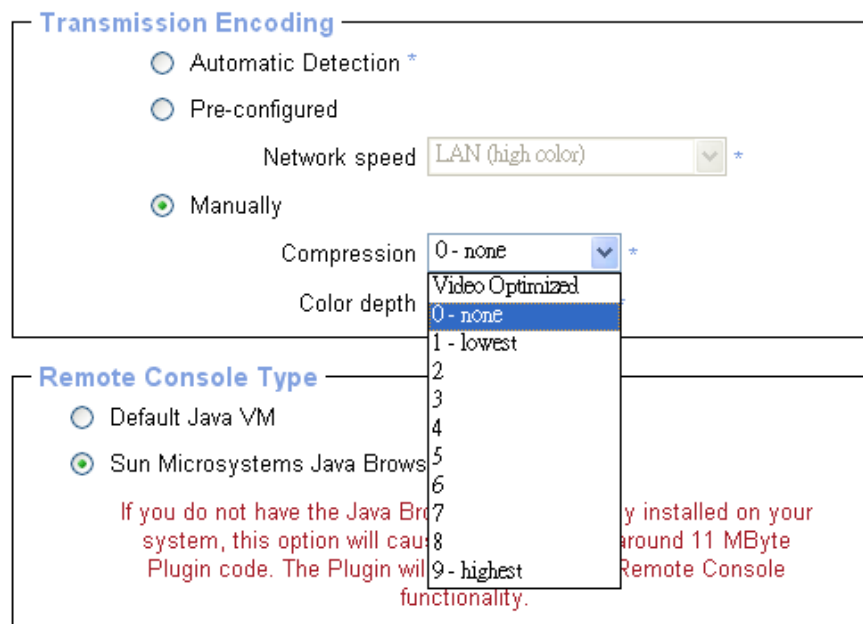


Figure 4-10 Remote Console Confirmation Dialog

- **Encoding** These options are used to adjust the encoding level in terms of compression and color depth. They are only available unless "Transmission Encoding" is determined manually (select **Manually** in **KVM Settings > User Console > Transmission Encoding** of web page).



Compression Level You may select a value between 1 and 9 for the desired compression level with level 1 enabling the fastest compression and level 9 the

best compression. The most suitable compression level should always be seen as a compromise between the network bandwidth that is available, on your video picture to be transferred, and on the number of changes between two single video pictures. We recommend using a higher compression level if the network bandwidth is low. The higher the compression level the more time is needed to pack and unpack the video data on either side of the connection. The compression quality depends on the video picture itself, e.g. the number of the colors or the diversity of pixels. The lower the compression quality, the more data have to be sent and the longer it may take to transfer the whole video picture.

If level 0 is chosen the video compression is disabled, completely.

The option "Video Optimized" has its advantages if transferring high-quality motion pictures. In this case the video compression is disabled, completely and all video data is transferred via network as full-quality video snippets. Therefore, a high amount of bandwidth is required to ensure the quality of the video picture.

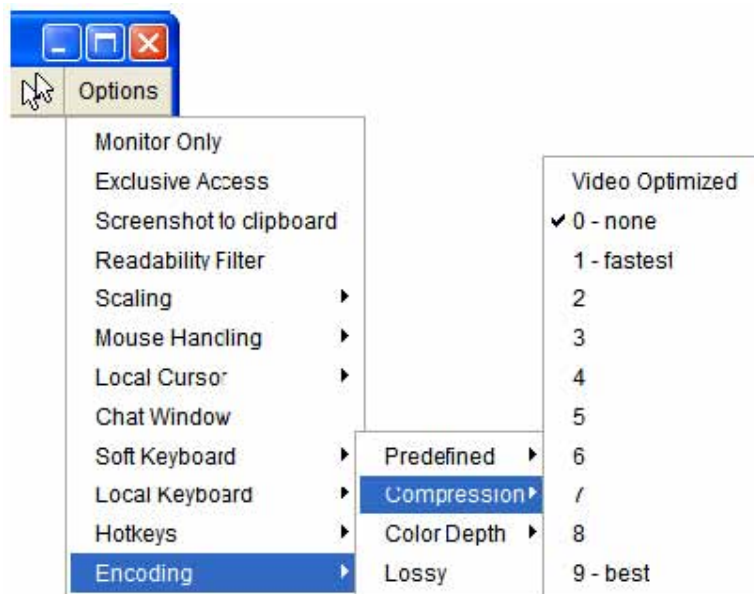


Figure 4-11 Encoding Compression

The next two options allow you to set the compression level to a predefined level OR to set a level for *lossy* compression. This compresses well but leads to degradation in image quality.

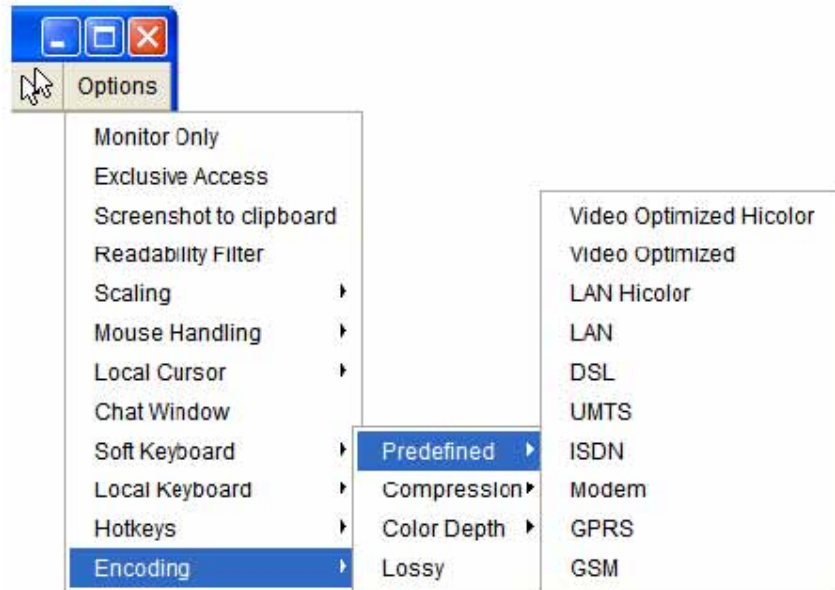


Figure 4-12 Predefined Compression

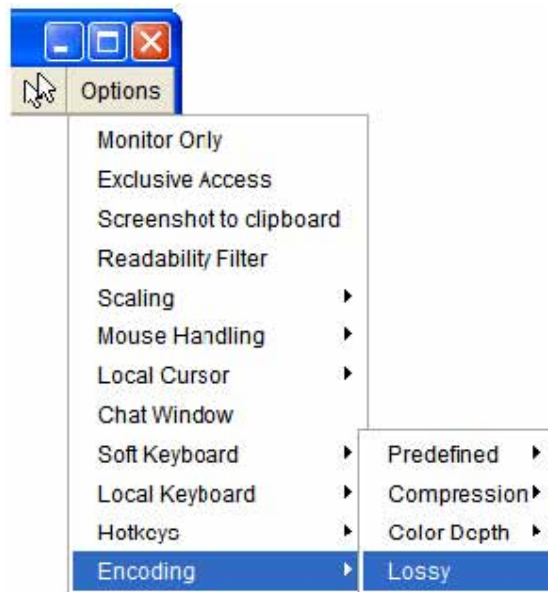


Figure 4-13 Lossy Compression

Color Depth Set the desired color depth. You may select between 8 or 16 bit for Video Optimized/compression level 0, or between 1 and 8 bit for compression level 1 to 9. The higher the color depth, the more video information has to be captured and to be transferred.

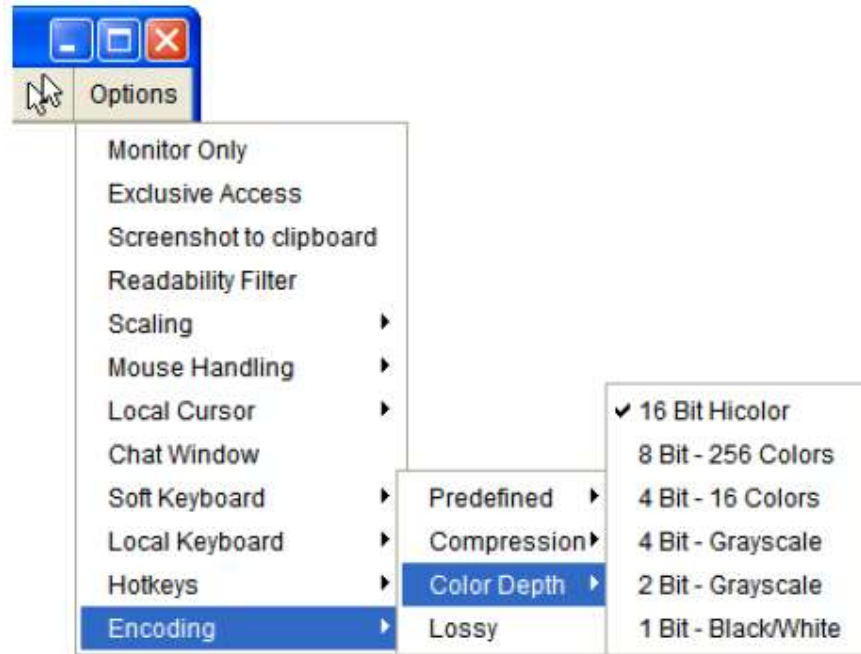


Figure 4-14 Encoding Color depth

Note: If displaying motion pictures on a connection with low speed you may achieve an improvement regarding the video transfer rate by lowering the color depth and disabling the option "Video Optimized". As a general result, the data rate is reduced (less bits per color). Furthermore, the IP-KVM will not have to do any video compression. In total, this will lead to less transfer time of the motion picture.

4.3.3 Status Line of Remote Console

The status line shows both console and the connection state. The size of the remote screen is displayed. Figure 4.15 below was taken from a Remote Console with a resolution of 800x600 pixels. The value in brackets describes the connection to the Remote Console. *Norm* indicates a standard connection without encryption whereas *SSL* means a secure connection.

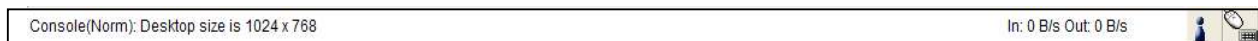


Figure 4-15 Status line

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

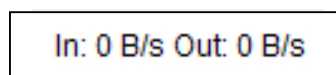


Figure 4-16 Status line transfer rate

5. Menu Options

Introduction

This chapter details the main menu options of the IP-KVM. The menu buttons on the left hand side of the main screen allow you to navigate Keyboard, Mouse and Video settings; configure the network and serial port; access the KVM console; set up users and use Virtual Media.



5.1 Remote Control

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



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

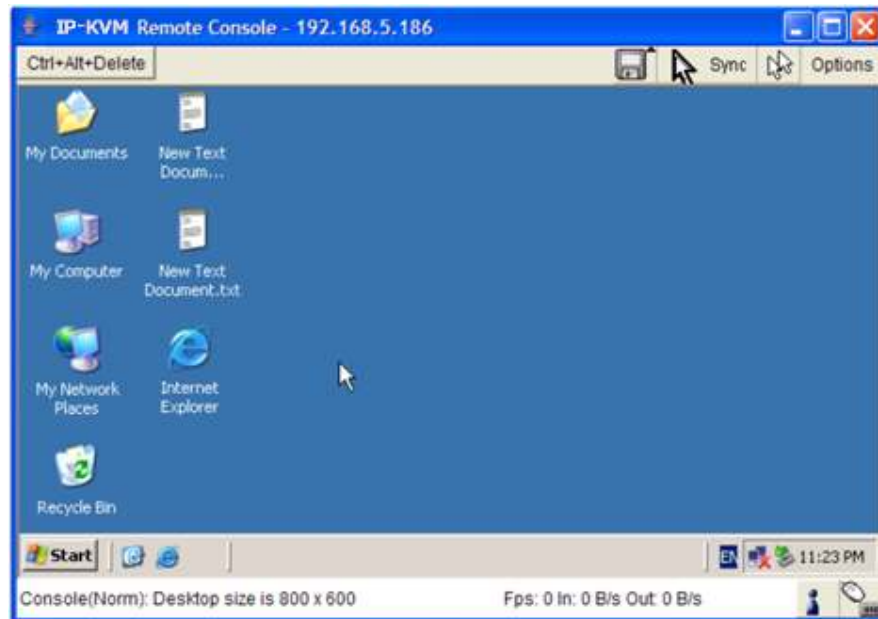


Figure 5-1 KVM Console

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 must first enable the access settings from **Device Settings: Network**

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 *

Apply **Reset to defaults**

* Stored value is equal to the default.

- **Telnet Console**

The IP-KVM firmware features a Telnet server that enables a user to connect via a standard Telnet client. In case the Telnet program is using a VT 100, VT 102 or VT 220 terminal or an according emulation, it is even possible to perform a console redirection as long as the IP-KVM host machine is using a text mode screen resolution. To log into the Telnet Console either:

- click **Remote Control > Telnet Console** or

Telnet Console

```

KVM-IP Terminal Server (c) 2000-2002

Login: super
Password:
eSB> help

Usage: help [<cmd> [<subcmd> [<subcmd> ...]]

A help screen for specified command is printed.
With no arguments given a table of all commands
is printed to the screen.

The following commands are supported :

help          quit          cls          version
terminal     vscap        vscreset

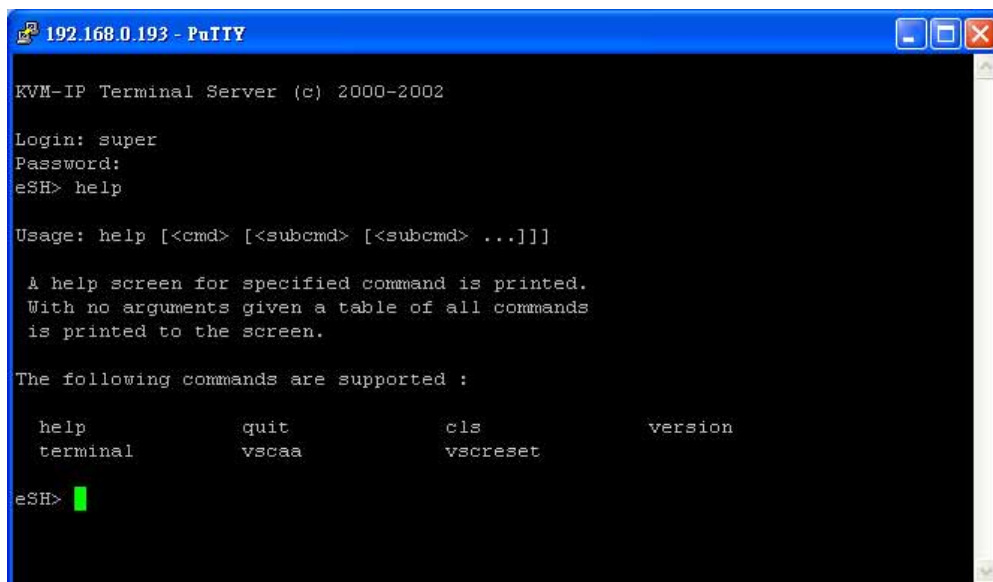
eSB>

```

- enter a *telnet* command as required by the Telnet client (for instance in a UNIX shell type *telnet 192.168.0.70*) or
- run the SSH-supported terminal emulation program (such as **PuTTY**).

Replace the IP address by the one that is actually assigned to the IP-KVM. This will prompt for username and password in order to log into the device. The credentials that need to be entered for authentication are identical to those of the web interface. So the user management of the Telnet interface is entirely controlled with the according functions of the web interface.

Once you have successfully logged into the IP-KVM a command line will be presented and you can enter according management commands.



```

192.168.0.193 - PuTTY
KVM-IP Terminal Server (c) 2000-2002
Login: super
Password:
eSH> help

Usage: help [<cmd> [<subcmd> [<subcmd> ...]]

A help screen for specified command is printed.
With no arguments given a table of all commands
is printed to the screen.

The following commands are supported :

  help          quit          cls          version
  terminal      vscaa        vsreset
eSH>

```

Figure 5-2 Telnet Console

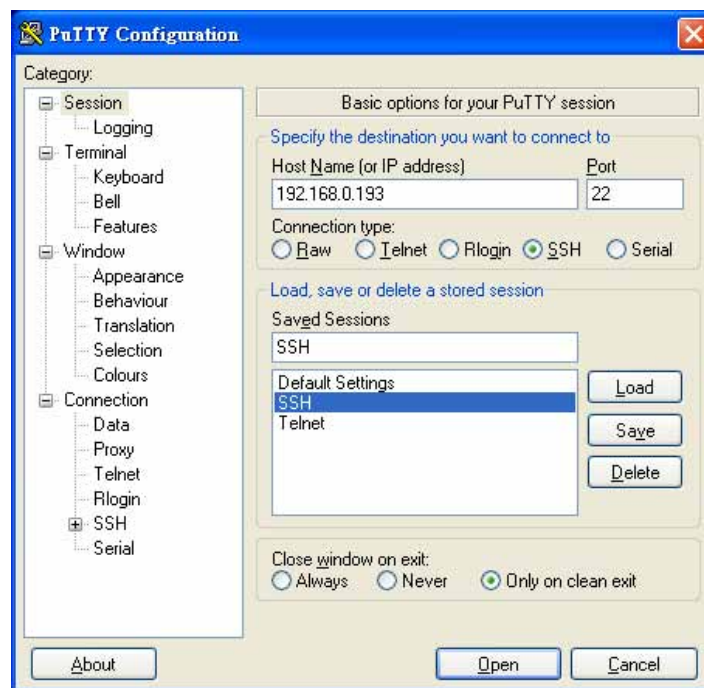
The following list shows the according command mode command syntax and their usage.

- Help** Displays the list of possible commands
- cls** Clears the screen
- quit** Exits the current session and disconnects from the client
- version** Displays the release information
- terminal** Starts the terminal **passthrough** mode for RS-232 serial port. This mode provides **Serial over IP** function. The key sequence *ESC + exit* switches back to the command mode.
- vscaa** Auto adjustment of the Remote Console.

vscreset [modes/allmodes/all] Reset the video modes like in the remote console under option *Video Settings*. *vscreset modes*: reset settings for the current video mode *vscreset allmodes*: reset settings for all video modes *vscreset all*: reset all video modes and global settings (Brightness and Contrast)

- **SSH Console**

The IP-KVM supports SSH security protocol. The SSHv2 will encryption the transferred data so as to keep the data communication secured. Basically the SSH's configuration interface is the same as Telnet console, except that SSH is data encrypted and secured (and can be accessed using SSH-supported terminal emulation programs such as **PuTTY**).



5.2 Virtual Media

The IP-KVM provides a powerful capability called Virtual Media (or Virtual Disk). Using the USB port the IP-KVM 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.

Note Drive Redirection supports only Windows as the client computer since it redirects based on a drive letter.

Before using Virtual Media connect the USB cable from IP-KVM to host computer. After connecting the USB cable you can see a new removable risk on the host computer (e.g. the host computer screen below shows a new CD Drive F)



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.

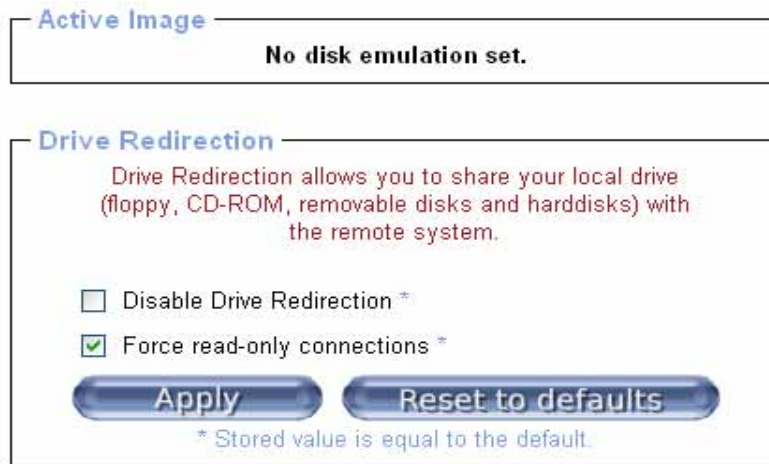


Figure 5-3 Options of Drive Redirection

Drive Redirection works on a level below the operating system. That means that neither the local nor the remote operating system is aware that the drive is currently redirected. 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 you use the Drive Redirection with care, especially the write support.

To use Drive Redirection

- Click **Virtual Media** and select **Drive Redirection**. Drive Redirection (read only) is enabled by default

To disable the Drive Redirection function:

- Check **Disable Drive Redirection**
- **Force read-only connections** if enabled switches off the write support for the Drive Redirection is (so it is not possible to write on a redirected device)
- Click **Apply** to submit your changes

5.2.2 Virtual Drive

To use disable the mass storage emulation (and hide the virtual drive):

- Click **Virtual Media** and select **Virtual Drive**
- Click **Apply** to submit your changes

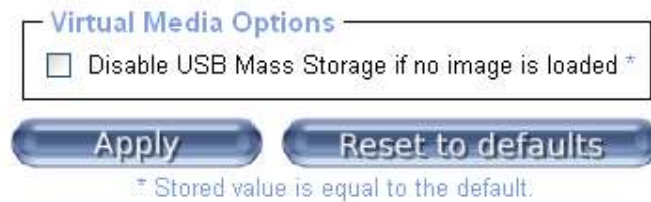


Figure 5-4 USB mass storage option

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

To use an image on Windows share (via SAMBA)

- click **Virtual Media** and select **Virtual Drive**
- select **CD/DVD Image** from the submenu



Figure 5-5 Virtual Media - CD-ROM Image

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

Note

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 supports 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 step if necessary.
5. 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.

Operation Procedure

- Run Nero (or any similar CD/DVD imaging tool) to create the CD/DVD ISO image
- Create a folder and share this folder **in the PC that shares out the image file**. Copy the CD/DVD ISO image file to this sharing folder. (Make sure password has to be setup with the authorized user during Sharing-Permission settings)

For Windows

Open the Explorer, navigate to the directory (or share) and press the right mouse button to open the context menu. Select **Sharing** to open the configuration dialog

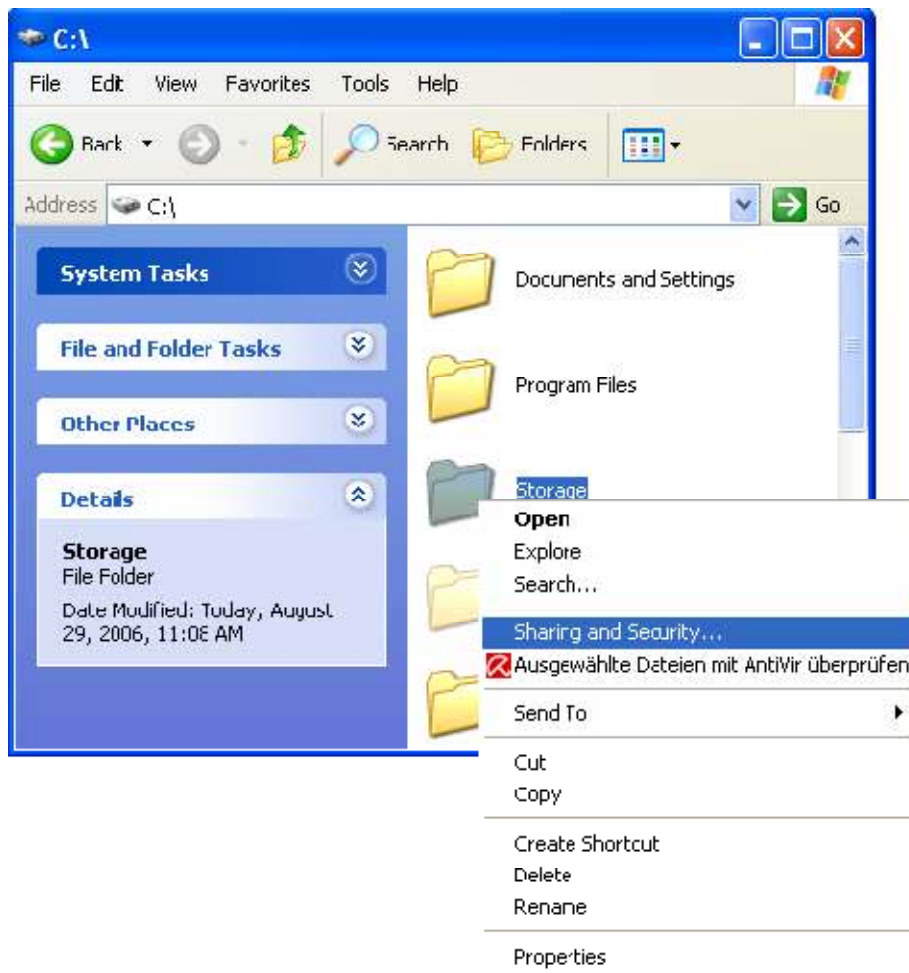


Figure 5-6 Explorer Context Menu



Figure 5-7 Share Configuration Dialog

Adjust the settings for the selected directory.

- Activate the selected directory as a share. Select **Share this folder**.
- Choose an appropriate name for the share. You may also add a short description for this folder (input field **Comment**).
- If necessary, adjust the permissions (**Permissions** button).
- Click **OK** to set the options for this share.

For UNIX and UNIX-like OS (UNIX, Solaris, Linux)

If you like to access the share via SAMBA, SAMBA has to be set up properly. You may either edit the SAMBA configuration file `/etc/samba/smb.conf` or use the Samba Web Administration Tool (SWAT) or WebMin to set the correct parameters.

Also looking at the **man**-entry of **smb.conf** is very helpful.

- Fill in the sharing information on **Image on Windows Share**, click on the **Set** button.

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):

- If the Image file set successfully (shown below) then ...

Image file set successfully

Active Image

CD-ROM Image

Share Host: 59.120.208.56

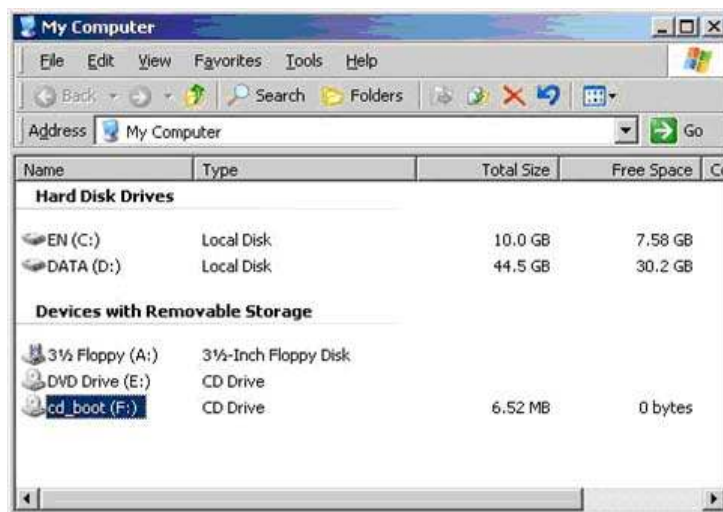
Share folder name: storage

Image file name: Cdrom_image.iso

User name: fae

Password: not displayed

... open the remote console and you can see the virtual CD as pictured below



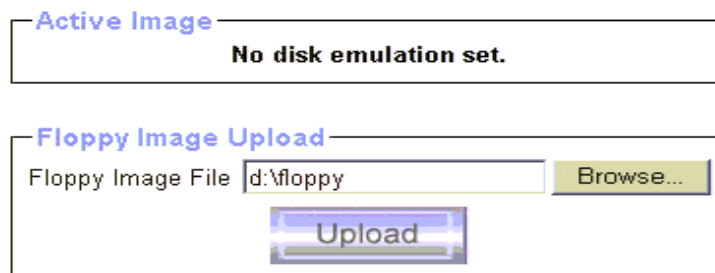
5.2.4 Floppy Disk



Figure 5-8 Virtual Media - Floppy Disk

Operation Procedures

- You need to create the floppy image file first (Please refer to the section “Creating a floppy image”). For this example, we use *RawWrite* software (or any other image-creator software) to create floppy image. Locate where the image file you create is saved
- Open the browser to log into the IP-KVM. Click **Virtual Media** and select **Floppy Disk**
- Click the **Browse** button to choose the image file

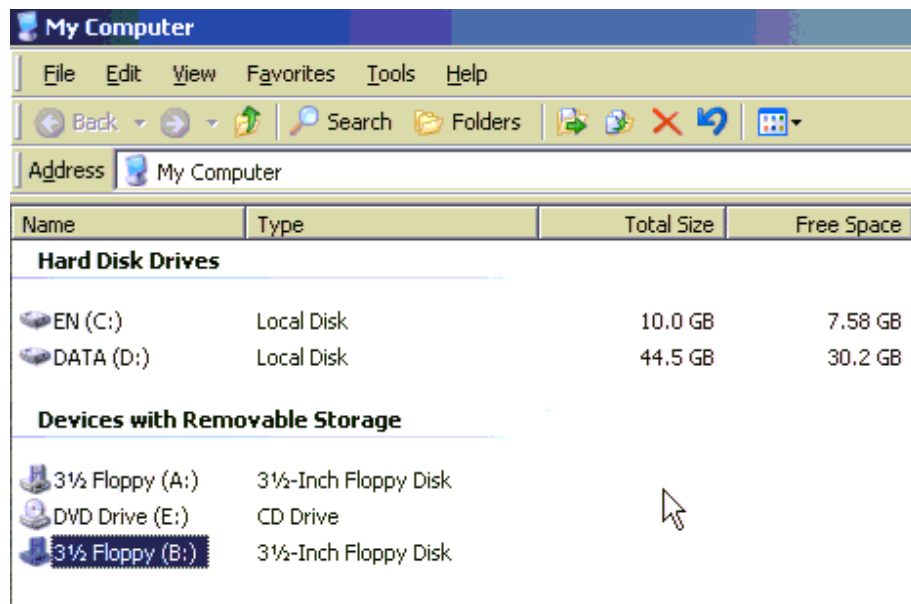


- Click on the button **Upload** to initiate the transfer of the chosen image file into the IP-KVM module’s on-board memory. After you uploading the image file, you will see the information below

Floppy image uploaded successfully.



- Open the remote console and you will see a virtual Floppy drive is created on the host computer that connect to IP-KVM



You may create a floppy image size up to 1.44Mb. 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 supporting USB BOOTABLE function. The maximum image size is limited to 1.44MB. To use a larger image mount this image via Windows Share (or SAMBA).

Notes:

1. If using other image-creator software, the output image extension file name has to be 'img', e.g. *floppy_vir.img*.
2. The uploaded image file will be kept in the onboard memory of the IP-KVM until the end of the current session, as you logged out, or initiated a reboot of the IP-KVM.

5.2.5 Creating an Image

5.2.5.1 Creating a Floppy Image

For Windows

You can use the tool “Raw Write for Windows”. You can get the *RawWrite* software from the website <http://www.chrysocome.net/rawwrite>.

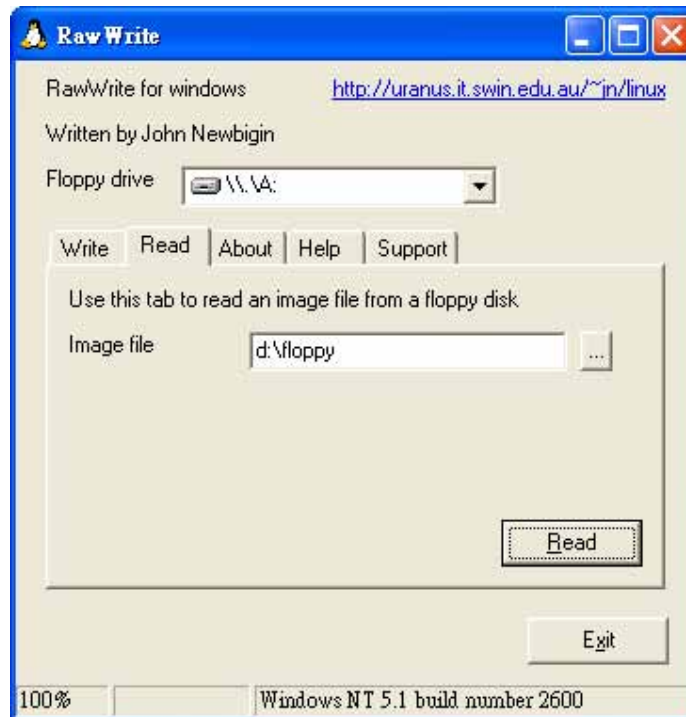


Figure 5-9 RawWrite for Windows selection dialog

From the menu, select the tab “Read”. Enter (or choose) the name of the file in which you would like to save the floppy content. Click on the button “Copy” to initiate the image creation process.

For UNIX and UNIX-like OS

To create an image file, make use of “dd”. This is one of the original UNIX utilities and is included in every UNIX-like OS (UNIX, Sun Solaris, and Linux).

To create a floppy image file, copy the contents of a floppy to a file. You can use the following command:

```
dd [ if=/dev/fd0 ] [ of=/tmp/floppy.image ]
```

dd reads the entire disc from the device `/dev/fd0`, and saves the output in the specified output file `/tmp/floppy.image`. Adjust both parameters exactly to your needs (input device etc.)

5.2.5.2 Creating a CD/DVD ISO Image

For Windows

To create the image file, use your favorite CD imaging tool. Copy the whole contents of the disc into one single image file on your hard disk.

For example, with “Nero” you choose “Copy and Backup”. Then, navigate to the “Copy Disc” section. Select the CD-ROM or DVD drive you would like to create an image from. Specify the filename of the image, and save the CD-ROM content in that file.



Figure 5-10 Nero selection dialog

For UNIX and UNIX-like OS

To create an image file, make use of “dd”. This is one of the original UNIX utilities and is included in every UNIX-like OS (UNIX, Sun Solaris, and Linux).


To create a CD-ROM image file, copy the contents of the CD-ROM to a file. You can use the following command:

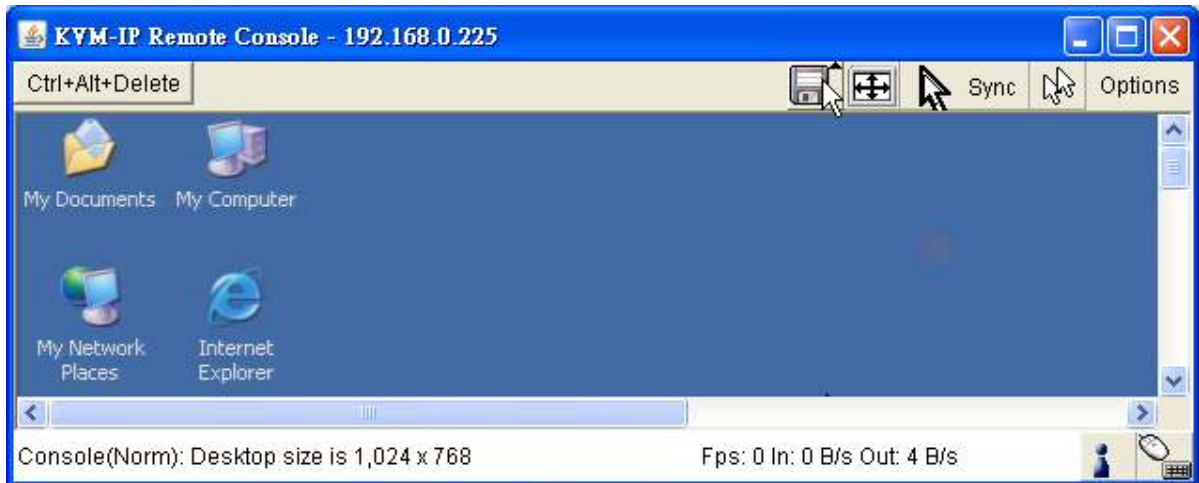
```
dd [ if=/dev/cdrom ] [ of=/tmp/cdrom.image ]
```

dd reads the entire disc from the device `/dev/cdrom`, and saves the output in the specified output file `/tmp/cdrom.image`. Adjust both parameters exactly to your needs (input device etc.).

5.2.6 Making a Drive Redirection

The operation procedures to make a drive redirection are as follows.

- Click **Remote Control** and select **KVM Console**
- Click on the *Floppy* icon 



You will see the Driver Redirection window as below:

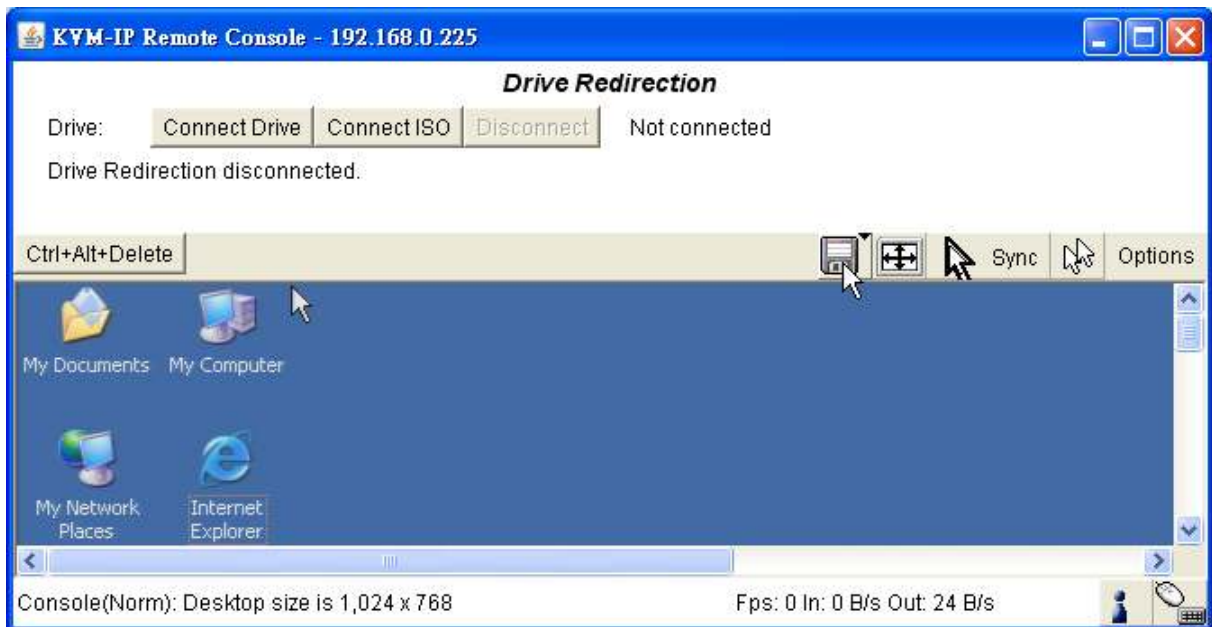
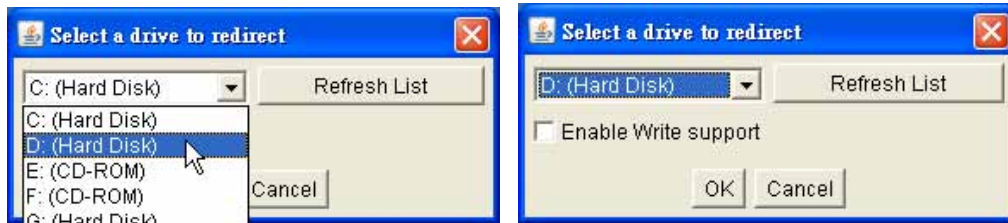


Figure 5-11 Built-in Java Drive Redirection

You can either redirect a local drive (only available under Windows) or redirect an ISO CD/DVD image.

- click on **Connect Drive** and elect the drive to be redirected
- click **OK**



Select the drive you would like to redirect. All available devices (drive letters) are shown here. Please note that the whole drive is shared with the remote computer, not only one partition. If you have a hard disc with more than one partition all drive letters that belong to this disc will be redirected. The Refresh button may be used to regenerate the list of drive letters, especially for an USB stick.



Please be cautious if “Allow Write Support” is selected. All data on the shared media can be destroyed

Write Support This feature may be enabled here. Write support means that the remote computer is allowed to write on your local drive. As you can imagine, this is very dangerous. If both the remote and the local system try to write data on the same device, this will certainly destroy the file system on the drive. Please use this only when you exactly know what you are doing.

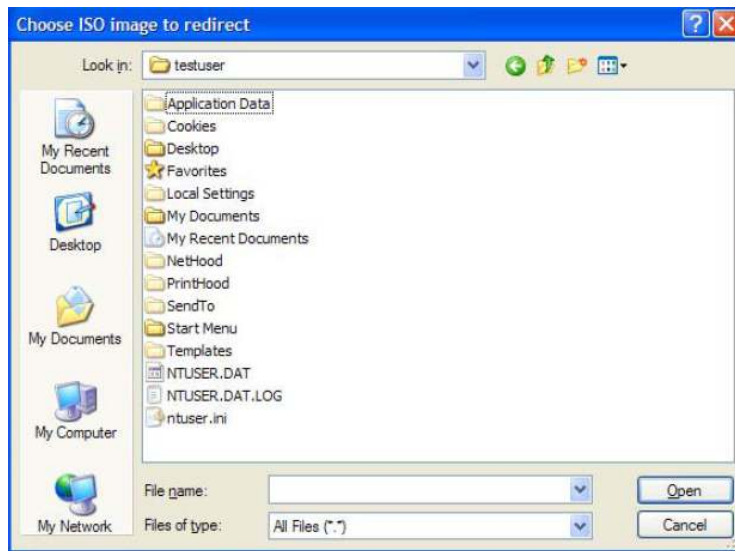
Device Authentication The factory default Username is “super” and the default Password is “pass”.

- click **Connect** to redirect drive

Note: Drive Redirection is only possible with Windows 2000 or later versions. The Drive Redirection works on a low SCSI level and the SCSI protocol cannot recognize partitions; therefore the whole drive selected will be shared instead of any particular partition.

While connecting to a legacy KVM switch, please select PS/2 mouse for **Keyboard/Mouse setting** from webpage. Otherwise you will not be able to use Hot-key.

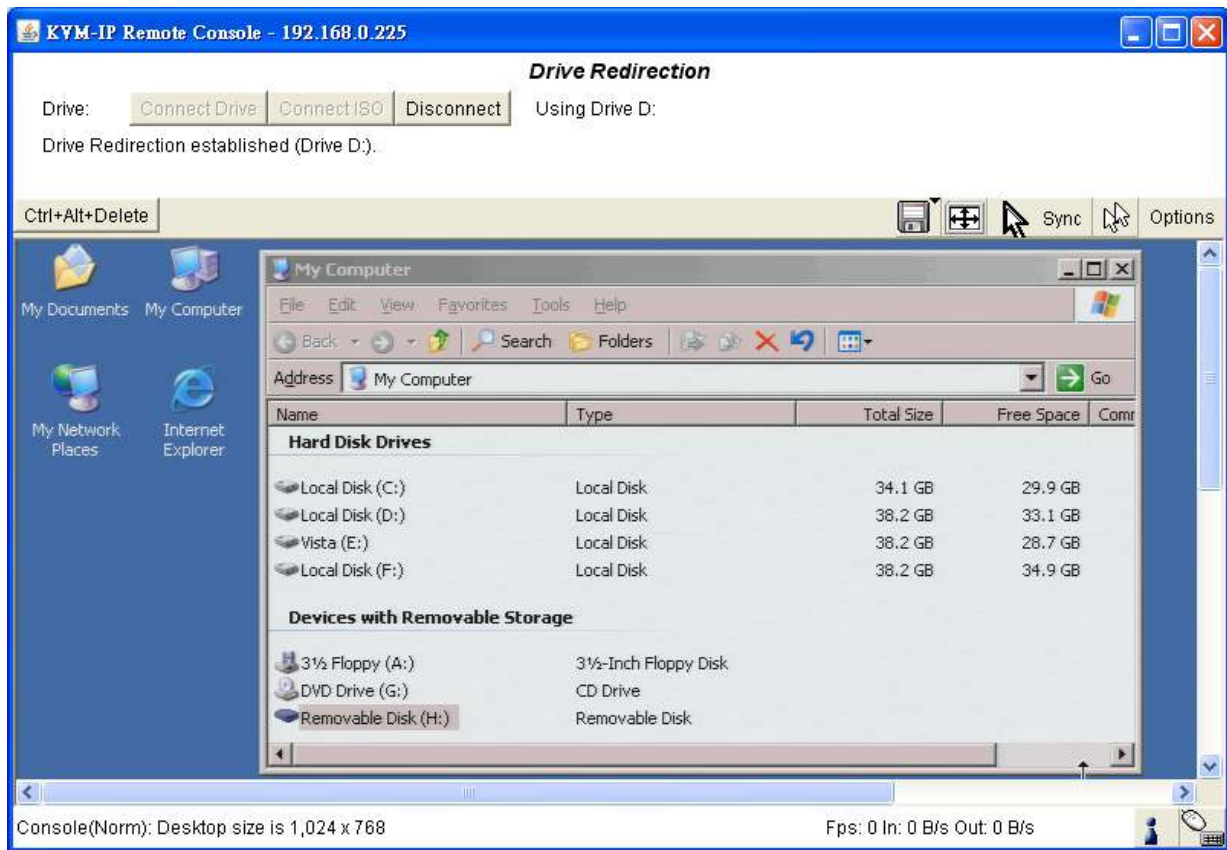
- click on **Connect ISO** then select the ISO image file and click **Open**



- the established Drive Redirection connection will now be displayed



- Open **My Computer** and you will see the virtual drive appears on the remote host PC window



The drive redirection software tries to lock the local drive before it is redirected. That means that it tries to prevent the local operating system from accessing the drive as long as it is redirected. This may also fail, especially if a file on the drive is currently open. In the case of a locking failure, you will be prompted if you want to establish the connection anyhow. This should not be a serious problem when the note above is respected. If the write support is enabled, a drive which is not locked might be damaged by the Drive Redirection.

- Clicking on the **Disconnect** button will disconnect the Drive Redirection connection.

Note: Virtual Drive creation is by Device manner not by Partition. Which means it looks for I/O in BIOS and sends the corresponding signal to host computer. This way, you are sending the entire hard drive (may consist of 'X' numbers of partitions) and emulate whatever number of partitions on host computer. You may also emulate a DVD-Drive with the same procedure. However, this DVD-Drive **Does NOT** support Bootable function like Floppy and CD-ROM emulation.

5.3 User Management

Each user on an IP-KVM 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

A currently logged in user can change their password:

- Click **User Management** and select **Change Password**



Figure 5-12 Setting Password

- Enter the current password In **Old Password**
- Enter the new password in **New Password**
- Re-type the new password for verification in **Confirm New Password**
- Click **Apply** to submit changes

5.3.2 Users and Groups

The screenshot shows a web interface titled "User Management". It contains the following elements:

- "Existing users" dropdown menu with a "Lookup" button.
- Text input fields for "New user name", "Full user name", "Password", "Confirm Password", "Email address", and "Mobile number".
- "Role" dropdown menu with "Administrator" selected.
- Checkbox labeled "Enforce user to change password on next login *".
- Three buttons at the bottom: "Create", "Modify", and "Delete".

The IP-KVM comes with one pre-configured user account that 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.

To create a new user:

- Enter details for the new user:

New User name The new user name for the selected account

Password The password for the login name (which must be 4 to 32 characters long)

Confirm password Confirmation of the password above

Email address This information may be optionally provided

Mobile number This information may be optionally provided

Role Each user can be a member of a group (named a "role"). There are three kinds of roles. *Super* has all possible rights to configure the device. *Administrator* has partial rights to change configuration apart from critical settings. *User* has permission to access basic function of open Remote Console. You can choose the desired level from the *Role* selection box

Note: The IP-KVM accepts 32 letters of username and password

- Click the **Create** button and the displayed new user profile settings will be saved

To modify the settings for an existing user:

- Select an **Existing user** and click the **Lookup** button to see the existing user profile
- Modify the user profile (e.g. Change **New User name, Password** etc)
- Click the **Modify** button and the displayed user profile settings will be saved

Note: The IP-KVM is equipped with an host-independent processor and memory unit which both have a limitation in terms of the processing instructions and memory space. To guarantee an acceptable response time we recommend not to exceed 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 to store 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 of the same group (role).

- Select the particular user from selection box and make the stting changes:

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 (Help)

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

* Stored value is equal to the default.

Figure 5-13 User Console Setting

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 is 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 colour depth for the indicated network speed.

Manually Allows to adjust both compression rate and the colour 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 Plugin

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 this JVM

versions and offers wider range of functionality when run in SUN's JVM. Please make sure that you are installing Sun JVM 1.5 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 to specify 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 or *Control+Backspace* on Unix or Unix-like OS. 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

Host Interface * active: USB

To use the *USB* and/or *PS/2* interface you need a correct cabling between the managed host and the managing device. If the managed host has no USB keyboard support in the BIOS and you have connected the USB cable only then you will have no remote keyboard access during the boot process of the host. If USB and PS/2 are both connected and you selected *Auto* as host interface then the card will choose USB if available or otherwise falls back to PS/2.

Keyboard Model *

Key release timeout enabled *

Timeout after msec *

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

USB Mouse Type *

Mouse speed Auto *

Fixed scaling : *

Absolute mouse scaling for MAC server *

* Stored value is equal to the default.

Figure 5-14 Keyboard and Mouse Settings

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

USB Mouse Type Enables USB mouse type. Choose between “Windows >= 2000 , MacOSX” for MS Windows 2000 or Windows XP, Mac OSX or “Other Operating Systems” for MS Windows NT, Unix or Unix-like OS, or OS X. In “Windows >= 2000 , MacOSX” mode the remote mouse is always synchronized with the local mouse.

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.

- Click **Apply** to set these options

5.4.3 Video



Figure 5-15 Video Settings

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.

- Click **Apply** to set these options

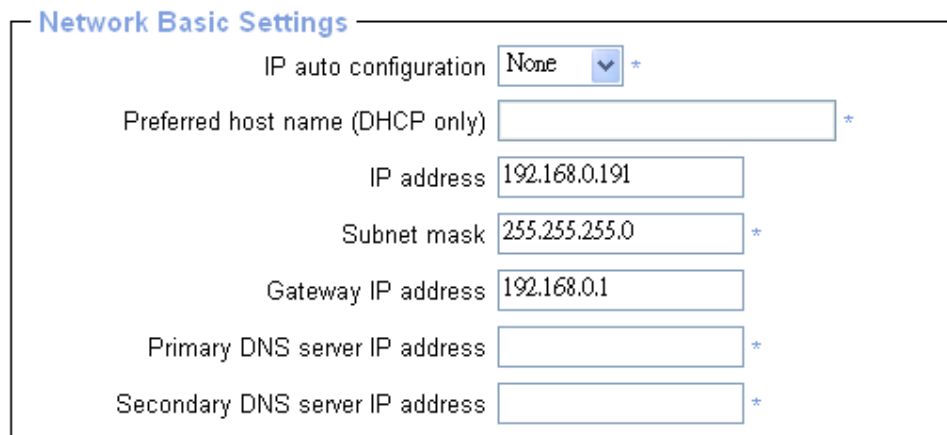
5.5 Device Settings



5.5.1 Network

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

- Select **Device Settings: Network** and under **Network Basic Settings** you can set new IP address or enable DHCP/BOOTP

A screenshot of the 'Network Basic Settings' panel. The panel has a title bar that says 'Network Basic Settings'. Below the title bar, there are several configuration fields. The first field is 'IP auto configuration' with a dropdown menu set to 'None' and an asterisk to its right. The second field is 'Preferred host name (DHCP only)' with an empty text box and an asterisk to its right. The third field is 'IP address' with a text box containing '192.168.0.191'. The fourth field is 'Subnet mask' with a text box containing '255.255.255.0' and an asterisk to its right. The fifth field is 'Gateway IP address' with a text box containing '192.168.0.1'. The sixth field is 'Primary DNS server IP address' with an empty text box and an asterisk to its right. The seventh field is 'Secondary DNS server IP address' with an empty text box and an asterisk to its right.

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

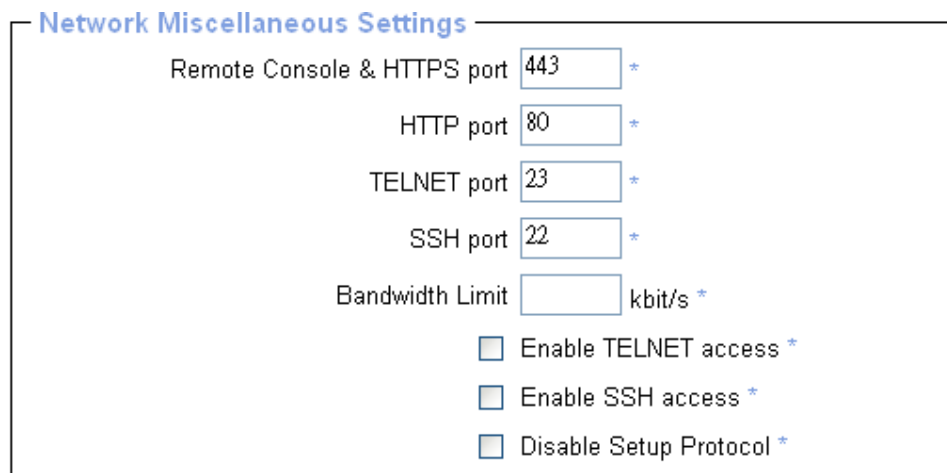
Subnet Mask The net mask of the local network

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

- Under **Network Basic Settings** you can set the ports that are to be used by the various TCP/IP services



The screenshot shows a configuration window titled "Network Miscellaneous Settings". It contains several input fields and checkboxes:

- Remote Console & HTTPS port: 443 *
- HTTP port: 80 *
- TELNET port: 23 *
- SSH port: 22 *
- Bandwidth Limit: [] kbit/s *
- Enable TELNET access *
- Enable SSH access *
- Disable Setup Protocol *

Figure 5-16 Network Settings

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

- Under **LAN Interface Settings** the **Autodetect** will set the ethernet speed to the fastest possible value supported by both endpoints of the link.

The screenshot shows a configuration window titled "LAN Interface Settings". At the top, it displays "Current LAN interface parameters: autonegotiation on, 100 Mbps, full duplex, link ok". Below this, there are two dropdown menus: "LAN interface speed" and "LAN interface duplex mode", both currently set to "Autodetect" with a small asterisk to the right of each. At the bottom of the panel are two buttons: "Apply" and "Reset to defaults". Below the buttons, a note reads: "* Stored value is equal to the default."

For example if you use a 10Mb half duplex HUB this speed will be auto-selected. If this option does not work with some network device (HUB, switches, and routers), you can set the Ethernet interface speed of IP-KVM manually to the values as supported by the network device

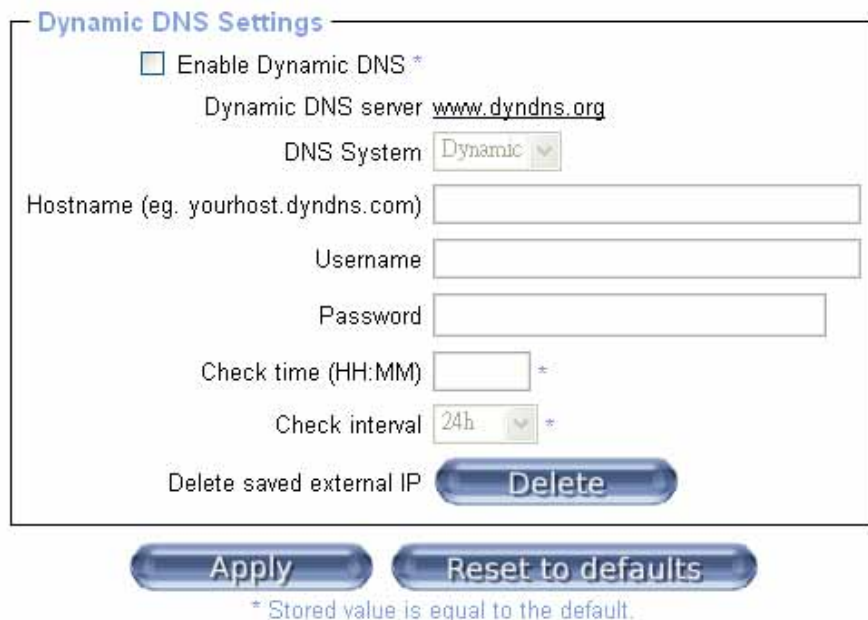
NOTE: Changing the network settings of the IP-KVM might result in losing connection to it. In case you change the settings remotely make sure that all the values are correct and you still have an option to access the IP-KVM.

5.5.2 Dynamic DNS

When users connect their IP-KVM to a DSL line or use a DHCP configuration, their IP address might be changed whenever it reconnects to the network. So it can become very difficult to post all related contacts for each new IP address. Also if the remote administrator only has access through the remote console they have no way to know if an IP-KVM IP address has changed and if it has what the new IP address is.

The solution is the Dynamic DNS service which is provided by various ISPs and organizations. Using the Dynamic DNS service users can access the IP-KVM through the hostname registered in the Dynamic DNS Server regardless of any IP address change.

The remote administrator does not know the IP address assigned by the provider, however the IP-KVM connects to the dynamic DNS server in regular intervals and registers its IP address there. So the administrator can contact this server as well and pick up the same IP address relating to his IP-KVM unit.



The image shows a web-based configuration interface titled "Dynamic DNS Settings". It contains the following elements:

- An unchecked checkbox labeled "Enable Dynamic DNS *".
- A text field for "Dynamic DNS server" containing the value "www.dyndns.org".
- A dropdown menu for "DNS System" with "Dynamic" selected.
- A text input field for "Hostname (eg. yourhost.dyndns.com)".
- A text input field for "Username".
- A text input field for "Password".
- A text input field for "Check time (HH:MM)" with a "+" button to its right.
- A dropdown menu for "Check interval" with "24h" selected and a "+" button to its right.
- A button labeled "Delete" next to the text "Delete saved external IP".
- At the bottom, two large buttons: "Apply" and "Reset to defaults".
- A small note below the buttons: "* Stored value is equal to the default."

Figure 5-17 Dynamic DNS

By default the IP-KVM supports Dynamic DNS service offered at Dynamic DNS Network Services, LLC (www.dyndns.org). To use these services the user must set up an account in their Members' NIC (Network Information Center (<http://members.dyndns.org>)).

The administrator has to register an IP-KVM that is supposed to take part in the DDNS service with the Dynamic DNS Server and assign a certain hostname to it. They will then 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

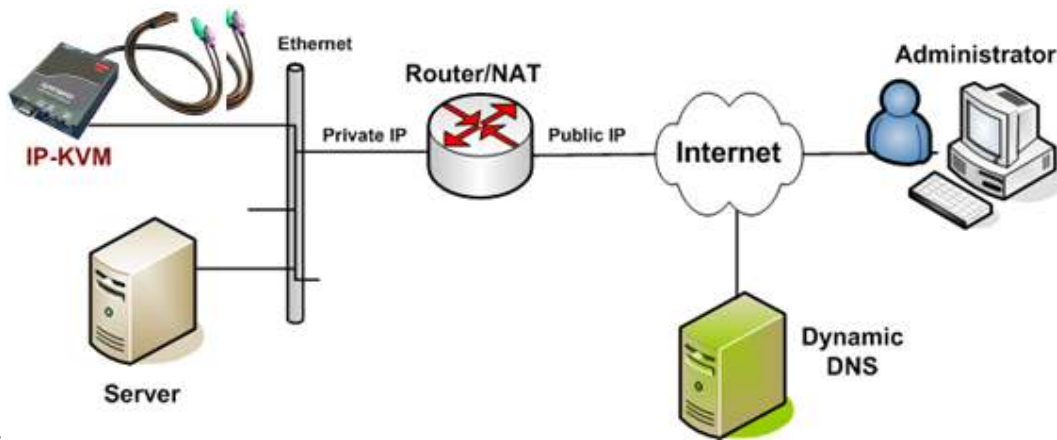


Figure 5-18 Dynamic DNS Scenario

To enable Dynamic DNS:

- Select **Device Settings: Dynamic DNS**
- Make sure that the LAN interface of the IP-KVM is properly configured
- Enable Dynamic DNS and change the settings according to your needs (as shown in Figure 5.17):

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

The screenshot displays three configuration sections:

- HTTP Encryption:** A checkbox labeled "Force HTTPS for Web access" is currently unchecked.
- KVM Encryption:** Radio buttons for "Off" (selected), "Try", and "Force" are visible.
- Group based System Access Control:** A red warning message states "Please note: 'Apply' is required, or changes will be lost." Below it, a checkbox for "Enable Group based System Access Control" is unchecked. A "Default Action" dropdown menu is set to "ACCEPT".

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"/>

Buttons for "Append", "Insert", "Replace", "Delete", "Apply", and "Reset to defaults" are located below the table. A note at the bottom states: "* Stored value is equal to the default."

Figure 5-19 Device Security

HTTPS Encryption

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. (And if you want to create your own SSL certificate that is used to identify the IP-KVM refer the *Certificate* section in this manual

KVM encryption

This 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 which keeps unauthorized hosts from accessing to the IP-KVM by specifying IP filtering rules.

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 any particular Group level (All, User, Super or 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 as the packet will enter the chain Rule 1 first and if it meets the rule then it will take Action 1 directly; otherwise go to chain rule 2.

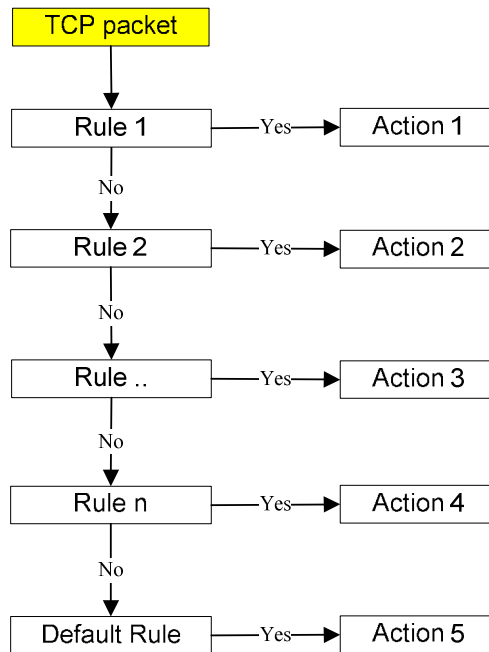


Figure 5-20 Chain Rules of IP Filtering

- Check the **Enable Group based System Access Control** to edit the rules
- 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**

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" value="2"/>	<input type="text" value="192.168.123.99"/>	<input type="text" value="192.168.123.230"/>	<input type="text" value="super"/>	<input type="text" value="ACCEPT"/>

* Stored value is equal to the default.

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" value="2"/>	<input type="text" value="192.168.123.99"/>	<input type="text" value="192.168.123.230"/>	<input type="text" value="super"/>	<input type="text" value="ACCEPT"/>

* Stored value is equal to the default.

Figure 5-21 IP Filter Settings

5.5.4 Certificate

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 that comes with the 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.



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) *

Create

* Stored value is equal to the default.

Figure 5-22 Certificate Settings

In order to do that, the IP-KVM must be enabled 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.

To create and install a SSL certificate for the IP-KVM:

- Create a SSL Certificate Signing Request using the panel shown in Figure 5.22. To do this you will need to fill out a number of fields as explained below.

Common name This is the network name of the IP-KVM once it is installed in the user's network (usually the fully qualified domain name). It is identical to the name that is used to access the IP-KVM with a web browser (without the "http://" prefix). In

case the name given here and the actual network name differ, the browser will pop up a security warning when the IP-KVM is accessed using HTTPS

Organizational unit This field is used for specifying to which department within an organization the IP-KVM belongs

Organization The name of the organization to which the IP-KVM belongs

Locality/City The city where the organization is located

State/Province The state or province where the organization is located

Country (ISO code) The country where the organization is located. This is the two-letter ISO code, e.g. DE for Germany, or US for the USA. (Note: the country code has to be entered in CAPITAL LETTERS)

Challenge Password Some certification authorities require a challenge password to authorize later changes on the certificate (e.g. revocation of the certificate). The minimal length of this password is 4 characters

Confirm Challenge Password Confirmation of the Challenge Password

Email The email address of a contact person that is responsible for the IP-KVM and its security

Key length This is the length of the generated key in bits. 1024 Bits are supposed to be sufficient for most cases. Longer keys may result in slower response time of the IP-KVM during connection establishment

- Once this is done, click on the button **Create** which will initiate the Certificate Signing Request generation. The CSR can be downloaded to your administration machine with the **Download CSR** button
- Send the saved CSR string to a CA for certification. You will get the new certificate from the CA after a more or less complicated traditional authentication process (depending on the CA)
- Upload the certificate to the IP-KVM using the **Upload** button as shown below

Certificate Signing Request (CSR)

The following CSR is pending:

countryName	=	TW
stateOrProvinceName	=	taipei
localityName	=	taipei
organizationName	=	test org
organizationalUnitName	=	test
commonName	=	test
emailAddress	=	test@test.com

Download
Delete

Certificate Upload

SSL Certificate File Browse...

Upload

Figure 5-23 SSL Certificate Upload

Home
Console
Logout

```

-----BEGIN CERTIFICATE REQUEST-----
MIIBIDCCATOCAQAvfjELMAkGA1UEBhMCVFcxDzANBgNVBAGTBnRhaXBlaTEPMAAG
A1UEBzMGdGFpcG9pMREwDwYDQKKEwhOZXRNOIG9yZzENMAsGA1UECzMEdGVzZDEN
MA8GA1UEAxMEdGVzZDEcMB0cCqQSS1b3DQEJARYNAGVz4EB0ZCN0LmNvTCBnzAN
BgkqhkiG9w0BAQEPAAOBjQAvgYkCgYEAu93rTI0bu4MVKsATZzSLp5Oymdnjwi4c
Np4w0Urgqymwzsg6Cmb5JMVe2T33UN/acRjyx7KfXY1+s++9++k+kaKRvZyjt7HE
IuMU1X2xy1F78EvFRmORu+YV0e9zd29Wa5Z5bqz9QeLLVqczDk8F06jBDMqaj9u
dR0hMR//X50CAwEAAaAWMBQCQSQS1b3DQEJzEHEWUzNM)MONTANBgkqhkiG9w0B
AQQFAA0BgQBD60ZD6hflJd4CDa3k2QU0h0lycehIosw4AMZrSrn1u5a1YTI915+
2Ra0URAlQoTryn1kUZZNFjBDum38R3WzNVmZp3uehBaD8yEXQmNT08BU10nlf
4596mg137W4Uz2YEgLTejw5FYgnd1JkM3ya/sge0DrcH13kDTg==
-----END CERTIFICATE REQUEST-----

```

Figure 5-24 CSR string

After completing these three steps, the IP-KVM has its own certificate that is used for identifying the IP-KVM to its clients.



If you destroy the CSR on the IP-KVM there is no way to get it back! In case you deleted it by mistake, you have to repeat the three steps as described above

5.5.5 Serial Port

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

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"/>

* Stored value is equal to the default.

Figure 5-25 Serial Port

Configuration or console login Do not use the serial port for any special function, use it only for the initial configuration

Modem The IP-KVM offers remote access using a telephone line in addition to the standard access over the built-in Ethernet adapter. The modem needs to be connected to the serial interface of the IP-KVM.

Logically, connecting to the IP-KVM using a telephone line means nothing else than building up a dedicated point-to-point connection from your console computer to the IP-KVM. So the IP-KVM acts as an Internet Service Provider (ISP) to which you can dial in. The connection is established using the Point-to-Point Protocol (PPP). Before you connect to the IP-KVM, make sure to configure your console computer accordingly. For instance, on Windows based operating systems you can configure a dial-up network connection, which defaults to the right settings like PPP.

The Modem Settings panel allows you to configure the remote access to the IP-KVM using a modem. The meaning of each parameter will be described below. The modem settings are part of the serial settings panel.

Serial line speed

The speed the IP-KVM is communicating with the modem. Most modern modems will support the default value of 115200 bps. If you are using an old modem and have problems try lowering this speed

Modem Init String

The initialization string used by the IP-KVM to initialize the modem. The default value will work with all modern standard modems directly connected to a telephone line. In case you have a special modem or the modem is connected to a local telephone switch that requires a special dial sequence in order to establish a connection to the public telephone network, you can change this setting by giving a new string. (Refer to the modem's manual about the AT command syntax.)

Modem server IP address

This IP address will be assigned to the IP-KVM itself during the PPP handshake. Since it is a point-to-point IP connection virtually every IP address is possible but you must make sure, it is not interfering with the IP settings of the IP-KVM and your console computer. The default value will work in most cases.

Modem client IP address

This IP address will be assigned to your console computer during the PPP handshake. Since it is a point-to-point IP connection virtually every IP address is possible but you must make sure, it is not interfering with the IP settings of the IP-KVM and your console computer. The default value will work in most cases.

Pass-through access to serial port via Telnet

Using this option, it is possible to connect an arbitrary device to the serial port and access it (assuming it provides terminal support) via Telnet. Select the appropriate options for the serial port and use the Telnet Console or a standard Telnet client to connect to the IP-KVM.

5.5.6 Date / Time

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.

This link enables you to set up the internal real-time clock of the IP-KVM. You have the possibility to adjust the clock manually, or to use a NTP timeserver:

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.

Figure 5-26 Date / Time

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

The common way to log events is to use the internal log list of the IP-KVM. These logs can be viewed by selecting **Event Log** on the **Maintenance** page menu. To configure the event logs:

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 *
Community *

[Click here to view the KVM-IP SNMP MIB](#)

Event Log Assignments

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

* Stored value is equal to the default.

Figure 5-27 Event Log

- Select **Device Settings: Event Log**

- You can choose how many log entries are shown on each page. Furthermore, you can clear the log file and specify the extent of the logging:

List logging enabled 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.

Since the IP-KVM's system memory is used to save all the information, the maximum number of possible log list entries is restricted to 1,000 events. Every entry that exceeds this limit overrides the oldest one, automatically.

If the reset button on the HTML frontend is used to restart the IP-KVM, all logging information is saved permanently and is available after the IP-KVM has been started. If the IP-KVM loses power or a hard reset is performed, all logging data will be lost. To avoid this, use one of the following log methods:

NFS Logging enabled

Define a NFS server, where a directory or a static link have to be exported, to write all logging data to a file that is located there. To write logging data from more than one IP-KVM devices to only one NFS share, you have to define a file name that is unique for each device. When you change the NFS settings and press the button **Apply**. The NFS share will be mounted immediately. That means, the NFS share and the NFS server must be filled with valid sources or you will get an error message.

SMTP Logging enabled

With this option, the IP-KVM is able to send Emails to an address given by the Email address text field in the Event Log Settings. These mails contain the same description strings as the internal log file and the mail subject is filled with the event group of the occurred log event. In order to use this log destination you have to specify a SMTP server, that has to be reachable from the IP-KVM device and that needs no authentication at all (<serverip>:<port>).

SNMP Logging enabled

If this is activated, the IP-KVM sends a SNMP trap to a specified destination IP address, every time a log event occurs. If the receiver requires a community string, you can set it in the appropriate text field. Most of the event traps only contain one descriptive string with all information about the log event. Only authentication and host power events have an own trap class that consists of several fields with detailed information about the occurred event. To receive this SNMP traps, any SNMP trap listener may be used.

Here is a example of all generated event and its event group:

Device succesfully started	device
Board Reset performed by user...	device

Firmware upload failed.	device
No firmware file uploaded.	device
Uploaded firmware file discarded.	device
Firmware validation failed.	device
Firmware file uploaded by user...	device
Firmware updated by user...	device
Internal log file cleared by user...	device
Security Violation	security
Host Power	host
Host Reset	host
Connection to Remote Console failed: reason.	console (several)
Connection to client ... established.	console
Connection to client ... closed.	console
Login failed.	auth
Login succeed.	auth

Note: In contrast to the internal log file on the IP-KVM, the size of the NFS log file is not limited. Every log event will be appended to the end of the file so it grows continuously and you may have to delete it or move it away from time to time

5.5.8 Authentication

To log in to the IP-KVM a user must be authenticated by means of a password. By default this authentication takes place locally with the user name and associated password being stored in the IP-KVM's internal database.

Alternately the IP-KVM can be configured to query a remote database server using RADIUS or LDAP to determine if a given user may log in.

To configure authentication settings:

- Select **Device Settings: Authentication** and check **Local Authentication** , **LDAP** or **Radius**

Local Authentication

When Local Authentication is selected, the IP-KVM will authenticate against its internal database of users and passwords

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"/>

* Stored value is equal to the default.

LDAP Access

When you select LDAP Authentication, the IP-KVM will communicate with a Microsoft Active Directory or generic LDAP server for user authentication (i.e. password verification). The user profile must be set up in the local database as described in Local User Management, but no password is stored locally. When a user attempts to log in, the IP-KVM contacts the specified LDAP server, which will either approves or denies access

In order to configure the IP-KVM for LDAP access:

➤ Check **LDAP** and enter details for:

User LDAP Server Enter the name or IP address of the LDAP server containing all the user entries. If you choose a name instead of an IP address you need to configure a DNS server in the network settings. E.g.: 192.168.1.250

Base DN of User LDAP Server Specify the distinguished name (DN) where the directory tree starts in the user LDAP server. E.g.: dc=test, dc=domain, dc=com

Type of external LDAP Server With this option you set the type of the external LDAP server. This is necessary since some server types require special handling. Additionally, the default values for the LDAP scheme are set appropriately. You can choose between a Generic LDAP Server, a Novell Directory Service and a Microsoft Active Directory. If you have neither a Novell Directory Service nor a Microsoft Active Directory then choose a Generic LDAP Server and edit the LDAP scheme used (as detailed below)

Name of login-name attribute This is the name of the attribute containing the unique login name of a user. To use the default leave this field empty. The default depends on the selected

LDAP server type

Name of user-entry object class This is the object class that identifies a user in the LDAP directory. To use the default leave this field empty. The default depends on the selected LDAP server type

User search subfilter Here you can refine the search for users that should be known to the IP-KVM

Active Directory Domain This option represents the active directory domain that is configured in the Microsoft Active Directory server. This option is only valid if you have chosen a Microsoft Active Directory as the LDAP server type e.g.: test.domain.com

RADIUS Access

RADIUS (Remote Authentication Dial In User Service) is a protocol specified by the Internet Engineering Task Force (IETF) working group. There are two specifications that make up the RADIUS protocol suite: Authentication and Accounting. These specifications aim to centralize authentication, configuration and accounting for dial-in services to an independent server. The RADIUS protocol exists in several implementations (such as freeRADIUS, openRADIUS or RADIUS on UNIX systems). The RADIUS protocol itself is well specified and tested.

Note: The IP-KVM currently does not support challenge/response. An Access Challenge response is seen and evaluated as an Access Reject.

To configure the IP-KVM to use the RADIUS protocol.

➤ Check **RADIUS** and enter details for:

Server Enter the name or IP address of the RADIUS server, reachable by the IP-KVM over the network. (Configure a DNS server if a name rather than an address is used.)

Shared Secret A shared secret is a text string that serves as a password between the RADIUS client and RADIUS server. In this case the IP-KVM acts as a RADIUS client. A shared secret is used to verify that RADIUS messages are sent by a RADIUS-enabled device that is configured with the same shared secret and to verify that the RADIUS message has not been modified in transit (message integrity). Enter a maximum of 128 alphanumeric characters and symbols such as an exclamation point ("!") or an asterisk ("*")

Auth. Port The authentication port the RADIUS server listens for authentication requests (default value **1812**)

Acc. Port The accounting port the RADIUS server listens for accounting requests. The default value is **1813**

Timeout This sets the request time-to-live in seconds. The time-to-live is the time to wait for the completion of the authentication request. If the request job is not completed within this interval of time it is cancelled. The default value is **1** second

Retries Sets the number of retries if a request could not be completed. The default value is **3** times

- Click **Apply** to save the new authentication configuration

When RADIUS has been selected and configured the IP-KVM communicates with a RADIUS server for user authentication. To access:

- Log in with a name and password and the IP-KVM will contact the RADIUS server for authentication. The RADIUS server reads your input data (Authentication) and the IP-KVM looks for your profile (Authorization). The profile defines (or limits) your actions and may differ depending on your specific situation. If there is no such profile your access via RADIUS will be refused. The RADIUS implementation also has a timeout whereby if there is no activity for half an hour the connection to the IP-KVM will be terminated

5.5.9 USB

USB 2.0 is the default setting. However 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

- Click **Backup** to save a copy of the IP-KVM config file in a file (config.gz) on your computer



- Click **Restore** to upload a saved config file

Device Configuration

Configuration Restore

Configuration Backup [Click here to download the configuration file.](#)

5.5.11 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"/> *

* Stored value is equal to the default.

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.

LDAP Access

The IP-KVM uses LDAP only for authentication (password verification). User privileges and private settings are still stored locally at the IP-KVM. That's why a user account has to be created on the IP-KVM before this user can login via LDAP. Also, all privilege configurations have to be done within the IP-KVM user management.

In order to configure the LDAP access, you can set the following options:

User LDAP Server

Here you enter the name or IP address of the LDAP server containing all the user entries. If you choose a name instead of an IP address you need to configure a DNS server in the network settings e.g. 192.168.1.250

Base DN of User LDAP Server

Here you specify the distinguished name (DN) where the directory tree starts in the user LDAP server e.g. dc=test,dc=domain,dc=com

Type of external LDAP Server

With this option you set the type of the external LDAP server. This is necessary since some server types require special handling. Additionally, the default values for the LDAP scheme are set appropriately. You can choose between a Generic LDAP Server, a Novell Directory Service and a Microsoft Active Directory. If you have neither a Novell Directory Service nor a Microsoft Active Directory then choose a Generic LDAP Server and edit the LDAP scheme used (see below)

Name of login-name attribute

This is the name of the attribute containing the unique login name of a user. To use the default leave this field empty. The default depends on the selected LDAP server type

Name of user-entry object class

This is the object class that identifies a user in the LDAP directory. To use the default leave this field empty. The default depends on the selected LDAP server type

User search sub-filter

Here you can refine the search for users that should be known to the IP-KVM

Active Directory Domain

This option represents the active directory domain that is configured in the Microsoft Active Directory server. This option is only valid if you have chosen a Microsoft Active Directory as the LDAP server type e.g. *test.domain.com*

5.6 Maintenance

The administrator performs various maintenance activities on the IP-KVM including viewing the status, updating firmware, viewing the event log and resetting the unit.



5.6.1 Device Information

The Device Information 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: KVM-IP
Server Name: KVM Server
Serial Number: ABC00001
Board ID: 0623d9013448456a
Device IP Address: 192.168.0.220
Device MAC Address: 00:22:e4:00:00:0f
Firmware Version: 04.02.00
Firmware Build Number: 6302
Firmware Description: Standard_101_090423
Hardware Revision: 0x15

[View the datafile for support.](#)

Connected Users

super (192.168.0.98) RC active
super (192.168.0.30) 15 min idle

Figure 5-28 Device Information

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.

Connected Users

test (62.238.0.39)	active
test (80.145.25.183)	26 min idle
test (212.183.10.29)	20 min idle
test (62.153.241.228) RC (exclusive)	active

Figure 5-29 Connected Users

Connected Users displays the IP-KVM user activity. From left to right it displays:

- the connected user
- the user's IP address (from which host the user comes from)
- its activity status is displayed (RC means that the Remote Console is open. If the Remote Console is opened in exclusive mode the term (exclusive mode) is added. For more information about this option see the *Remote Console Control Bar* section in this manual.)
- the last column contains either the term *active* for an active user or *30 min idle* for a user who is inactive for a certain amount of time.

5.6.2 Event log

The *Event Log* displays the log list including the events that are logged by the IP-KVM

Event Log			[Prev] [Next]
Date	Event	Description	
10/12/2007 07:26:07	Authentication	User 'super' logged in from IP address 220.135.171.106	
10/12/2007 00:07:54	Remote Console	Connection to client 59.120.210.87 closed.	
10/12/2007 00:06:19	Remote Console	Connection to client 59.120.210.87 established.	
10/12/2007 00:05:57	Authentication	User 'super' logged in from IP address 59.120.210.87	
10/12/2007 00:05:41	Remote Console	Connection to client 59.120.210.87 closed.	
10/12/2007 00:05:20	Remote Console	Connection to client 59.120.210.87 established.	
10/12/2007 00:04:39	Authentication	User 'demo' logged in from IP address 59.120.210.87	
10/11/2007 10:22:00	Remote Console	Connection to client 220.135.171.106 closed.	
10/11/2007 10:17:11	Remote Console	Connection to client 220.135.171.106 established.	
10/11/2007 10:16:46	Authentication	User 'demo' logged in from IP address 220.135.171.106	
10/11/2007 08:31:28	Remote Console	Connection to client 60.250.63.98 closed.	
10/11/2007 08:30:15	Remote Console	Connection to client 60.250.63.98 established.	
10/11/2007 08:29:56	Authentication	User 'super' logged in from IP address 60.250.63.98	
10/11/2007 08:29:16	Authentication	User 'super' logged in from IP address 60.250.63.98	
10/11/2007 07:06:54	Remote Console	Connection to client 60.250.63.98 closed.	
10/11/2007 07:00:15	Remote Console	Connection to client 60.250.63.98 established.	
10/11/2007 07:00:02	Authentication	User 'super' logged in from IP address 60.250.63.98	
10/11/2007 06:59:30	Remote Console	Connection to client 60.250.63.98 closed.	
10/11/2007 06:55:26	Remote Console	Connection to client 60.250.63.98 established.	
10/11/2007 06:55:20	Remote Console	Connection to client 60.250.63.98 closed.	

Figure 5-30 Event Log List

5.6.3 Update Firmware

Firmware can be easily upgraded via web page.

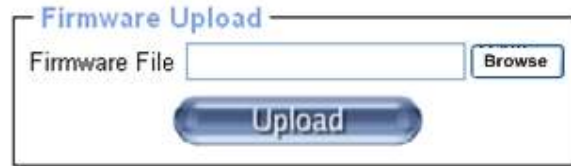


Figure 5-31 Update Firmware

The IP-KVM is a complete standalone computer. The software it runs is called *firmware* and this firmware can be updated remotely in order to install new functionality or special features.

A new firmware update is a binary file which will be sent to you by email or which you can download from the Opengera web site. If the firmware file is compressed (file suffix .zip) then you must unzip it before you can proceed. Under Windows you can use WinZip (<http://www.winzip.com>) or similar for decompression. Other operating systems might provide a program such as *unzip*.

Before you can start updating the firmware of your IP-KVM the new uncompressed firmware file has to be accessible on the system that you use for connecting to the IP-KVM.



This process is not reversible and will take few minutes. During this upgrading process you must not disconnect the power or the Ethernet cable as this may cause upgrade failure and destroy the image in Flash memory

The IP-KVM will automatically initiate a self-reboot upon completion of upgrade process to make newly upgraded firmware effective. At the end of countdown counter expires, the browser will redirect user to the login homepage. Users shall refer to *Maintenance: Device Information* page to check the firmware version and confirm the operation.



The IP-KVM will verify firmware checksum before proceed upgrade procedure. The mechanism helps to prevent false firmware files from damaging the IP-KVM. It also is crucial to keep a steady power supply during the procedure otherwise the power-off event may damage the permanent storage and disable the IP-KVM

Updating the firmware is a three-stage process:

- Upload the new firmware file onto the IP-KVM unit



In order to do that you need to select the file on your local system using the **Browse** button. Click **Upload**. Once the firmware file has been uploaded, it is checked whether it is a valid firmware file and whether there were any transmission errors. In case of any error the Upload Firmware function will be aborted.

- If everything went well, you see the *Update Firmware* panel

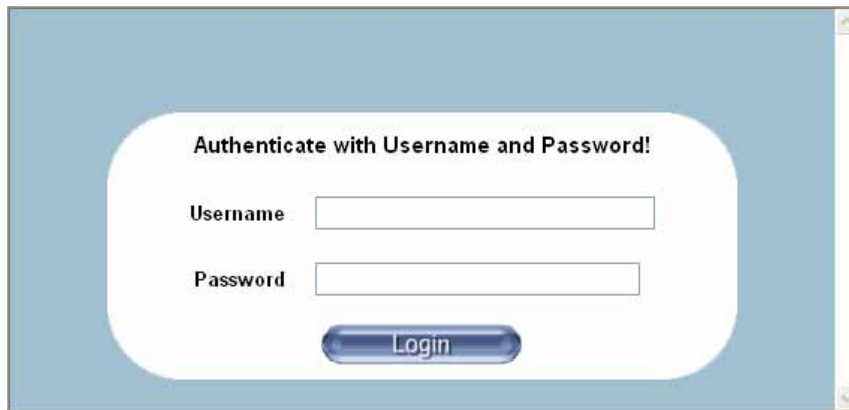


The panel shows you the version number of the currently running firmware and the version number of the uploaded firmware. Pressing **Update** will store the new version and substitute the old one completely

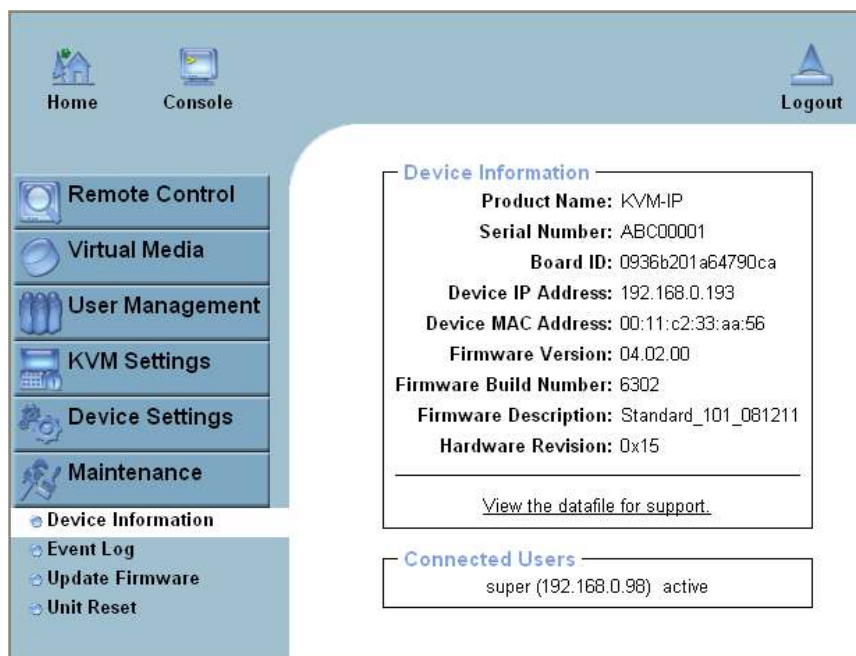
- You will be advised when the firmware has updated successfully



- The device will be rebooted and redirected to the login web page



- Log in to check out the **Device Information** to confirm the updated firmware is running



5.6.4 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.

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

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



Figure 5-32 Unit Reset

- To reset a certain IP-KVM functionality click on the appropriate **Reset** button. 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 sub-devices (e.g. video engine) will take few seconds only and does not result in closing connections.

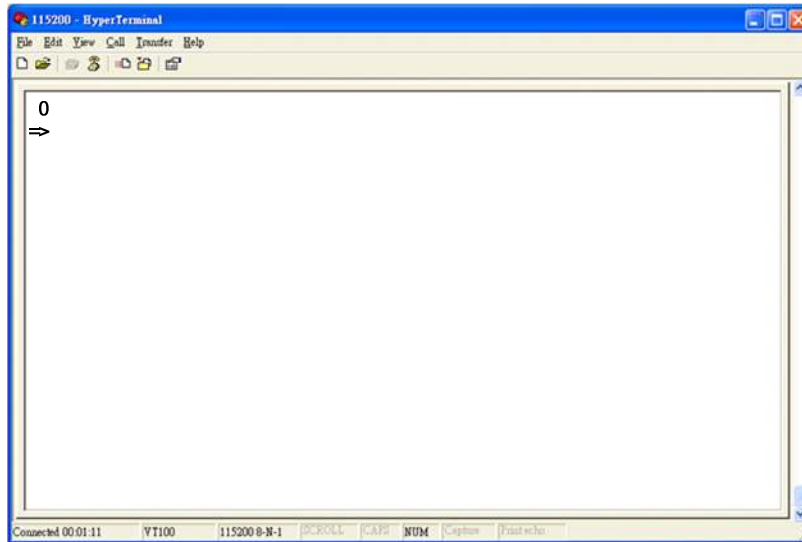
5.6.5 Reset to Factory Defaults

This function may be used when you forgot the password to log in the IP-KVM.

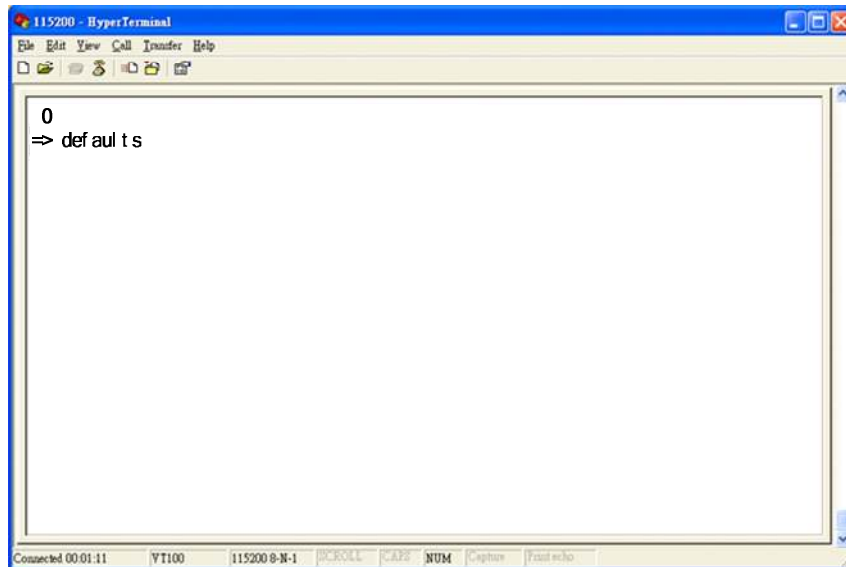
Note: The unit will reboot after this command. All current settings will be lost

The following procedures will revert to factory default settings:

- Connect a RS232 null modem cable from your local console PC to the IP-KVM Serial port. Configure your terminal emulation program (such as *HyperTerminal* or *PuTTY*) to the following settings: Baud rate **115200**, Data/stop bits **8-1**, Parity **none**, Flow control **none**.
- Enter the debugging mode via reboot the IP-KVM system and hit the ESC key. There are two ways to enter the debugging mode:
 - (a) Power cycle (reboot) the IP-KVM device. Within 2 seconds of booting the IP-KVM, enter the **Esc** key a few times to get a => prompt.
 - (b) Press & hold **ESC** AND push and release **Reset** button, and then release **ESC** in 2 seconds. The debugging mode window will display as below.



- Key in **defaults** command and then **Enter**. The unit will automatically set to factory default settings and reboot the system



- The following window displays if reverting to factory default is complete

```
115200 - HyperTerminal
File Edit View Call Transfer Help
[Icons]
0
=> defaults
Please wait ...
Installing default configuration ...
Writing configuration data to flash ...
Done.
Rebooting ...
Connected 00:01:11 VT100 115200 B-N-1 [SCROLL] [CAPS] NUM [Copy] [Print echo]
```


B. Video Modes

The table below lists the video modes IP-KVM supports. Please don't use other custom video settings besides of these or the IP-KVM may not be able to detect them.

Resolution (x, y)	Refresh Rates (Hz)
640 x 350	70, 85
640 x 400	56, 85
640 x 480	60, 72, 75, 85, 90, 100, 120
640 x 480	66.6
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, 76
1280 x 960	60, 85
1280 x 1024	60, 75, 85
1600 x 1200	60
2048 x 1536 (local console)	85

C. User Role Permissions

The table below lists the user role permissions granted for three user role groups (*Super*, *Administrator* and *User*).

Function	User	Administrator	Super
Remote Control: KVM	x	x	x
Remote Control: Remote Power	-	x	x
Remote Control: Telnet Console	x	x	x
Virtual Media	x	x	x
User Management: Change Password	x	x	x
User Management: Users	-	-	x
KVM Settings: User Console	x (w/o Misc. Settings)	x	x
KVM Settings: Keyboard/Mouse	-	x	x
KVM Settings: Video	-	x	x
Device Settings	-	-	x
Maintenance: Device Information	x	x	x
Maintenance: Event Log	-	-	x
Maintenance: Update Firmware	-	-	x
Maintenance: Unit Reset	Keyboard/ Mouse, Video	Keyboard/ Mouse, Video	Keyboard/ Mouse, Video, Device

D. Bandwidth Consumption

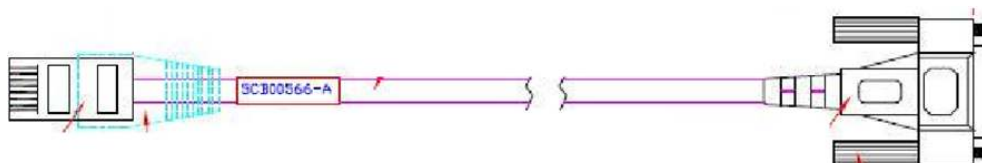
The preconfigured network speed selection simply results in different Compression and Color Depth configurations in order to match the different bandwidth limitations of the network type (UMTS, ISDN, etc.)

The following suggested network bandwidth planning table for IP-KVM installation is from the test results with 3D-Labyrinth screen saver at Resolution 800x600, the worst case consuming the highest network bandwidth.

	Compression	Color Depth	Used Bandwidth	Comment
Video Optimized	Video Optimized	8 bit	3.0 - 3.3 MB/s	uncompressed, synchronized video data, most bandwidth needed
Video Optimized (high color)	Video Optimized	16 bit	4.3 - 5.0 MB/s	uncompressed, synchronized video data, most bandwidth needed
LAN (high color)	0 (no compression)	16 bit	1.0 - 1.3 MB/s	uncompressed video data
LAN	0 (no compression)	8 bit	500 - 700 kb/s	uncompressed video data
DSL	2	8 bit	110 - 140 kb/s	slower video because of compression
UMTS	4	8 bit	80 - 100 kb/s	slower video because of compression
ISDN 128k	6	4 bit	20 - 30 kb/s	16 colors
ISDN/Modem V.90	7	2 bit	13 - 17 kb/s	gray scale
GPRS/HSCSD	8	2 bit	5 - 7 kb/s	gray scale
GSM Modem	9 (best compression)	1 bit	1 - 3 kb/s	black&white video

E. Pin-outs of RJ45-DB9F Cable

Signal	RJ45		DB9-Female (DCE)
DSR	1	←	4
+6 (DCD)	2	→	8
GND	3	----	5
TxD	4	→	2
RxD	5	←	3
DCD	6	→	1
CTS	7	←	7
DTR	8	→	6 +1 (DCD)



F. TCP/UDP Port Numbers

Port numbers are divided into three ranges: *Well Known Ports*, *Registered Ports* and *Dynamic and/or Private Ports*. Well Known Ports are those from 0 through 1023. Registered Ports are those from 1024 through 49151. Dynamic and/or Private Ports are those from 49152 through 65535.

Well Known Ports are assigned by IANA, and on most systems, can only be used by system processes or by programs executed by privileged users. Table below shows some of the well-known port numbers. For more details, please visit the IANA website:

<http://www.iana.org/assignments/port-numbers>

Port Number	Protocol	TCP/UDP
21	FTP (File Transfer Protocol)	TCP
22	SSH (Secure Shell)	TCP
23	Telnet	TCP
25	SMTP (Simple Mail Transfer Protocol)	TCP
37	Time	TCP, UCP
39	RLP (Resource Location Protocol)	UDP
49	TACACS, TACACS+	UDP
53	DNS	UDP
67	BOOTP server	UDP
68	BOOTP client	UDP
69	TFTP	UDP
70	Gopher	TCP
79	Finger	TCP
80	HTTP	TCP
110	POP3	TCP
119	NNTP (Network News Transfer Protocol)	TCP
161/162	SNMP	UDP
443	HTTPS	TCP

G. Protocol Glossary

Term	Meaning
BOOTP	Bootstrap Protocol is similar to DHCP, but for smaller networks. Automatically assigns the IP address for a specific duration of time.
CHAP	Challenge Handshake Authentication Protocol is a secure protocol for connecting to a system; it is more secure than the PAP.
DHCP	Dynamic Host Configuration Protocol is an Internet protocol for automating

	the configuration of computers that use TCP/IP.
DNS	Domain Name Servers is system that allows a network name server to translate text host names into numeric IP addresses.
LDAP	Lightweight Directory Access Protocol is a protocol for accessing directory information.
NAT	Network Address Translation is an Internet standard that enables a LAN to use one set of IP addresses for internal traffic and a second set of addresses for external traffic. This enables a company to shield internal addresses from the public Internet.
NFS	Network File System is a protocol that allows file sharing across a network. Users can view, store, and update files on a remote computer. You can use NFS to mount all or a portion of a file system. Users can access the portion mounted with the same privileges as the user's access to each file.
NTP	Network Time Protocol is a protocol used to synchronize time on networked computers and equipment.
PAP	Password Authentication Protocol is a method of user authentication in which the username and password are transmitted over a network and compared to a table of name-password pairs.
PPP	Point-to-Point Protocol is a protocol for creating and running IP and other network protocols over a serial link.
RADIUS	Remote Authentication Dial-In User Service is an authentication and accounting protocol. Enables remote access servers to communicate with a central server to authenticate dial-in users and their access permissions. A company stores user profiles in a central database that all remote servers can share.
SNMP	Simple Network Management Protocol is a protocol that system administrators use to monitor networks and connected devices and to respond to queries from other network hosts.
SMTP	Simple Mail Transfer Protocol is a TCP/IP protocol for sending email between servers.
SSL	Secure Sockets Layer is a protocol that provides authentication and encryption services between a web server and a web browser.
SSH	Secure Shell is a secure transport protocol based on public-key cryptography.
Telnet	A terminal protocol that provides an easy-to-use method of creating terminal connections to a network host.

H. Regulation Information

FCC This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a commercial 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. Operation of this equipment in a residential environment may cause harmful interference.

CE This equipment has been tested and found to comply with the CE regulations of Class A.

RoHS All contents of this package, including products, packing materials and documentation comply with RoHS.



I. Service and warranty

STANDARD WARRANTY

Opengear, Inc., its parent, affiliates and subsidiaries, (collectively, "Opengear") warrant your Opengear IP-KVM product to be in good working order and to be free from defects in workmanship and material (except in those cases where the materials are supplied by the Purchaser) under normal and proper use and service for the period of two (2) years from the date of original purchase from an Authorized Opengear reseller. In the event that this product fails to meet this warranty within the applicable warranty period, and provided that Opengear confirms the specified defects, Purchaser's sole remedy is to have Opengear, in Opengear's sole discretion, repair or replace such product at the place of manufacture, at no additional charge other than the cost of freight of the defective product to and from the Purchaser. Repair parts and replacement products will be provided on an exchange basis and will be either new or reconditioned. Opengear will retain, as its property, all replaced parts and products. Notwithstanding the foregoing, this hardware warranty does not include service to replace or repair damage to the product resulting from accident, disaster, abuse, misuse, electrical stress, negligence, any non- Opengear modification of the product except as provided or explicitly recommended by Opengear, or other cause not arising out of defects in material or workmanship. This hardware warranty also does not include service to replace or repair damage to the product if the serial number or seal or any part thereof has been altered, defaced or removed. If Opengear does not find the product to be defective, the Purchaser will be invoiced for said inspection and testing at Opengear's then current rates, regardless of whether the product is under warranty.

RMA RETURN PROCEDURE

If this product requires service during the applicable warranty period, a Return Materials Authorization (RMA) number must first be obtained from Opengear. Product that is returned to Opengear for service or repair without an RMA number will be returned to the sender unexamined. Product should be returned, freight prepaid, in its original or equivalent packaging, to:

Opengear Service Center
Suite A, 630 West 9560 South
Sandy, Utah 84070

Proof of purchase date must accompany the returned product and the Purchaser shall agree to insure the product or assume the risk of loss of damage in transit. Contact Opengear by emailing support@opengear.com for further information.

TECHNICAL SUPPORT

Purchaser is entitled to thirty (30) days free telephone support (USA ONLY) and twelve (12) months free e-mail support (world wide) from date of purchase provided that the Purchaser first register their product(s) with Opengear by filling in the on-line form:

<http://www.opengear.com/registration.html>.

Telephone support is only available from 9:00 AM to 5:00 PM, Mountain Time USA.

Opengear's standard warranty also includes free access to Opengear's Knowledge Base as well as any application notes, white papers and other on-line resources that may become available from time to time.

Opengear reserves the right to discontinue all support for products that are no longer covered by warranty.

LIMITATION OF LIABILITY

No action, regardless of form, arising from this warranty may be brought by either party more than two (2) years after the cause of action has occurred. Purchaser expressly agrees that Opengear's liability, if any, shall be limited solely to the replacement or repair of the product in accordance with the warranties specifically and expressly set forth herein. The remedies of the Purchaser are the exclusive and sole remedies available, and, in the event of a breach or repudiation of any provision of this agreement by Opengear, the Purchaser shall not be entitled to receive any incidental damages as that term is defined in Section 2-715 of the Uniform Commercial Code. Opengear waives the benefit of any rule that disclaimer of warranty shall be construed against Opengear and agrees that such disclaimers herein shall be construed liberally in favor of Opengear.

THE FOREGOING WARRANTIES ARE THE SOLE ANDEXCLUSIVE WARRANTIES GIVEN IN CONNECTION WITH THE PRODUCT AND THE HARDWARE. OPENGEAR DISCLAIMS ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, ANY WARRANTIES AS TO THE SUITABILITY OR MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. OPENGEAR DOES NOT PROMISE THAT THE PRODUCT IS ERROR-FREE OR WILL OPERATE WITHOUT INTERRUPTION. IN NO EVENT SHALL OPENGEAR BE LIABLE FOR ANY LOST

OR ANTICIPATED PROFITS, OR ANY INCIDENTAL, EXEMPLARY, SPECIAL OR CONSEQUENTIAL DAMAGES, REGARDLESS OF WHETHER OPENGear WAS ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.