



CAT.5 IP COMBO-KVM SWITCH 8-PORT/16-PORT



User Manual DS-15202-1 / DS-16202-1

Index

1.	INTRODUCTION.....	5
2.	SPECIFICATIONS	7
3.	SYSTEM REQUIREMENTS	8
4.	INSTALLATION	8
4.1.	FRONT VIEW.....	8
4.2.	REAR VIEW.....	9
4.3.	SINGLE STAGE INSTALLATION	9
4.3.1.	<i>Precaution:</i>	9
4.3.2.	<i>Console connection:</i>	10
4.3.3.	<i>System connection:</i>	10
4.4.	CASCADE CHAINING.....	12
4.5.	FIRMWARE DOWNLOAD CONNECTOR	14
4.6.	RACK MOUNTING	14
5.	OPERATION	14
6.	HOT KEY OPERATION	15
6.1.	CALL OSD MENU	15
6.2.	LEADING HOT KEY SELECT	15
6.3.	CHANNEL SELECT - SINGLE KVM.....	15
6.3.1.	<i>Specific channel selection</i>	15
6.3.2.	<i>Arrow Key Channel Shift Function</i>	16
6.3.3.	<i><ALT> Channel Shift Function</i>	16
6.4.	CHANNEL SELECT - CASCADE CHAIN LAYER	17
6.5.	BUZZER SOUND DISABLE / ENABLE.....	17
6.6.	AUTO-SCAN FUNCTION	18
6.6.1.	<i>Start auto-scan function</i>	18
6.6.2.	<i>Stop auto-scan function</i>	19
6.6.3.	<i>Auto-scan mode</i>	19
6.6.4.	<i>Auto-scan time interval</i>	19
6.7.	CONSOLE LOCK.....	19
6.8.	CALL ADJUST VIDEO MENU.....	19
7.	OSD OPERATION	20
7.1.	OSD MAIN MENU.....	20
7.1.1.	<i>KVM layer number</i>	20
7.1.2.	<i>Channel name</i>	20
7.1.3.	<i>Computer & KVM status</i>	20
7.1.4.	<i>Current active channel number</i>	21
7.1.5.	<i>Cascade parent channel number</i>	21
7.1.6.	<i>Page down / up indicator</i>	21
7.1.7.	<i>Function Control Menu</i>	21
7.2.	CHANNEL SELECTION IN OSD.....	22
7.2.1.	<i>Channel select to computer</i>	22
7.2.2.	<i>Channel select to cascade port</i>	22
7.2.3.	<i>Return from cascade port</i>	22
7.3.	SETUP IN OSD: <F1>	23
7.3.1.	<i>Scan Mode</i>	23
7.3.2.	<i>Scan Time</i>	23
7.3.3.	<i>Banner Time</i>	23
7.3.4.	<i>Position</i>	24
7.3.5.	<i>Hot key</i>	24
7.3.6.	<i>Sound</i>	24
7.3.7.	<i>Language</i>	25
7.4.	AUTO-SCAN IN OSD: <F2>	25
7.4.1.	<i>Start to auto-scan in OSD</i>	25
7.4.2.	<i>Stop auto-scan</i>	25
7.4.3.	<i>Auto-scan mode</i>	25
7.4.4.	<i>Auto-scan time interval</i>	25
7.5.	CONSOLE LOCK IN OSD: <F3>	25
7.6.	CHANNEL RENAME: <F4>.....	26

7.7.	SECURITY SETUP: <F5>.....	27
7.7.1.	Security mode login.....	27
7.7.2.	Security Mode	27
7.7.3.	Change administrator password.....	28
7.7.4.	Authorized user setup.....	28
7.7.5.	User Authority setup	28
7.8.	LOCK PORT: <F6>.....	29
7.8.1.	Lock Port	29
7.8.2.	Channel selection of the locked port.....	30
7.8.3.	Unlock Port.....	30
7.9.	EXIT OSD: <ESC>	30
7.10.	ADJUST VIDEO IN OSD	30
8.	SUN MICROSYSTEMS FUNCTION KEY EMULATION:.....	31
9	CONFIGURATION	32
9.1	NETWORK CONFIGURATION USING PSETUP UTILITY	32
9.2	CONFIGURATION SETUP VIA SERIAL CONSOLE	37
9.3	KEYBOARD, MOUSE, AND VIDEO CONFIGURATION	38
9.3.1	CAT5 8-PORT/16-PORT IP-KVM keyboard settings	38
9.3.2	Remote Mouse Settings	38
9.3.3	Automatic mouse speed and mouse synchronization	39
9.3.4	Single and Double Mouse Mode.....	39
9.3.5	Host system mouse settings	40
9.3.6	Video Modes.....	41
10	USAGE.....	42
10.1	PREREQUISITES	42
10.2	LOG IN/OUT CAT5 8-PORT/16-PORT IP-KVM	44
10.2.1	LOG IN THE CAT5 8-PORT/16-PORT IP-KVM	44
10.2.2	LOG OUT FROM THE CAT5 8-PORT/16-PORT IP-KVM	46
10.3	THE REMOTE CONSOLE.....	46
10.3.1	MAIN WINDOW OF REMOTE CONSOLE.....	47
10.3.2	CONTROL BAR OF REMOTE CONSOLE	48
10.3.3	STATUS LINE OF REMOTE CONSOLE	60
11	MENU OPTION.....	61
11.1	REMOTE CONTROL.....	61
11.1.1	KVM CONSOLE.....	62
11.1.2	TELNET CONSOLE/SSH CONSOLE.....	62
11.1.3	REMOTE WAKEUP	66
11.2	VIRTUAL MEDIA	69
11.2.1	DRIVE REDIRECTION	70
11.2.2	VIRTUAL DRIVE.....	71
11.2.3	CD/DVD IMAGE.....	73
11.2.4	FLOPPY DISK.....	78
11.2.5	CREATING AN IMAGE.....	80
11.2.5.1.	CREATING A FLOPPY IMAGE	80
11.2.5.2.	CREATING A CD/DVD ISO IMAGE	81
11.2.6	MAKING A DRIVE REDIRECTION	82
11.3	USER MANAGEMENT	86
11.3.1	CHANGE PASSWORD.....	86
11.3.2	USERS AND GROUPS.....	87
11.4	KVM SETTINGS	88
11.4.1	USER CONSOLE.....	89
11.4.2	KEYBOARD/MOUSE.....	93
11.4.3	VIDEO.....	94
11.5	DEVICE SETTINGS	95
11.5.1	NETWORK.....	95
11.5.2	DYNAMIC DNS.....	98
11.5.3	SECURITY.....	100
11.5.5	SERIAL PORT.....	107
11.5.6	DATE/TIME	110
11.5.7	EVENT LOG	111
11.5.8	AUTHENTICATION.....	115
11.5.9	USB	118
11.5.10	CONFIG FILE.....	119
11.6	MAINTENANCE	119
11.6.1	DEVICE INFORMATION	119

11.6.2	EVENT LOG	121
11.6.3	UPDATE FIRMWARE.....	122
11.6.4	UNIT RESET	125
11.6.5	RESET FACTORY DEFAULTS	126
12.	FAQ	128
13.	TROUBLESHOOTING.....	129
14.	KVM FIRMWARE UPGRADE PROCEDURES	135
15.	ADDENDUM	139

1. Introduction

Thank you for purchasing CAT5 8-Port / 16-Port Combo Free KVM Switch Over IP (or CAT5 8-PORT/16-PORT IP-KVM for simplicity)! You now have a high quality, durable system to control 8 or 16 computers through PS/2 and/or USB connection from one console (PS/2 & USB Mouse, PS/2 & USB Keyboard, and Monitor). And it allows you to control one or more 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 secure via SSL authentication and encryption. Use in conjunction with a KVM switch for multiple-server access.

● Features

CAT5 KVM Over IP

1. 1-Console 8/16-Port CAT5 KVM switch
2. Each server can be 40 meters away from this KVM Switch by CAT5 UTP cable
3. Manage servers remotely around the world
4. Remote KVM (keyboard, video, and mouse) access over IP or analogous telephone line (modem needed)
5. Console your Keyboard / Mouse via PS/2 and/or USB at will
6. Connect computers via PS/2 and/or USB at will
7. Full control under all OS, in BIOS level, during boot, or at Blue Screens
8. On-Screen-Display (OSD) & Cascade Chain functions
9. OSD is intuitive menus driven for quick and efficient navigation
10. Supports cascade chain with 3 level cascades: up to 3 levels; control up to **8 / 64 / 512 (for 8-Port only) and 16 / 256 / 4096 PCs (for 16-Port only)**, from a single console; cascaded chaining units does not need special configuration
11. Emulates PS/2 or USB keyboard on each PC to allow your computers to boot normally without a keyboard error
12. Supports hot-pluggable. All devices connected to the KVM can be added or removed at any time, without shutting the unit down
13. Supports 3 types of switching:
 - Hardware Front Push Buttons
 - Hot-Keys on PS/2 and/or USB of keyboard
 - Menu driven OSD (On Screen Display)
14. Supports Auto-Scan function to switch video inputs automatically among computers in present intervals sequentially by OSD menu driven
15. Supports LED display for PC and/or server status monitoring
16. Supports VGA resolutions up to 1920x1200@60 Hz
17. Supports Beeper during Switching enabled
18. Adjustable control of focus and brightness to improve video quality by Hot-Keys

19. Fully compliant with the USB 1.1/ 2.0 specification
20. Rack Mountable in 19" system rack (1U)
21. KVM firmware is upgradeable via on-board mini-USB download connector and external mini-programmer
22. Remote power wakeup on the target computer
23. Remote mass storage control and redirection
24. Remote control over Java-enabled Browsers
25. No additional software necessary on client console side
26. SSL Secure access through certificate authentication and data encryption
27. 256-bit SSL encryption of all transmitted data
28. Persistent logging of all important events
29. Up to 63 users profile with definable, three categories users authorized levels.
30. Auto-optimize the frame rate and video quality according to the bandwidth availability.
31. Automatically senses video resolution for best possible screen capture
32. High-performance mouse tracking and synchronization
33. KVM firmware is upgradeable via on-board mini-USB download connector and external mini-programmer and web interface

KVM Transmission

1. Transmission of video signals with up to resolution 1600x1200@ 60 Hz
With 16, 8, 4, 2, 1 Bit video encoding, manual and automatic adjustment.
2. Supports of all standard VGA and VESA modes (graphics and text)
3. Video resolution at the local video port up to 1920x1200@60 Hz
4. Works with all states of the web browsers

Network access

1. Access via 10/100 Mbps LAN
2. Communication over TCP/IP port 80 and port 443 (reconfiguration possible)
3. IP-configuration via DHCP/BOOTP or static
4. HTTP and HTTPS (secure) Web Server
5. Supports of standard Hayes compatible modems
6. Speed of modem up to 115200 bps
7. Automatic adjustment of video compression ratio to available bandwidth

2. Specifications

Specification		
Number Of Computer Controlled		8 or 16
Selection Method		Push Button and Hot-Key (PS2 and/or USB keyboard)
		Or On-Screen-Display(OSD)
LEDs		Red for PC Selection
		Green for PC ON-Line ready
Compliant with USB Version		USB1.0 / USB1.1 / USB2.0
Compliant with HID Version		USB HID 1.11
PC port Connectors		8 / 16 RJ45 connector
CAT5 Dongle (DS-19202)	Video	8/16 x HDB-15 male
	(KB/MS)	(PS2 & USB signal combined)
	Data transmit	RJ45 connector
Console port	Keyboard	1 x 6 pin mini-DIN female
	Mouse	1 x 6 pin mini-DIN female
	Video	1 x HDB-15 female
	Keyboard	1 x USB – A type female
	Mouse	1 x USB – A type female
Firmware upgrade connector		1 x Mini USB female
Serial port		1 x RS232 male
Ethernet port		1 x RJ45
Virtual Media port		1 x Mini USB female
Remote console screen resolution		Up to 1600 x 1200 @ 60Hz
DDC,DDC2 monitor		Supports DDC2B, max resolution up to 1920 x 1200 @60Hz
Operating system supported		Win 98/98SE/ME/2000/XP/Vista/7/2003 Mac OS9/X, Linux, Sun Micro OS
Power		By External Adaptor DC 12V 2A
Hot Pluggable		Yes
Device driver		No
Dimensions (LxWxH)		44 x 15.7 x 4.5 cm (17.3 x 6.1 x 1.5 inch)
Unit Weight		1810g/1960g
Housing material		Metal
Operating Temperature		32~122 °F (0~50°C)
Storage Temperature		4~140 °F (-20~60°C)
Humidity		0%~80%RH

3. System Requirements

■ Hardware

- Local Host side :

The following equipment must be equipped with each computer or server

A VGA, SVGA or Multisync card

Type A USB port or PS/2 6 pin mini-DIN for Keyboard and Mouse.

- Local console side:

A VGA, SVGA, Multisync monitor capable of the highest resolution.

PS/2 and/or USB Keyboard/Mouse.

- Remote Console side:

One Computer or Multiple Computers are linked into the network

- Cables

The CAT5 IP-KVM Switch must be used CAT5 UTP cables with specific custom CAT5 dongle (such as DS-19202). To purchase the specific dongle, please contact your dealer.

■ Remote Console side

- 1 Java Runtime Environment : version 1.5 or above.
- 2 Browser: Microsoft Internet Explorer version 6.0 or above or Netscape or Mozilla or Safari.

4. Installation

4.1. Front View

- 8-Port

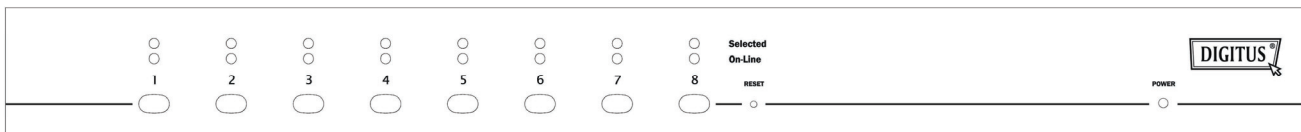


Figure 1: CAT5 8-Port IP-KVM front view

- 16-Port

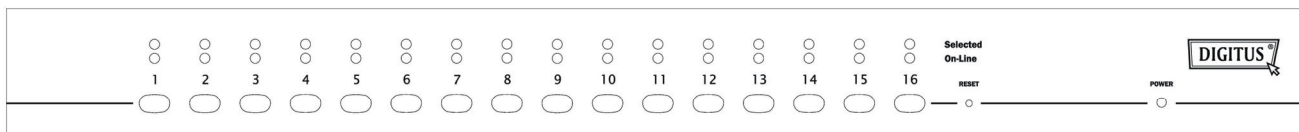


Figure 2: CAT5 16-Port IP-KVM front view

- LED Indicators:

- Selected:

RED LED indicates that the CAT5 8-PORT/16-PORT IP-KVM is selected to the

corresponding PC.

➤ **On-Line:**

GREEN LED indicates that the CAT5 8-PORT/16-PORT IP-KVM is ready to the corresponding PC.

● **Reset Switch :**

Press Reset switch when you want to reset the system. This switch must be pushed with a thin object like the end of a paper clip, or a ball point pen.

4.2. Rear View

● **8-Port**

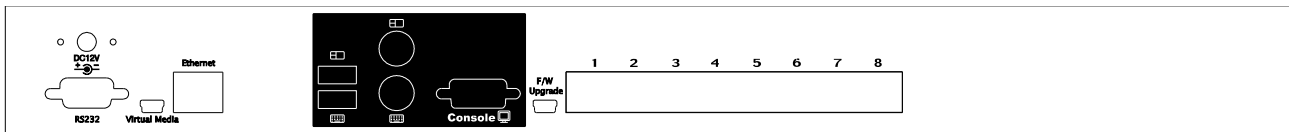


Figure 3: CAT5 8-Port IP-KVM rear view

● **16-Port**

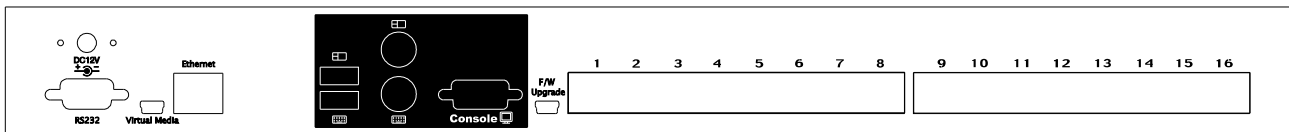


Figure 4: CAT5 16-Port IP-KVM rear view

● **Ethernet LED Indicators:**

➤ **IP-Ready:**

ORANGE LED blinking per second when system is ready.

➤ **Ethernet-Link:**

GREEN LED indicates that Ethernet connection established.

4.3. Single stage installation

4.3.1. Precaution:

- Please turn off computers and devices when you start to install KVM Switch.
- For computers with Keyboard Power On function, please unplug the power cords in advance. Otherwise, the switch might not work properly.
- If your computers work under Windows 98, please connect KVM switch to computers via PS/2 ports, because Windows 98 does not support installation at first time as through USB HID installation driver.
- Some kind of old computers must enable USB setting in BIOS in advance to make USB interface work.
- This KVM switch does not guarantee to fully support USB keyboard with USB HUB.

- (Optional) Connect the USB connectors of USB A-mini cable to the host computer and the CAT5 8-PORT/16-PORT IP-KVM module while for remote mass storage control.
- Connect one end of Ethernet cable to ethernet jack of CAT5 8-PORT/16-PORT IP-KVM, and the other end to the Remote Console computer.

4.3.2. Console connection:

Plug keyboard, mouse and monitor to the console ports on the real panel of CAT5 8-PORT/16-PORT IP-KVM (Figure 5).

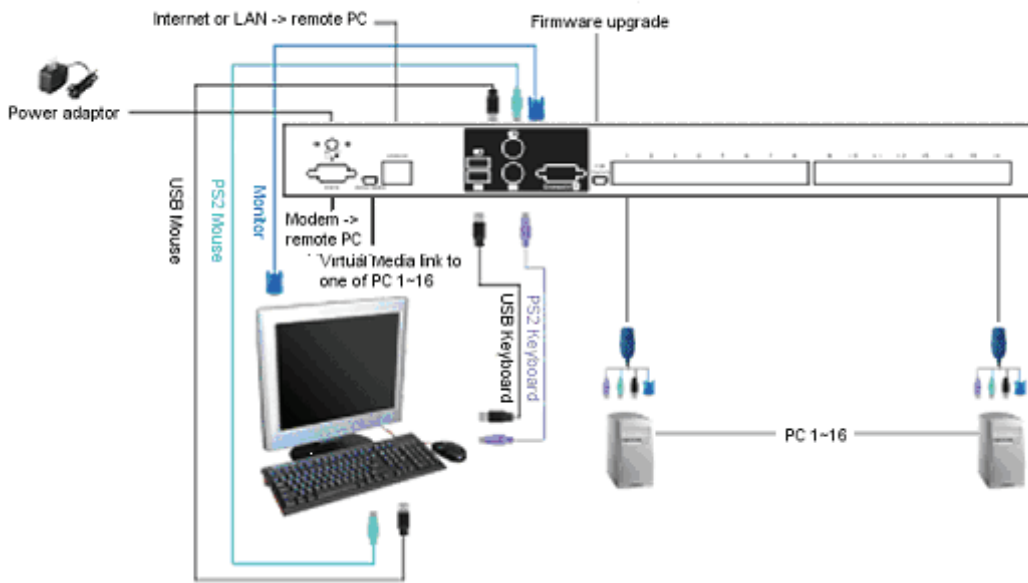


Figure 5: Console connection

4.3.3. System connection:

Please use Custom CAT5 cable to connect your computers.
Please refer to the figures and instruction shown below for System connection.

Note: Please contact your dealer to purchase the custom combo 4-in-1 CAT5 dongle (DS-19202) if you need.



Figure 6: Custom combo 4-in-1 CAT5 dongle (DS-19202)

You can connect CAT5 8-POR/16-POR IP-KVM to computers via three methods shown below:

- A. Connect **USB, PS/2 (keyboard/mouse)** and **VGA** connectors to computers. We recommend users to connect computers in this way.

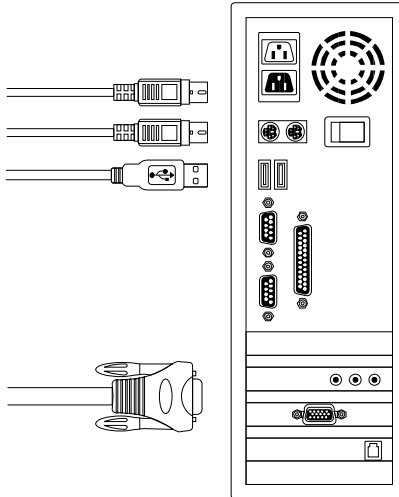


Figure 7: USB & PS/2 (Keyboard & Mouse) and VGA connected

- B. Connect only PS/2 (keyboard/mouse) and VGA connectors to computers.

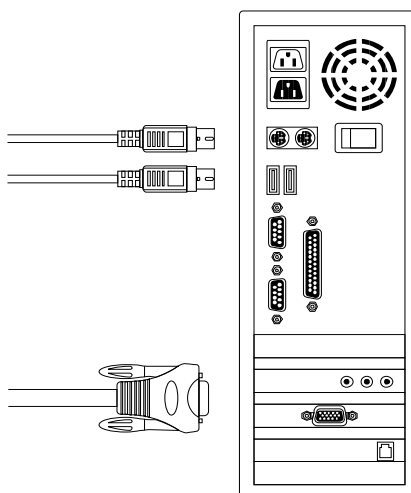


Figure 8: PS/2 (Keyboard & Mouse) and VGA connected

Connect only USB and VGA connectors to computers.

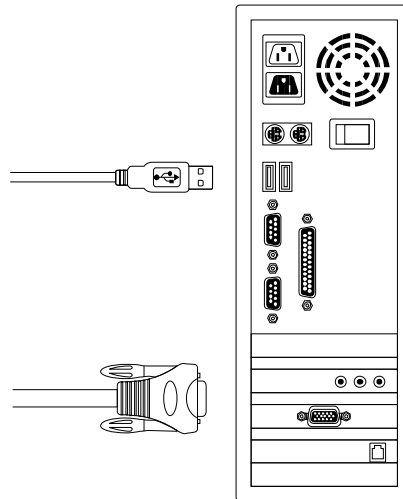


Figure 9: USB and VGA video connected

4.4. Cascade Chaining

CAT5 Combo Free 8-Port & 16-Port KVM switch support 3 level cascades; control up to **8/64/512 PCs (for 8-Port only)** and **16/256/4096 PCs (for 16-Port only)**, from a single console; cascaded chaining units do not need special configuration. Cascaded configuration expands system ability and allows you to select computers connected to the Master or Slave. After connected, KVM Switches automatically configure Master and Slave.

Note: CAT5 8-PORT/16-PORT IP-KVM should be the master KVM Switches, and the second & third layers could use Standard KVM Switches without Over-IP function (Combo KVM Switches connected to 2nd & 3rd layers).

To Install cascade chain, please follow the instruction below:

- A. Please turn off computers and devices when you start to install KVM Switch.
- B. Uses the custom combo 4-in-1 CAT5 dongle (DS-19202) (**See Figure 6**) to connect one or more Slave KVM Switches to any PC port of Master KVM Switch. **The connection between KVM to KVM must be connected through PS/2 connection. (Please refer to Figure 7 & Figure 8).**
- C. **You can do console Master KVM Switch via either USB and/or PS/2 keyboard and mouse at will.**
- D. Plug in the power adapter of the first level Master KVM Switch and connect Master KVM switch to computers.

- E. Next, plug in power adapter for each level Slave KVM Switch and connect Slave KVM switch to computers .
- F. The power on sequence should be:
1. Master KVM Switch
 2. Second level Slave KVM Switch (connecting to Master KVM Switch) if any.
 3. Third level Slave KVM Switch (connecting to second level Slave KVM Switch) if any.
 4. All computers connecting to Master/Slave KVM Switch.
- G. After all KVM Switches are powerd by power adaptor, trun on the computers.
- Initial Plug-in Process:
Please plug in the Master KVM Switch first before turning on any other devices like montior or computers.
 - Hot plug and Hot Swap:
Combo Free 8-Port & 16-Port KVM switch support Hot plug and Hot swap function.

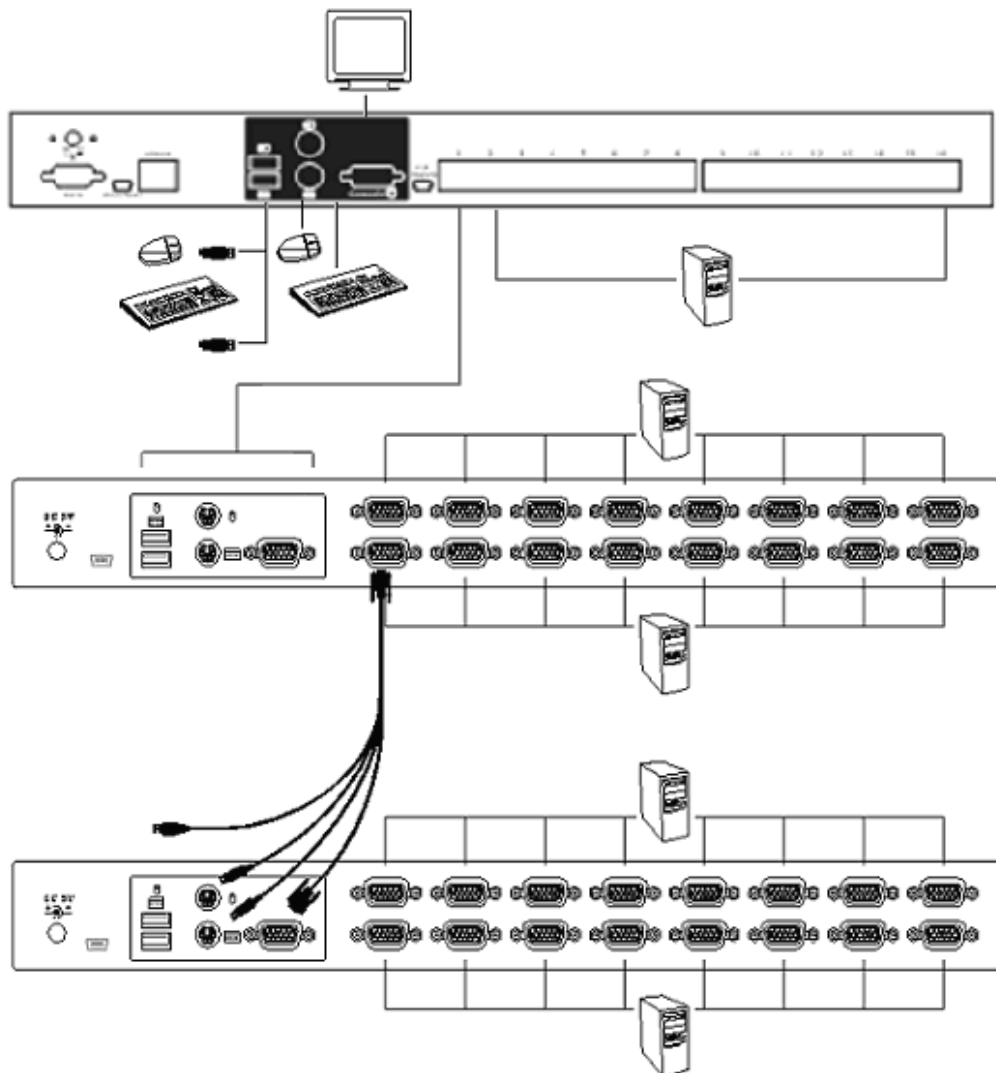


Figure 10: Cascade chaining

4.5. Firmware download connector

The min-USB female connector on the rear of KVM switch is for firmware upgrade function. To update your KVM firmware, please contact with your dealer.

4.6. Rack Mounting

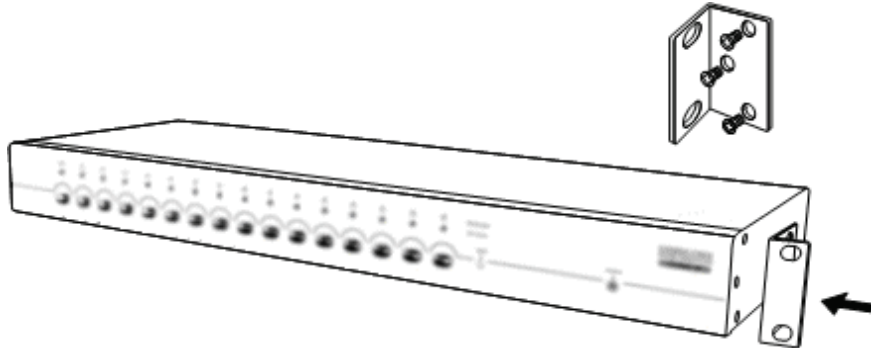


Figure 11: Rack mounting

Figure 11 shows you how to attach mounting brackets to the KVM Switches unit for standard 19-inch rack cabinet.

1. Screw the mounting brackets into the sides of the KVM-Switches unit. (See Figure 11)
2. Install the KVM-Switches unit into the rack cabinet.

5. Operation

You can control computers via CAT5 8-Port or 16-Port Combo Free KVM Switch Over IP by push button, hot key and OSD.

- Push button operation
Press the front panel push button to select the PC and operate it.
- Hot Key operation
Please refer to section 6. Hot Key Operation.
- OSD operation
Please refer to section 7. OSD Operation.

6. Hot Key Operation

6.1. Call OSD Menu

Press **< Scroll Lock >** twice and **<Enter>**, then the OSD “Main Menu” will be displayed on the monitor screen. All of the KVM parameters can be setup in OSD mode. You can also execute some KVM functions in OSD.

<Scroll Lock> → <Scroll Lock> → <Enter>

6.2. Leading Hot Key Select

The two-steps hot key sequence is used for quick function execution.

The leading key is **<Scroll Lock>** by default. However, you can change the leading hot key if you want.

By pressing **<CTRL>** twice, **<New Hot Key>**, then press **<Enter>**, you can change the leading hot key.

The available leading hot key are **<Scroll Lock>**, **< Num Lock >** or **< Caps Lock >** for option.

- **Setup leading hot key to < Scroll Lock >**
< CTRL > → < CTRL > → < Scroll Lock > → < Enter >
- **Setup leading hot key to < Num Lock >**
< CTRL > → < CTRL > → < Num Lock > → < Enter >
- **Setup leading hot key to < Caps Lock >**
< CTRL > → < CTRL > → < Caps Lock > → < Enter >

Note: You can also change leading hot key by pressing **<F1>** in OSD main menu.

Please refer to section **7.3.5 Setup in OSD – Hot Key**.

6.3. Channel Select - Single KVM

6.3.1. Specific channel selection

You can select the connected computers by using the two-step Hot Key sequence. Press **<Scroll Lock>** key twice (Step 1), then press **key (1 to 16)** and **<Enter>** (step 2) to select the computer you want to control.

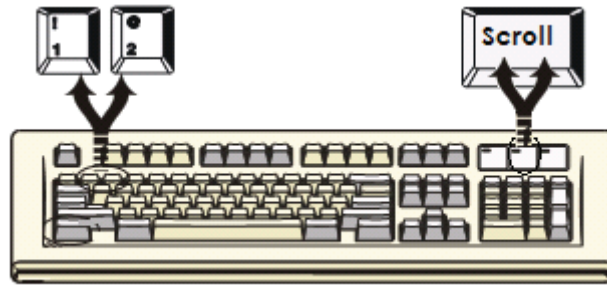


Figure 12: Specific channel selection hot key

<Scroll Lock> → **<Scroll Lock>** → **<1>** → **<Enter>** or
<Scroll Lock> → **<Scroll Lock>** → **<2>** → **<Enter>** or
 ⋮
<Scroll Lock> → **<Scroll Lock>** → **<16>** → **<Enter>**

Note: You can also select computers in OSD menu. Move the indicator bar to the channel to switch by using **<arrow key>**, **<Page Up>** or **<Page Down>**, then press **<Enter>** to select the connected computer. Please refer to section **7.2 Channel Selection in OSD**.

6.3.2. Arrow Key Channel Shift Function

Press **<Scroll Lock>** twice, and press **<Left Arrow>** or **<Right Arrow>** key to shift left/right one channel.

- **Switch to left one channel**
<Scroll Lock> → **<Scroll Lock>** → **<Left Arrow>**
- **Switch to right one channel**
<Scroll Lock> → **<Scroll Lock>** → **<Right Arrow>**

6.3.3. <ALT> Channel Shift Function

1. Start <ALT> Channel shift Function

< ALT > channel shift function default was off. You can press Hot-Key **<Scroll Lock>** twice, **<ALT>** and then press **<Enter>** to turn on or turn off this function alternately.

2. Shift the channel by <ALT> key

Press left **< ALT >** or right **< ALT >** key twice, the PC channel will automatically shift to left or right one channel (channel decrease / increase to next) when **< ALT >** channel shift function is enabled.

- **Enable/Disable <ALT> channel shift function**

<Scroll Lock> → <Scroll Lock> → < ALT > → <Enter>

- **Switch to left one channel**

<Left ALT> → < Left ALT >

- **Switch to right one channel**

<Right ALT> → < Right ALT >

6.4. Channel Select - Cascade Chain Layer

You can select the active channel directly under cascade chain connection.

The following hot key sequence is used for quick channel selection.

Press **<Scroll Lock>** twice, **<D>**, the cascade **channel number (1, 2, 3.....16)**, and Press **<Enter>**.

- **Channel select to first layer**

< Scroll Lock > → < Scroll Lock > → <D> → < CH-L1 > → < Enter >

- **Channel select to second layer**

< Scroll Lock > → < Scroll Lock > → <D> → < CH- L1 >
→ <D> → < CH-L2 > → < Enter >

- **Channel select to third layer**

< Scroll Lock > → < Scroll Lock > → <D> → <CH-L1 >
→ <D> → < CH-L2 >
→ <D> → < CH-L3 > → < Enter >

Note: With cascading 3 layers, you can select last layer directly;

Example: press **<Scroll Lock>** twice, then **D2D5D7**, and **<Enter>**:

D2 : layer 1 channel 2 links to

D5 : layer 2 channel 5 links to

D7 : layer 3 channel 7 selected

Note: You can also select active channel of cascade chain in OSD menu. Move the indicator bar to the channel selected to switch by using **<arrow key>**, **<Page Up>** or **<Page Down>**, and then press **<Enter>** to switch to the target port.

Please refer to section **7.2.2 Channel select to cascade port.**

6.5. Buzzer sound Disable / Enable

Press **<Scroll Lock>** twice, then **** and **<Enter>**. The buzzer sound will be disabled / enabled alternately. The buzzer sound default setting is **ON**.

<Scroll Lock> → <Scroll Lock> → → <Enter>

Note: You can also enable/disable buzzer sound by pressing **<F1>** in OSD main menu.
Please refer to section **7.3.6 Setup in OSD - Sound**.

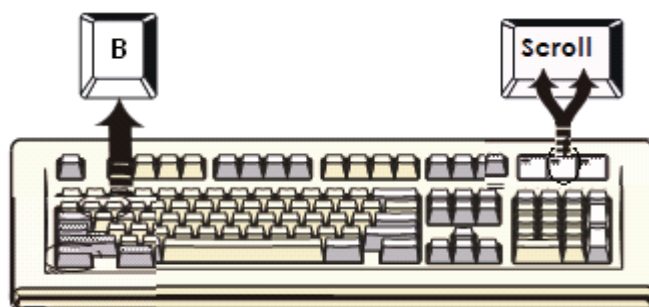


Figure 13: Buzzer setup hot key

6.6. Auto-Scan Function

You can enable Auto-Scan function by pressing **<Scroll Lock>** twice, then **<S>** and **<Enter>**. The KVM Switch will shift through all the ports and display them on the monitor.

The mouse and keyboard will be disabled under this mode. This is necessary to prevent errors such as erratic movement and wrong characters to display when using the mouse or keyboard in accident.

6.6.1. Start auto-scan function

<Scroll Lock> → **<Scroll Lock>** → **<S>** → **<Enter>**. The auto-scan banner will be shown on screen to indicate the scanning channel.



Figure 14: Auto-scan hot key

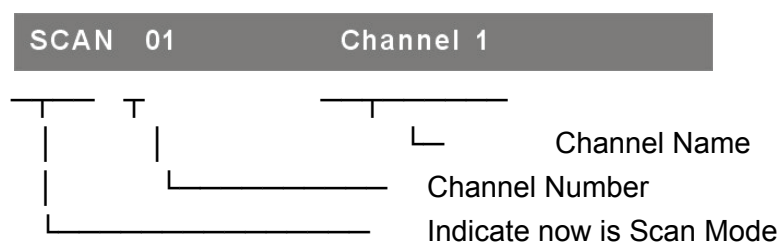


Figure 15: Auto-scan Banner

6.6.2. Stop auto-scan function

Press any key on keyboard to **STOP** the auto-scan function. Press the push button on KVM front panel to select active port can stop the auto-scan function, too.

6.6.3. Auto-scan mode

There are two auto-scan modes, please refer to section **7.3.1 Setup in OSD – Scan Mode** to setup the auto-scan mode.

- Scan all working computers.
- Scan all computers which are marked for auto-scan.

6.6.4. Auto-scan time interval

The auto-scan time interval can be adjustable by pressing **<F1>** in OSD main menu. Please refer section **7.3.1 Setup in OSD – Scan Time**.

Note: You can also start auto-scan function by pressing **<F2>** in OSD main menu. Please refer section **7.4 Auto-Scan in OSD**.

6.7. Console Lock

If the security mode is enabled in OSD mode (by pressing **<F5>** in OSD mode), you can lock console by pressing **<Scroll Lock>** twice, and then **<H>** and **<Enter>**. The KVM will be locked until an authorized user login.

<Scroll Lock> → <Scroll Lock> → <H> → <Enter>

To **UNLOCK** console, please press any key according to screen message, then key in User Name and Password. The KVM switch and console devices will be unlocked and back to normal status.

Note: You can also execute console lock function by pressing **<F3>** in OSD main menu. Please refer to section **7.5 Console Lock in OSD**.

6.8. Call Adjust Video Menu

Press **< Scroll Lock>** twice, then **<C>** and **<Enter>**, then the OSD “Adjust Video” will be displayed on the monitor screen. You can adjust video quality for current active channel in first layer.

<Scroll Lock> → <Scroll Lock> → <C> → <Enter>

7. OSD Operation

7.1. OSD Main Menu

Press < **Scroll Lock** > twice and < **Enter** >, then you will enter to **OSD (On Screen Display)** main menu. The channel number, names and the status will be displayed on the monitor screen. Please refer to (Figure 16)

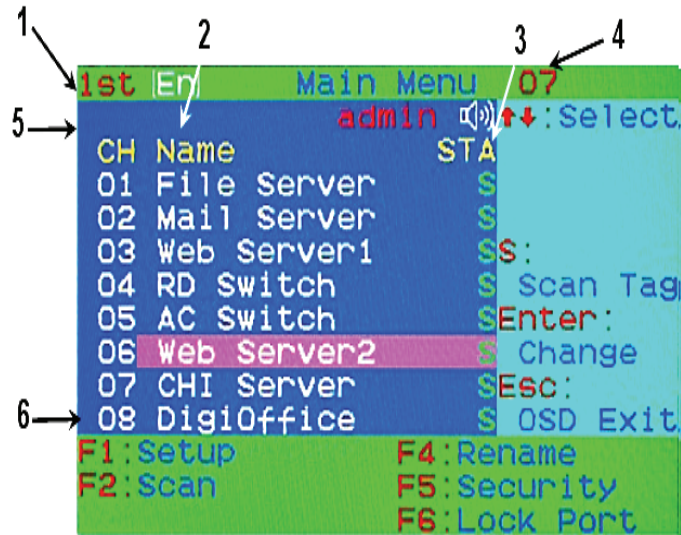


Figure 16: OSD main menu

7.1.1. KVM layer number

1st, 2nd or 3rd. indicates the current cascade level.

7.1.2. Channel name

- The channel name can be defined by using function key **F4**, it can remind user which computer is connected to this channel.
- A highlighted pink bar is shown in the selected channel row.
- A plus mark (+) showing in the left of channel name indicates that the port has cascades.

7.1.3. Computer & KVM status

➤ KVM buzzer stauts

Buzzer sound on

✗Buzzer sound off

➤ Logged user name

The system has one administrator and 3 users for security management. The name of current logged is displayed here.

- **Channel LOCK indicator** (Status **STA**)
 - L:** Indicating this channel is locked.
 - BLANK:** Indicating this channel is normal without locked.
- **Computer power on indicator** (Status **STA**), OSD menu will update the flag automatically if the computer status is changed
 - A:** Indicating this computer is powered on and ready to select.
 - BLANK:** Indicating this computer is not connected or powered on.
- **Channel scan indicator** (Status **STA**)
 - S:** This channel is marked for auto-scan if the scan mode is **Select** type.
 - BLANK:** Indicating this computer is not marked for auto-scan.

7.1.4. **Current active channel number**

Indicate current active channel number. The channel of the currently selected computer is displayed in the right-upper corner.

If the active channel is in 2nd or 3rd cascade layer, the display string is like XX-YY-ZZ. For example, 02-05-07 means the active channel is layer 1 channel 2 links to layer 2 channel 5, and layer 3 channel 7 is selected as active channel.

7.1.5. **Cascade parent channel number**

Indicate the parent channel of this cascade layer. The number at the left-upper corner below KVM layer number shows the number of port for the upper layer, i.e. 8 means link from channel 8 of upper KVM.

It's valid only for 2nd and 3rd cascade layer. It will show blank for 1st layer since there is no parent channel.

7.1.6. **Page down / up indicator**

This is for 16-Port KVM only. The information of port 1 ~ 8 are display in the first page, and information of port 9 ~ 16 are display in the second page. Since the port information is divide to two pages, the **page down / up indicator** can remind you to switch to alternative page by using **<page down>** and **<page up>** key.

7.1.7. **Function Control Menu**

The detail of control functions will be described in later sections. The list of control functions:

F1: Set up: basic set up menu

F2: Scan: autoscan function

F3: Lock: setup lock/unlock, only available when **F5 Security** is enabled.

F4: Rename: rename selected channel name.

F5: Security: security function and user authority settings

F6: Lock Port: PC port lock function (for administrator only)

7.2. Channel selection in OSD

7.2.1. Channel select to computer

Use the <UP> and <DOWN> arrow keys to highlight a computer and then <ENTER> to select it and leave OSD menu. A banner with the channel name will be shown on left-upper corner of the screen.

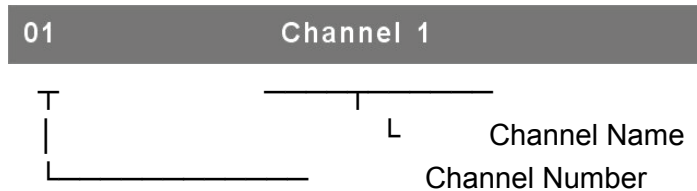


Figure 17: Channel Banner (Single Layer)

7.2.2. Channel select to cascade port

A plus mark (+) showing in the left of channel name indicates that the port is under cascade channing. Pressing <ENTER> in this channel will enter one level down, and the screen pops up the listing of the computers of the slave KVM.

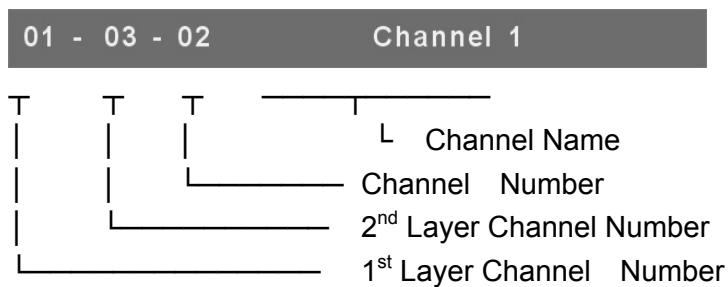


Figure 18: Channel Banner (Cascade Layer)

7.2.3. Return from cascade port

After entering cascade port, press <R> will return to upper layer OSD menu.

7.3. Setup in OSD: <F1>

Please use <Up> or <Down> arrow key to select the item you want to change, and use <Left> or <Right> arrow key to change the settings. Press <ESC> to exit and save the setup settings.

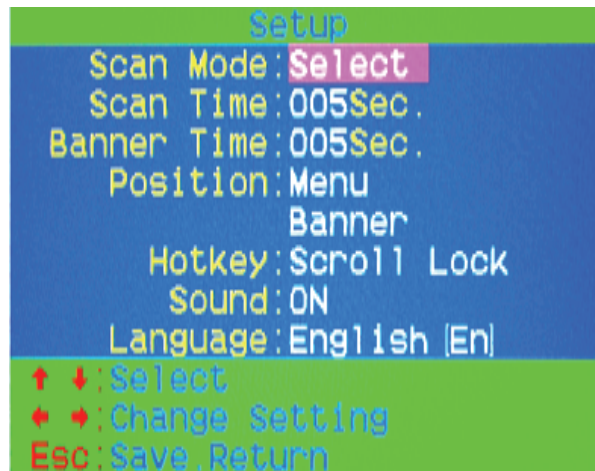


Figure 19: OSD Setup

7.3.1. Scan Mode

- **Select:**
Scan the selected channels marked with **S** in **STA** column on OSD main menu.
- **PC ON:**
Scan all powered on PC channels

7.3.2. Scan Time

The default scan time is 5 seconds. It can be changed up to 90 seconds by stepping 5 seconds.

7.3.3. Banner Time

The default banner time is 5 seconds. It can be changed to 10 seconds, 15 seconds, or always on (∞).

7.3.4. Position

➤ **Menu:**

Use four arrow keys to move the OSD main menu to the desired position. Press **<ESC>** to save the changed menu position.

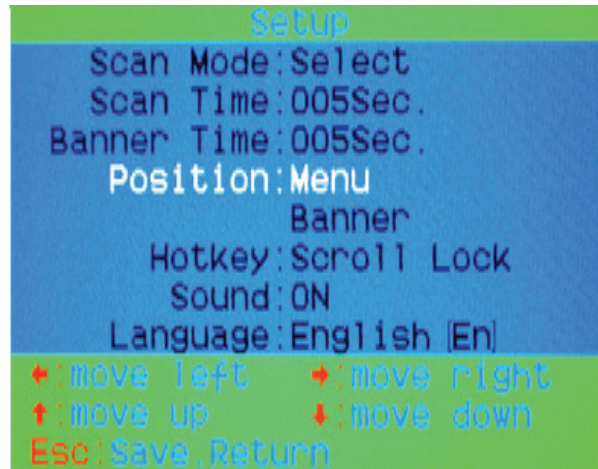


Figure 20: Menu Position Setup

Note: The different resolution setting between PC and KVM will change the desired position of OSD block shown on screen.

➤ **Banner:**

Use four arrow keys to move the channel banner to the desired position. Press **<ESC>** to save the changed banner position.



Figure 21: Banner Position Setup

7.3.5. Hot key

- **Scroll Lock:** **<Scroll Lock>** becomes the hot key.
- **Num Lock:** **<Num Lock>** becomes the hot key.
- **Cap Lock:** **<Cap Lock>** becomes the hot key.

Note: You can also change leading hot key via hot key by using **< CTRL > → < CTRL > → < New Hotkey > → < Enter >** outside the OSD mode. Please refer to section **6.2 Leading Hot Key Select**.

7.3.6. Sound

- **ON:** Buzzer sound enabled.
- **OFF:** Buzzer sound disabled.

Note: You can also enable/disable buzzer sound via hot key by using **<Scroll Lock> → <Scroll Lock> → → <Enter>** outside the OSD mode. Please refer to section **6.5 Buzzer sound Disable / Enable**.

7.3.7. Language

English (En) / Deutsch (De) / Francais (Fr), 3 languages are available.

7.4. Auto-Scan in OSD: <F2>

7.4.1. Start to auto-scan in OSD

Press <F2> in OSD main menu. The auto-scan banner will be shown to indicate the scanning channel.

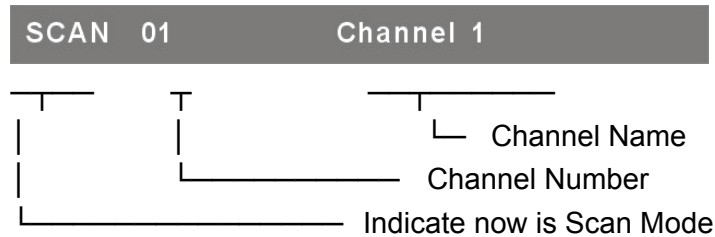


Figure 22: Auto-Scan Banner

Note: You can also start auto-scan function via hot key by using <Scroll Lock> → <Scroll Lock> → <S> → <Enter> outside the OSD mode. Please refer to section **6.6.1 Start Auto-Scan Function**.

7.4.2. Stop auto-scan

Press any key on keyboard to **STOP** the auto-scan function. The auto-scan banner will be disappeared when the scan stopped.

7.4.3. Auto-scan mode

There are two auto-scan modes, please refer to section **7.3.1 Setup in OSD – Scan Mode** to set up the auto-scan mode.

- Scan all computers which are power on.
- Scan all computers which are marked for auto-scan.

7.4.4. Auto-scan time interval

The auto-scan time interval of each port displayed can be adjustable by pressing <F1> in OSD main menu. Please refer to section **7.3.2 Setup in OSD – Scan Time**.

7.5. Console Lock in OSD: <F3>

If the security mode is enabled in OSD mode (by pressing <F5> in OSD mode, please refer to section **7.7 Security Setup in OSD**). You can logout to lock console by pressing <F3> In OSD mode. The **Console Lock Banner** will be shown on the screen.



Figure 23: Console Lock Banner

The KVM will be locked until an authorized user login.

```
Name : JERRY
Password :
```

Figure 24: Unlock window

Note: You can also logout to lock console via hot key by using

<Scroll Lock> → **<Scroll Lock>** → **<H>** → **<Enter>** outside the OSD mode.

Please refer to section **6.7 Console Lock**.

Note: If you forget the password, the only way to permanently disable the security function is to key in a universal password to unlock KVM. You need to key in this unlock password to release your device and KVM, and then you can restart everything. Please contact with your agency/distributor to get the universal password.

7.6. Channel rename: <F4>

Select the channel to rename by using up/down arrow key and press **<F4>** in OSD main menu. The channel rename window will be shown for setting up the channel name. Press **<ENTER>** to save the renamed channel name or **<ESC>** to cancel.

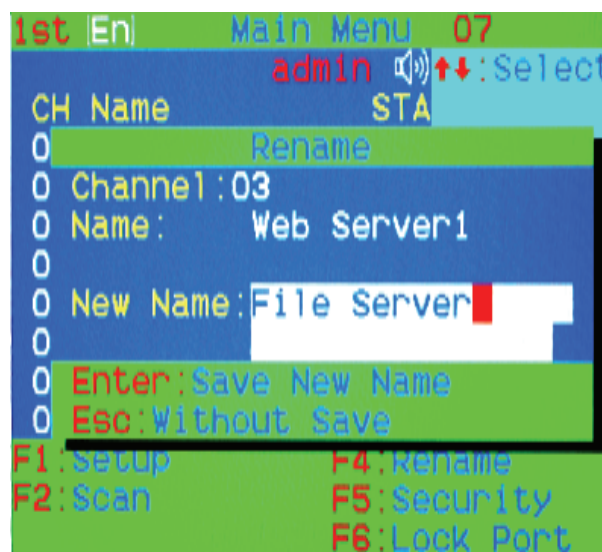


Figure 25: Channel Rename window

7.7. Security Setup: <F5>

7.7.1. Security mode login

Press <F5> in OSD main menu to enter security setup mode, the administrator login is required before entering into the security mode.



Figure 26: Security mode login window

The default administrator account is:

User Name: admin
Password: 123456

After login, the security setup main window will be shown on the screen. Please select the security item to setup via <up arrow> and <down arrow> key, and press <left arrow> or <right arrow> key to change the settings.

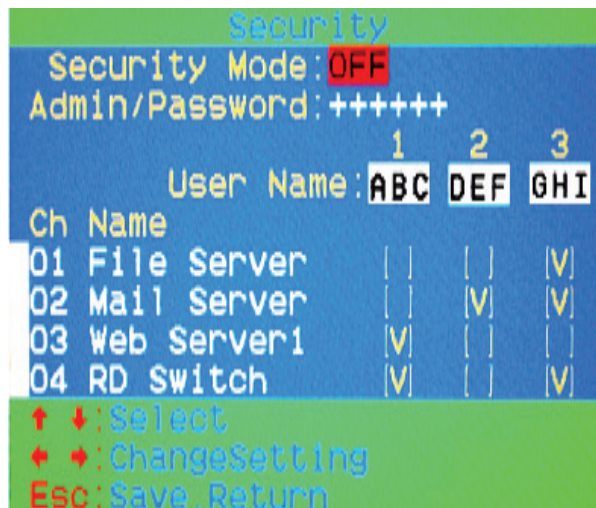


Figure 27: Security setup main window

7.7.2. Security Mode

To change the security mode setting, please move the highlight bar to **Security Mode**, and press <left arrow> or <right arrow> key to change it. The <F3> **Console Lock** and **user authority functions** can not be executed until the security mode is enabled.

7.7.3. Change administrator password

To change the administrator password, move the highlight bar to **Admin/password**, and press **<left arrow>** or **<right arrow>** key. The administrator password setup window will be shown on the screen. Input the new password twice and press **<ENTER>** to confirm, or press **<ESC>** to exit.

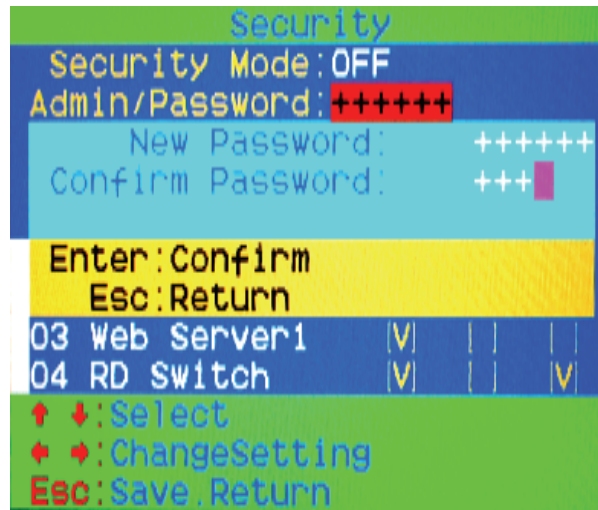


Figure 28: Administrator password setup window

7.7.4. Authorized user setup

3 authorized users are admitted to manage the KVM switch. To change the user name and password, please move the highlight bar to the user for editing. Press **<left arrow>** or **<right arrow>** key, the user name and password setup window will be shown on the screen. Please Input the new user's name and password twice, then press **<ENTER>** to confirm or **<ESC>** to cancel.

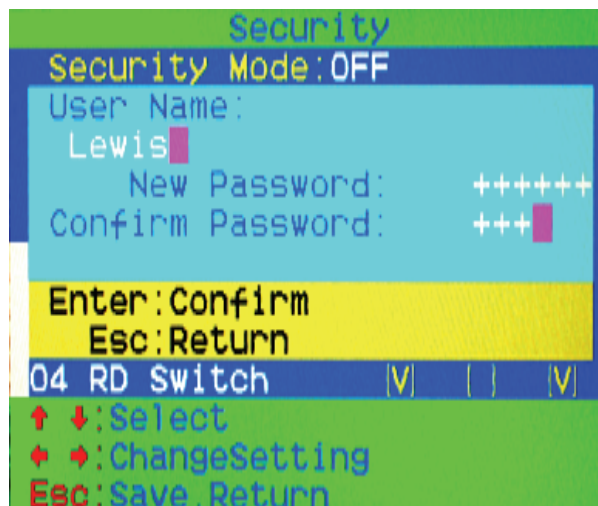


Figure 29: User name password setup window

7.7.5. User Authority setup

You can setup the authority which **only supports Layer 1 and Layer 2**, and **Layer 3 authority always enable for each user**. Different user has different

access right for each channel. To change the access authority of each channel for certain user, please move the highlight bar to the channel, and press **<A>**, **<1>**, **<2>** or **<3>** to setup the channel access authority for all or certain user. You don't have to setup the authority of administrator since the administrator has all channel access authorized right.

Please refer to section 7.2.2 and 7.2.3 to operate OSD menu properly.

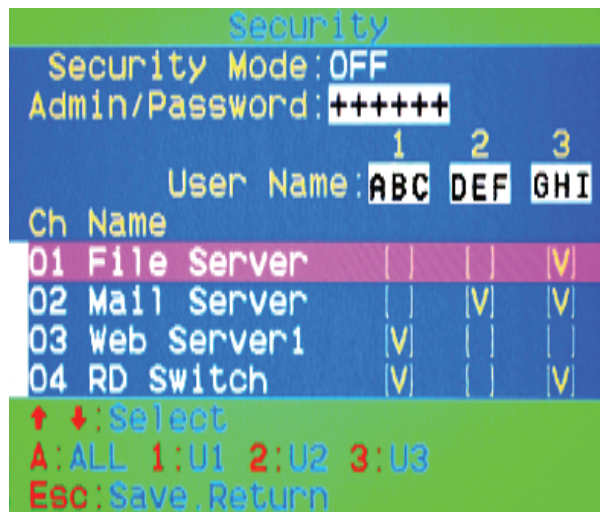


Figure 30: User authority setup window

7.8. Lock Port: <F6>

7.8.1. Lock Port

Only administrator can lock port. Please move the highlight bar to the channel to lock, and press **<F6>** to lock the selected channel. A red **L** mark will be shown in **STA** column of locked port.



Figure 31: Lock port in OSD main window

7.8.2. Channel selection of the locked port

If anyone selects the channel of the locked port either by panel push-button or hot key, the system will enter OSD mode waiting for administrator to unlock the port.

7.8.3. Unlock Port

Only administrator login with correct password can unlock the port. After the administrator login, the red **L** mark in **STA** column will disappear.

7.9. Exit OSD: <ESC>

Press <ESC> to exit OSD and to return to the selected computer. A banner with the channel name will be shown on left-upper corner of the screen.

7.10. Adjust Video in OSD

Please use <Up> or <Down> arrow key to options for video adjustment, and use <Left> or <Right> arrow key to change the value. Press <ESC> to exit and save the setup settings.



Figure 32: Adjust video window

8. Sun Microsystems Function Key Emulation:

There are 16 special functions on the Sun Microsystems keyboard, CAT5 Combo Free KVM Switch can emulate these function keys via PS/2 and/or USB keyboard. Please refer to the table shown below for Sun Microsystems keyboard special functions operation.

To active these emulation on the PS/2 and/or USB keyboard, you have to press the **<LEFT Window>** key first (this key usually is located between the **<LEFT CTRL>** and **<LEFT ALT>**). Then press the second key (Sun Microsystems Function Key). Please do not release **<LEFT Window>** when you press the second key.

Sun Microsystems Function Key	USB or PS/2 Keyboard
Stop	L_Win & L_Alt
Props	L_Win & L_Ctrl
Compose	L_Win & L_Shift
Front	L_Win & F1
Open	L_Win & F2
Find	L_Win & F3
Again	L_Win & F4
Undo	L_Win & F5
Copy	L_Win & F6
Paste	L_Win & F7
Cut	L_Win & F8
Help	L_Win & F11
Power	L_Win & F12
Mute	L_Win & 1
Volume Down	L_Win & 2
Volume UP	L_Win & 3

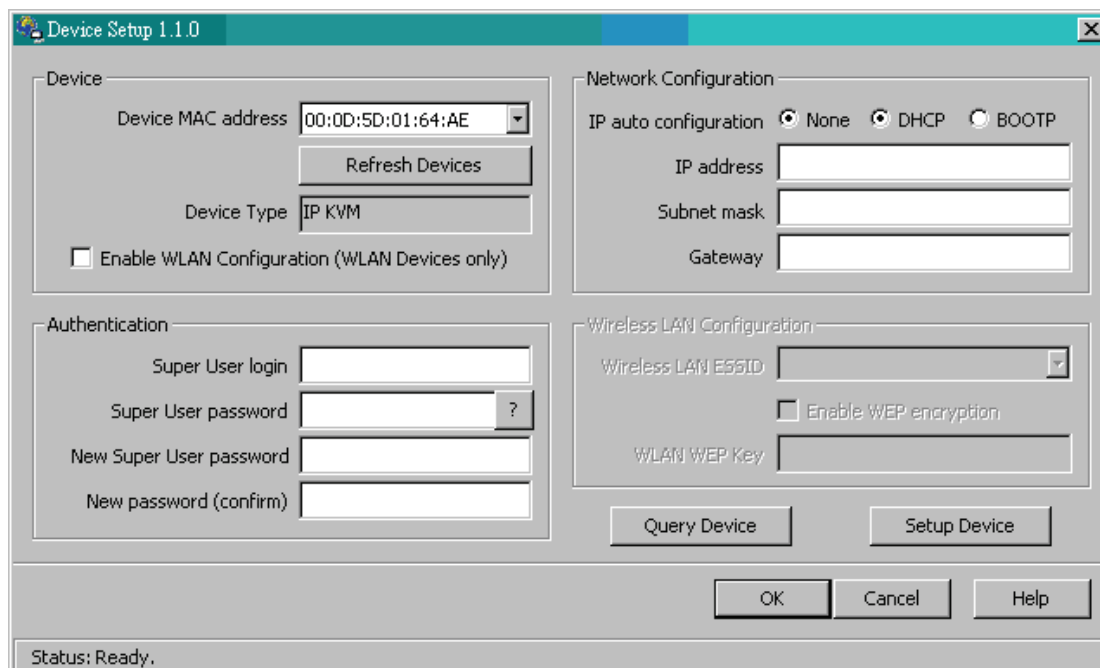
9 Configuration

9.1 Network configuration using PSetup utility

After the initial setup, the CAT5 8-PORT/16-PORT IP-KVM can be managed via the Internet using a standard browser that lets you control the device/s attached to it. However, to configure the CAT5 8-PORT/16-PORT IP-KVM's network access, the user must first run the PSetup Utility software that is included on the CD-ROM included in your package.

The PSetup Utility lets you set up the CAT5 8-PORT/16-PORT IP-KVM's network configuration (IP address, Subnet mask, DHCP, etc) from any computer that is connected to the same subnet. This program is also useful if you ever need to view or change the network settings of the unit. If the initial or default basic configuration does not meet your requirements, use the PSetup program to change the configuration to suit your needs.

When open the PSetup Utility on your computer, the PSetup Utility window (see the screenshot below) will appear.



The screenshot shows the 'Device Setup 1.1.0' window. It is divided into several sections: 'Device' with a MAC address dropdown (00:0D:5D:01:64:AE) and a 'Refresh Devices' button; 'Network Configuration' with radio buttons for 'None', 'DHCP', and 'BOOTP', and input fields for 'IP address', 'Subnet mask', and 'Gateway'; 'Authentication' with input fields for 'Super User login', 'Super User password', 'New Super User password', and 'New password (confirm)'; and 'Wireless LAN Configuration' with a 'Wireless LAN ESSID' dropdown, an 'Enable WEP encryption' checkbox, and a 'WLAN WEP Key' input field. At the bottom, there are buttons for 'Query Device', 'Setup Device', 'OK', 'Cancel', and 'Help'. A status bar at the very bottom indicates 'Status: Ready.'

To use the PSetup Utility, please follow the procedures described below.

Finding the CAT5 8-PORT/16-PORT IP-KVM on your network via the Psetup Utility:

- 1) Make sure the computer you are using to set up the CAT5 PORT/16-PORT IP-KVM is connected to the same local network that the CAT5 8-PORT/16-PORT IP-KVM is connected to.
- 2) Open the PSetup Utility on your computer. The PSetup Utility window (see the screenshot above) will appear.

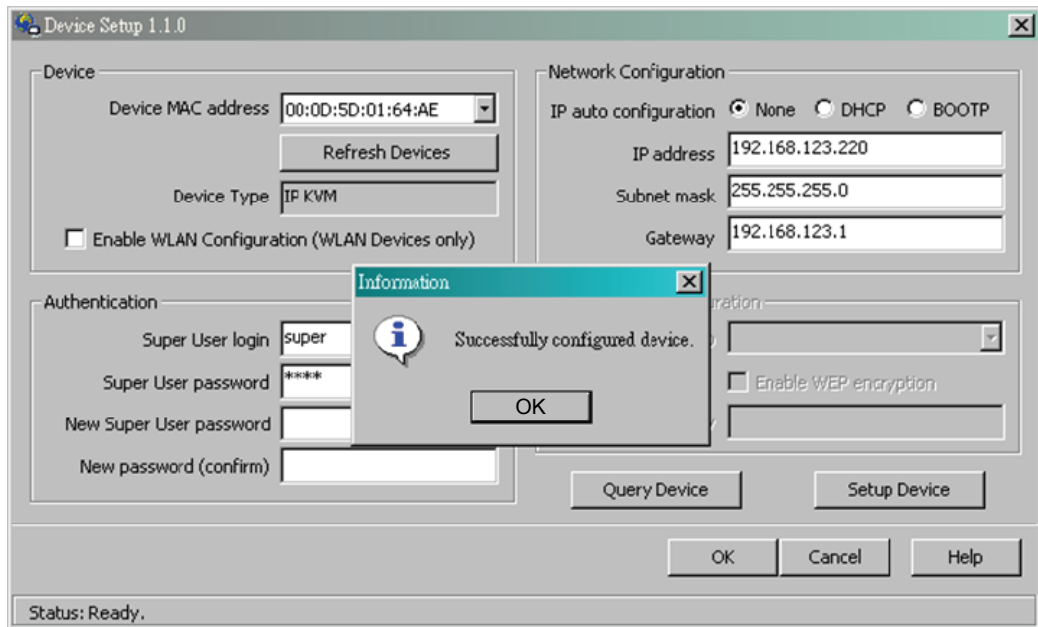
3) Use the **PSetup** Utility to search for the CAT5 8-PORT/16-PORT IP-KVM on your network:

- a) Click the **Refresh Devices** button to show the MAC addresses of all connected devices on your network.
- b) Find the MAC address of the CAT5 8-PORT/16-PORT IP-KVM by clicking on the “Device MAC Address” drop-down box. Select your device’s MAC address from the dropdown list.
- c) After selecting your CAT5 8-PORT/16-PORT IP-KVM’s MAC address, click Query Device to view the device’s Network Configuration in the top right area.
- d) By default, the DHCP function is disabled, and “None” will be selected for “IP auto configuration”. This means there would initially be a static IP address for the device. You can now configure the CAT5 8-PORT/16-PORT IP-KVM to use a static IP address, or you can turn on DHCP to automatically obtain an IP address from a DHCP server on your network. Both configurations are described in the following steps.

Note: We recommend that you manually set up a static IP address that is linked to the MAC address of your CAT5 8-PORT/16-PORT IP-KVM.

Setting up a static IP via the PSetup Utility:

- 1) Make sure that the correct MAC address is selected in the “Device” field at the top left of the PSetup Utility window.
- 2) Click **Query Device** (at bottom right) to view the device’s Network Configuration in the top right area.
- 3) In the “IP auto configuration” line at the top right, select “**None**”.
- 4) Enter the IP address, subnet mask, and gateway you want the CAT5 8-PORT/16-PORT IP-KVM to use.
- 5) In the Authentication area, enter the Super User login and password for the CAT5 8-PORT/16-PORT IP-KVM. The default login is **super**, and the default password is **pass**.
- 6) Click the **Setup Device** button. If the Super User login and password are correct, a “Successfully configured device” message will appear.
- 7) The CAT5 8-PORT/16-PORT IP-KVM’s web management interface can now be accessed via the Internet by simply browsing to the same IP address from a web browser.

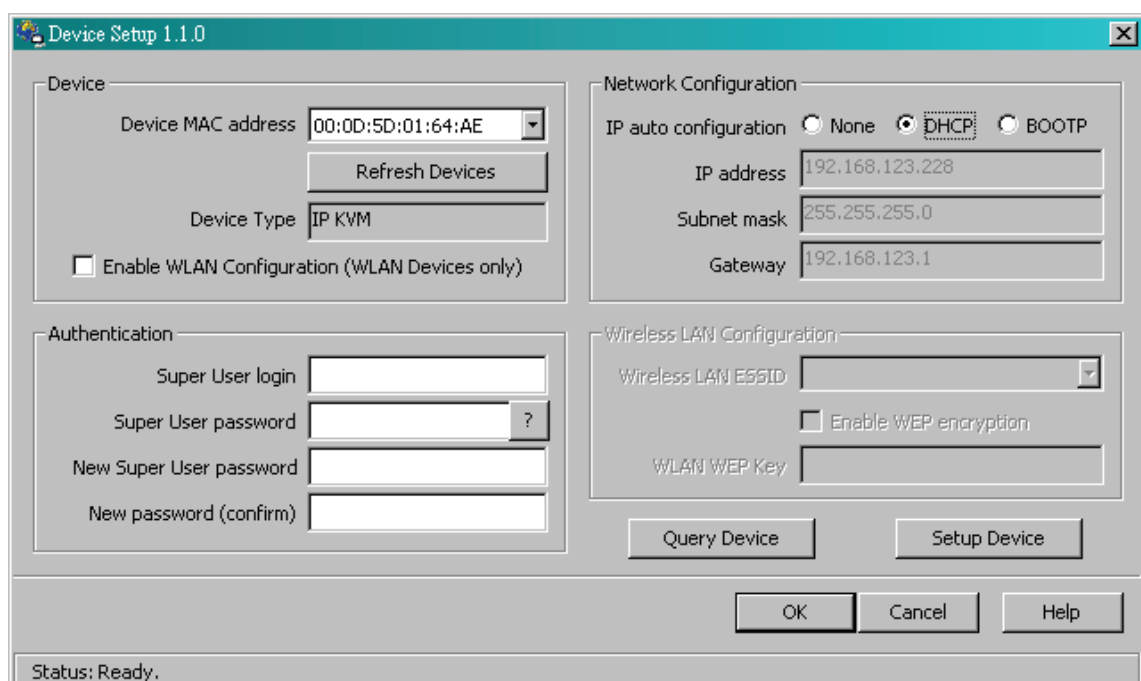


Enabling DHCP to get a dynamic IP address:

If you have installed the CAT5 8-POR/16-POR IP-KVM on the subnet (intranet) of a DHCP server, or the subnet of a router that supports DHCP, you can use the PSetup Utility to find the dynamic IP address of the CAT5 8-POR/16-POR IP-KVM. DHCP automatically assigns a dynamic IP address to the CAT5 8-POR/16-POR IP-KVM. This allows a device to be automatically assigned an IP, eliminating the need for intervention by a network administrator, who would otherwise have to manually assign the CAT5 8-POR/16-POR IP-KVM a static IP address.

- 1) Before connecting the CAT5 8-POR/16-POR IP-KVM to your network, make sure you complete the configuration of the network's DHCP server. The network's router may be acting as your network's DHCP server, or another device may be acting as the DHCP server.
- 2) Connect the CAT5 8-POR/16-POR IP-KVM to your network by using an Ethernet cable. Connect one end to your network, and the other end to the Ethernet port of the CAT5 8-POR/16-POR IP-KVM.
- 3) The DHCP function of the router/server will now automatically assign an IP address to the CAT5 8-POR/16-POR IP-KVM.
- 4) Make sure that the computer you are using to set up the CAT5 8-POR/16-POR IP-KVM is connected to the same network that the CAT5 8-POR/16-POR IP-KVM is connected to.
- 5) Open the PSetup Utility on your computer. The PSetup Utility window (see the screenshot above) will appear.

- 6) Use the PSetup Utility to search for the CAT5 8-PORT/16-PORT IP-KVM on the network (see the image below):
 - a) Click the **Refresh Devices** button to detect all connected devices.
 - b) Find the MAC address of the CAT5 8-PORT/16-PORT IP-KVM by clicking on the “Device MAC Address” drop-down box. Select your device’s MAC address from the dropdown list.
 - c) After selecting your CAT5 8-PORT/16-PORT IP-KVM’s MAC address, click Query Device (see the screenshot below) to view the device’s Network Configuration in the top right area.
 - d) In the “IP auto configuration” line at the top right, select “DHCP”.
 - e) In the Authentication area, enter the Super User login and password for the CAT5 8-PORT/16-PORT IP-KVM. The default login is **super**, and the default password is **pass**.
 - f) Click the **Setup Device** button. If the Super User login and password are correct, a “Successfully configured device” message will appear.
 - g) The CAT5 8-PORT/16-PORT IP-KVM will now try to contact a DHCP server in the subnet to which it is physically connected. If contact is made with a DHCP server, it will provide the CAT5 8-PORT/16-PORT IP-KVM with a dynamic IP address, subnet mask, and gateway.
 - h) Click the **Query Device** button again, and the device’s dynamic IP address and other network information should now be visible in the Network Configuration field (see the screenshot below).



Notes:

- **BOOTP**, a static configuration protocol, uses a table that maps IP addresses to physical addresses.
- **DHCP**, an extension to BOOTP that dynamically assigns configuration information. DHCP is backward compatible with BOOTP.

The factory default settings for the CAT5 8-PORT/16-PORT IP-KVM unit are as below:

DHCP: Disabled

Default IP address: 192.168.0.70

Default Subnet mask: 255.255.255.0

IN SHORT: If the currently selected device has DHCP selected for its Network Configuration, click OK and the CAT5 8-PORT/16-PORT IP-KVM will try to contact a DHCP server in the network to which it is physically connected. If contact is made with a DHCP server, it will provide the CAT5 8-PORT/16-PORT IP-KVM with a dynamic IP address, gateway address and subnet mask.

Changing your device's password through the PSetup Utility:

To change your password with the PSetup Utility, select your device from the Device MAC Address drop-down box, then in the "Authentication" section in the bottom-left part of the window, enter the Super User login and current password for your CAT5 8-PORT/16-PORT IP-KVM. The default login is **super**, and the default password is **pass**. Now enter your new password in the "New Super User password" text box, and enter it again in the "New Password (confirm)" text box to confirm it.

To save your new password and close the window, click the **OK** button. Otherwise, click the **Cancel** button.

WARNING:

Please make sure that you change the default Super User password immediately after you have installed and accessed your CAT5 8-PORT/16-PORT IP-KVM for the first time. Leaving the password as it is represents a severe security risk and may result in unauthorized access to the CAT5 8-PORT/16-PORT IP-KVM as well as the entire Remote console system and connected devices. The password can be changed in the setup program (as described above) or online on the browser-based Web Management GUI. Make sure you write your password down in a safe place.

NOTE:

Your web browser has to be set up to accept cookies, or else you won't be able to log in. If you experience login problems, check to see if your browser has been set up to accept cookies.

9.2 Configuration Setup via Serial Console

For connecting to serial-based terminals, the CAT5 8-PORT/16-PORT IP-KVM has a serial cable interface (for setup on the Host side). This connector is compliant with the RS-232 serial line standard. The serial connection has to be configured with the parameters given in Table below.

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

When configuring your device from a serial-based terminal such as Hyper Terminal, reset the CAT5 8-PORT/16-PORT IP-KVM and immediately press the “ESC” key. You will see some device information, and a “=>” prompt. Type in “config”, press the “Enter” key and wait a few seconds for the configuration questions to appear. As you proceed, you will be prompted for the following settings one after the other. To accept the default values shown in square brackets below, press the “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

You can specify whether the CAT5 8-PORT/16-PORT IP-KVM should get its network settings from a DHCP or BOOTP server. To enable IP auto-configuration via DHCP, type “dhcp” in the “IP auto-configuration” line. For BOOTP, type “bootp”. Press “Enter” to apply the setting.

If you do not specify either of these two options, IP auto-configuration will be disabled (it will be static IP configuration) and you will be asked for the following network settings:

IP address

Enter the IP address for the CAT5 8-PORT/16-PORT IP-KVM. This option is only available if IP auto-configuration is disabled.

Net mask

Enter the subnet mask of the connected IP subnet. This option is only available if IP auto-configuration is disabled.

Gateway address

Enter 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.

9.3 Keyboard, Mouse, and Video configuration

Between the CAT5 8-PORT/16-PORT 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.

9.3.1 CAT5 8-PORT/16-PORT IP-KVM keyboard settings

The keyboard model emulated by the CAT5 8-PORT/16-PORT IP-KVM must be set properly in order for keystrokes received by the Host computer to match the ones sent by a Remote computer. View these settings in the CAT5 8-PORT/16-PORT IP-KVM's Web Management GUI.

9.3.2 Remote Mouse Settings

A common problem with KVM devices is the synchronization between the Host-side and Remote-side mouse cursors. The CAT5 8-PORT/16-PORT IP-KVM resolved this problem with an intelligent synchronization algorithm. There are two mouse modes available on the CAT5 8-PORT/16-PORT 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 so that one pixel of movement will result in “n” number of pixel moves on the Host system. The value of “n” is adjustable. Please note that this works only when mouse acceleration settings are turned off on the Host computer.

9.3.3 Automatic mouse speed and mouse synchronization

The automatic mouse speed mode performs the speed detection during mouse synchronization. Whenever the Host-side and Remote-side mouse cursors move synchronously or not, there are two ways for re-synchronizing Host-side and Remote-side 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 hot-key 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 Sync. It 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.

9.3.4 Single and Double Mouse Mode

The CAT5 8-PORT/16-PORT IP-KVM features two different mouse synchronization modes: Double Mouse mode, and Single Mouse mode.

Double Mouse Mode: In this mode, both the Remote and Host mouse pointers are visible, allowing you to control the Host computer on your Remote computer while allowing you to move the mouse outside the Remote Console window. In this

mode, the mouse pointers may need to be synchronized in order to ensure they are pointing at the same position on your Host computer screen. You can define a hotkey to quickly sync the two mouse pointers.

Single Mouse Mode: In this mode, only one mouse pointer is visible – the Remote computer pointer. On the Remote computer, when you click on the Remote Console window, your mouse pointer will be “captured”, and all mouse movement will be inside the Remote Console window only. In order to “free” the Remote computer’s mouse pointer, you will need to use a hotkey to “release” the mouse pointer from the Remote Console window. The default hotkey for this is “Alt + F12”.

9.3.5 Host system mouse settings

While the CAT5 8-PORT/16-PORT IP-KVM supports accelerated mouse movements and is able to synchronize the Host-side pointer with the Remote-side mouse pointer, there are a few operating systems that limit this functionality and may prevent this synchronization from working properly. If you experience issues with mouse synchronization, please try the following:

Special Mouse Driver

Specific mouse drivers may influence the synchronization process and impede synchronization of dual mouse pointers. If this happens, make sure you are not using a special vendor-specific mouse driver on your Host system.

Windows Settings

All versions of Windows (on Host computer): In the CAT5 8-PORT/16-PORT IP-KVM’s web GUI, select “Auto Mouse Speed” (in KVM Settings > Keyboard/Mouse).

Windows 2000 (on Host computer): On the Host computer, you will need to go to Control Panel > Mouse > Motion > Acceleration and make sure “Improve Mouse Acceleration” is disabled.

Windows XP/Vista/7 (on Host computer): On the Host computer, you will need to go to Control Panel > Mouse > Pointer Options and make sure “Enhance Pointer Precision” is disabled.

Active Desktop

If the “Active Desktop” feature of Microsoft Windows is enabled, do not use a plain background. Instead, use a wallpaper image. Alternatively, disable “Active Desktop” completely.

Mac OS X Settings

Mac OS X (on Host computer): If the host computer is running on any version of Mac OS X, we recommend using Single Mouse mode.

SUN Solaris Settings

SUN Solaris (on Host computer): If the host system is running SUN Solaris, adjust the mouse settings of the system by entering “xset m 1” into the console, or use the CDE Control Panel to set the mouse to “1:1, no acceleration”. Alternatively, you could use the Single Mouse mode only. On SUN operating systems, Double Mouse Mode only functions if you use SUN JVM 1.5 or higher.

9.3.6 Video Modes

The CAT5 8-PORT/16-PORT IP-KVM recognizes a limited number of common video modes. If you run X11 on the host system, please do not use any custom mode lines with special video modes. If you do, the CAT5 8-PORT/16-PORT IP-KVM may not be able to detect them. We recommend using any of the standard VESA video modes instead.

.

10 Usage

10.1 Prerequisites

The CAT5 8-PORT/16-PORT IP-KVM features an embedded operating system and applications that support two standardized interfaces – HTTP/HTTPS and Telnet. This chapter will describe both these interfaces in detail, as well as how to use them. Both interfaces are accessed using the TCP/IP protocol family.

■ HTTP/HTTPS

Full access is provided by the embedded web server. The CAT5 8-PORT/16-PORT IP-KVM environment can be entirely managed by using a standard web browser. You can access the CAT5 8-PORT/16-PORT IP-KVM by using the non-secure HTTP protocol, or by using the encrypted HTTPS protocol. For security purposes, we suggest using HTTPS whenever possible.

■ Telnet

A standard Telnet client can be used to access an arbitrary device that is connected to the CAT5 8-PORT/16-PORT IP-KVM's serial port in terminal mode.

■ HTTP as the Primary Interface

The primary interface of the CAT5 8-PORT/16-PORT IP-KVM is the HTTP interface. This will be covered extensively in this chapter. Other interfaces are addressed in sub-topics.

In order to open the Remote Console window of your managed host system, the browser must support version 1.5 or above of the Java Runtime Environment. If the browser has no Java support (such as on a small handheld device), you can still manage your CAT5 8-PORT/16-PORT IP-KVM by using the administration forms displayed by the browser itself.

For a secure connection to the CAT5 8-PORT/16-PORT IP-KVM, we recommend the following browsers versions:

- Microsoft Internet Explorer version 6.0 or higher
- Netscape Navigator 7.0
- Mozilla 1.6 or higher

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 browser that supports a 128-bit passkey. Some older

browsers do not have a strong 128-bit encryption algorithm.

If you are using Internet Explorer, click on the top toolbar menu option marked “?”, then click on “About Internet Explorer” to see the current “Cipher Strength” (the passkey length that is currently activated). The dialog box contains a link that leads you to information on how to upgrade your browser to a more powerful encryption scheme. The screenshots below shows the dialog boxes presented by IE 8 and IE 6.



Figure 33: The Internet Explorer displaying the encryption key length

Newer web browsers generally support strong encryption by default.

10.2 Log in/out CAT5 8-PORT/16-PORT IP-KVM

10.2.1 Log in the CAT5 8-PORT/16-PORT IP-KVM

The CAT5 8-PORT/16-PORT IP-KVM has three levels of access privileges:

User Name	Default Password	Access Privileges
super (factory default)	pass (factory default)	Full access
administrator	(user-define)	Partial rights to configure the settings of critical functions
user	(user-define)	Rights to access basic functions of the Open Remote Console

The **super** user can add or remove a user easily via the web pages of **User Management > Users**. Please refer to Addendum C for details on what access rights are assigned for each user level.

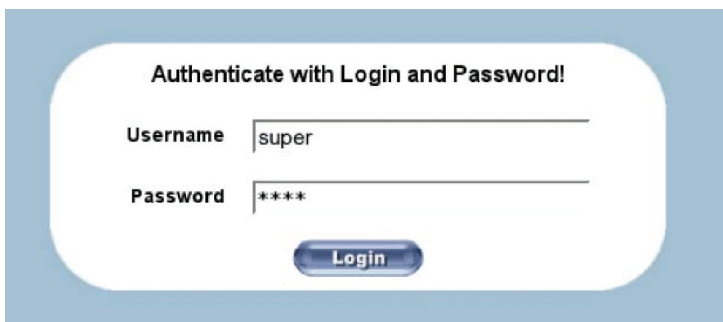
Launch your web browser and type in the IP address that you configured for your CAT5 8-PORT/16-PORT IP-KVM during the installation process. The address might be an IP address or a domain name, in the case where you have given your CAT5 8-PORT/16-PORT IP-KVM a symbolic name in the DNS. For instance, type the following in the URL field of your browser when establishing a non-secured connection:

http://<IP address of IP-KVM>

When using a secure connection, type in:

https://<IP address of IP-KVM>

The browser will open the IP-KVM login page, as shown below:



If you connect to the CAT5 8-PORT/16-PORT IP-KVM unit, the CAT5 8-PORT/16-PORT IP-KVM system (via its web server, Telnet server, or SSH server) will prompt you to enter your username and password in order to access the system. If this is the first time you log in, log in with the factory default username super and password pass, after which you will be prompted to change the default password.

WARNING:

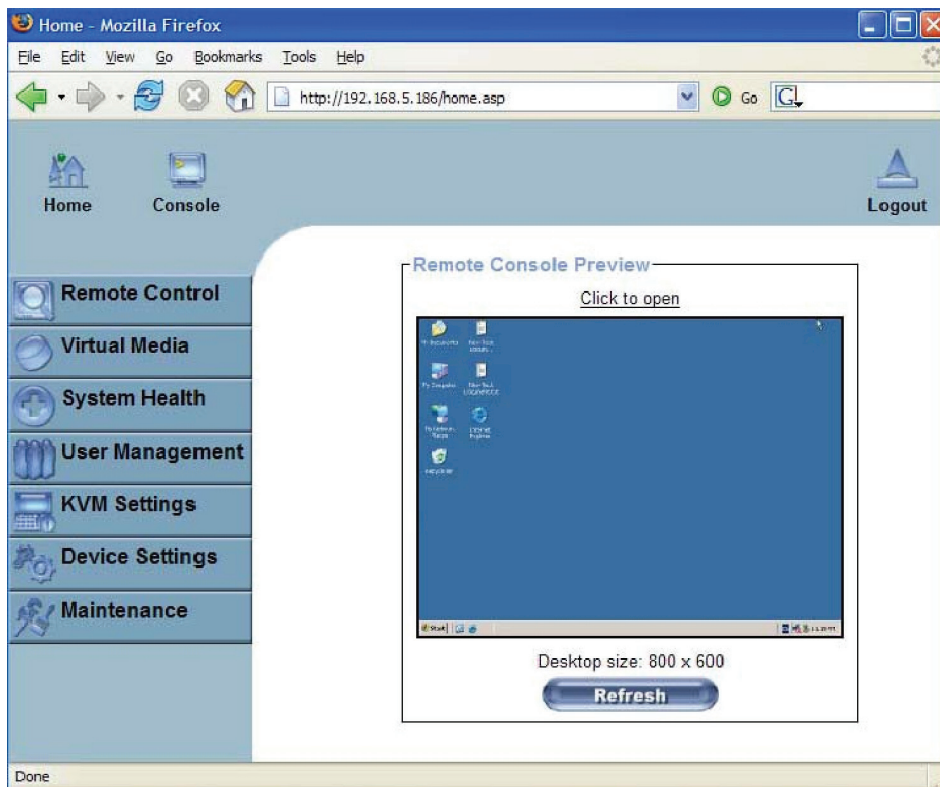
Please make sure that you change the default Super User password immediately after you have installed and accessed your CAT5 8-PORT/16-PORT IP-KVM for the first time. Leaving the password as it is represents a severe security risk and may result in unauthorized access to the CAT5 8-PORT/16-PORT IP-KVM as well as the entire Host system and connected devices!

NOTE:

Your web browser has to be set up to accept cookies, or else you won't be able to log in.

Navigation

After successfully logging into the CAT5 8-PORT/16-PORT IP-KVM, the main page of the IP-KVM web management GUI will appear. This page consists of three parts; each of them contains specific information. The buttons on the upper side are clickable shortcuts to go to the main page, to open the Remote Console or to log out. The left-hand column displays the configuration categories. Clicking on each configuration category will give a submenu of configuration/command options.





Home

Return to the main page of the IP-KVM's web GUI



Console

Open the IP-KVM Remote Console



Logout

Log out and exit from the IP-KVM's web GUI.

NOTE:

If there is no user activity for 30 minutes, the CAT5 8-POR/16-POR IP-KVM will log you out automatically. Clicking on any of the menu items will bring you back to the login screen.

Remote Console Preview

Click on **Click to open** to start the remote console redirection

Click on **Refresh** to refresh the picture.



10.2.2 Log out from the CAT5 8-POR/16-POR IP-KVM

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.

10.3 The Remote Console

The Remote Console is the redirected screen, keyboard and mouse of the remote host system that CAT5 8-PORT/16-PORT IP-KVM controls.

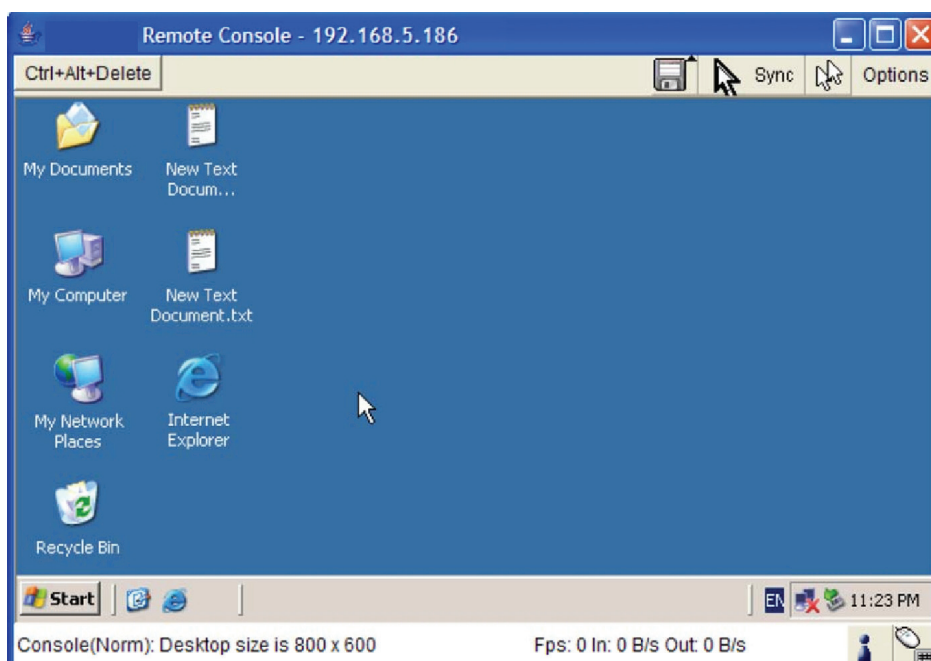
The Remote Console window is a Java Applet that tries to establish its own TCP connection to the CAT5 8-PORT/16-PORT IP-KVM. The protocol that is running over this connection is neither HTTP nor HTTPS, but RFB (Remote Frame Buffer Protocol). By default, RFB tries to establish a connection to TCP port 443. Your local network environment must 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.

If the CAT5 8-PORT/16-PORT IP-KVM is connected to your local network environment and your connection to the Internet is available by using a proxy server without NAT being configured, it is unlikely that the Remote Console will be able to establish the desired connection. This is because modern web proxies are not capable of relaying the RFB protocol.

If you experience any problems, please consult your network administrator to configure an appropriate networking environment.

10.3.1 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 in the left-hand column or click the **Click to open** link at the top of the Remote Console picture on the right.



Activating the Remote Console function opens a new window on the Remote-side user's screen. This window displays the screen content of your host system. The

Remote Console will behave exactly in the same way as if you were sitting in front of it. This means you can use your keyboard and mouse in the usual way. However, be aware of the fact that the feedback from keyboard and mouse actions on the Host system will be slightly delayed. The delay depends on the bandwidth of the between you and the CAT5 8-PORT/16-PORT IP-KVM.

Differences between the Remote computer's keyboard layout and the Host computer's keyboard settings may lead to some problems. For example, if the Remote-side user uses a German keyboard layout and the Host system is set up for an English keyboard layout, special German-specific keys on the German keyboard will not work as expected. Instead, the keys will have the same effect as those of an English-layout keyboard. The Remote-side user can circumvent such problems by adjusting the keyboard settings of the Host system to have the same mapping as the Remote user's keyboard.

The Remote Console window always tries to show the remote screen with its optimal size. That means it will resize the window to fit the Remote-side user's screen by default 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 is just another window on the Remote-side user's system. To get control of the Host system, the Remote-side user first needs to click inside the Host window to give it focus. In Single Mouse mode, this action will capture the mouse pointer, so all mouse input is directed to the Host computer, and making the Remote computer's mouse pointer disappear. To release the mouse from this captured state, use the Mouse hotkey. The default hotkey for this is Alt+F12, but this hotkey can be reconfigured manually.

10.3.2 Control Bar of Remote Console

The upper part of the Remote Console window contains a control bar. By clicking on the icons on this bar, you can view the state of the Remote Console and adjust the local Remote Console settings. The following is a description for each control:

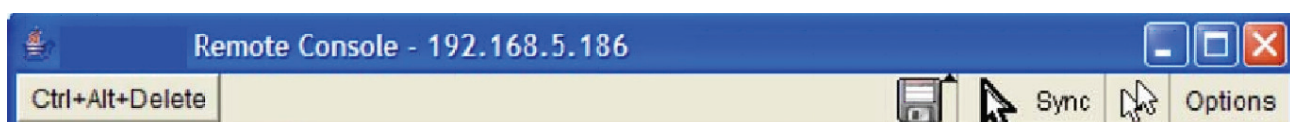
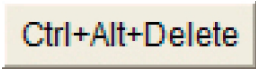


Figure 34: Remote Console Control Bar

Ctrl+Alt+Delete

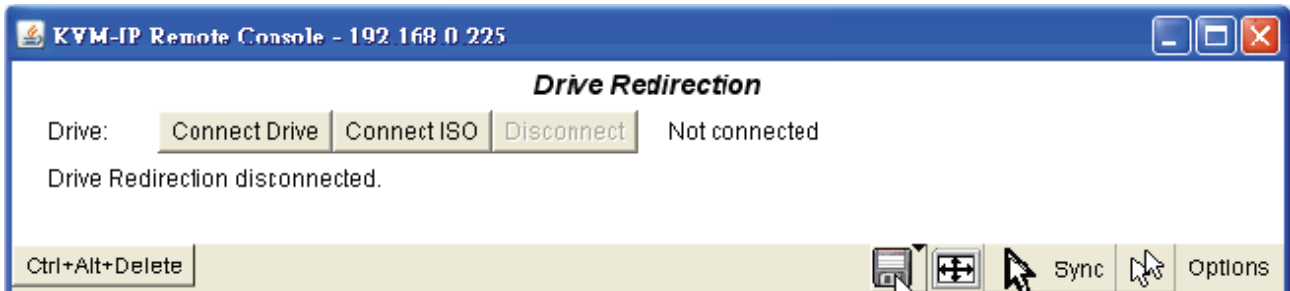
A rectangular button with a light beige background and a thin border, containing the text "Ctrl+Alt+Delete" in a dark font.

Click this button to send the “Control Alt Delete” key-sequence command to the remote system. (Also, see section 5.4.1 for configuring new key-sequence buttons).

Drive Redirection button



Click this button to open the Drive Redirection options at the top of the Remote Console window (see the screenshot below). For more details, see section 11.2.

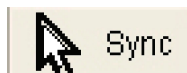


Auto Adjust button



If the quality of the Remote Console video is bad, or if the Remote Console window is distorted in some way, click this button and wait a few seconds while the CAT5 8-POR/16-POR IP-KVM tries to detect the video mode of the VGA connection of the Host system to the CAT5 8-POR/16-POR IP-KVM. Once detection is complete, the CAT5 8-POR/16-POR IP-KVM will adjust itself for the best possible video quality.

Sync mouse



Clicking this button activates the mouse synchronization process. Choose this option to synchronize the Host-side mouse cursor with the Remote-side mouse cursor. (Double Mouse Mode only).

Single/Double mouse mode



Clicking this button switches between Single Mouse Mode (where only the Host-side mouse pointer is visible) and the Double Mouse Mode (where the Host-side and Remote-side mouse pointers are both visible and need to be synchronized). On SUN operating systems, Double Mouse Mode only functions if you use SUN JVM 1.5 or higher. We recommend using only Single Mouse Mode on Mac OS X systems. For more information on Single and Double Mouse mode and troubleshooting mouse synchronization, please refer to Section 9.3.4.

Options Options

Click on this button to open the “Options” menu.

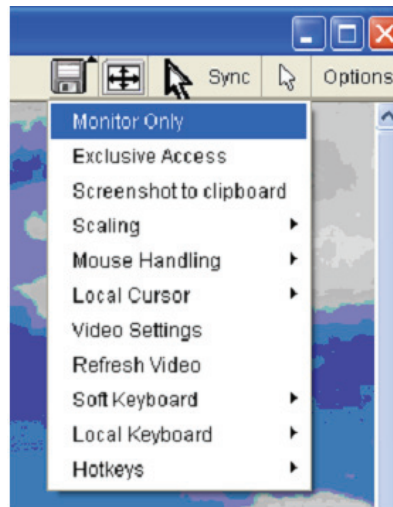


Figure 35: Remote Console Options Menu

A short description of the options as follows.

- **Monitor Only**

Click this command to toggle the Monitor Only function on or off. If this function is switched on, the Remote-side user can only monitor the Host-side user’s console, and cannot control it.

- **Exclusive Access**

If a user has the appropriate administration rights, he or she can force a shutout of all other Remote-side users from a Host system, so that he or she alone can control the Host systems. No one can re-open the selected Remote Consoles until this user deactivates Exclusive Access, or logs off.

The Access Mode icon in the status bar at the bottom of the screen will indicate the current status of the Exclusive Access function (see the screenshot below).



Figure 36: Remote Console Exclusive Mode

- **Screenshot to Clipboard**

Click on this menu item to take a screenshot of the Host view window. The screenshot will be saved to the clipboard of the Remote computer.

- **Scaling**

This allows the Remote-side user to scale down the Remote Console window on their monitor. The mouse and keyboard controls will stay the same, but the scaling algorithm will not preserve all the display details.

When you select 25%, 50%, or 100% scaling, the size of the Remote Console window is calculated according to the Host video settings and the scaling algorithm. When you select “Scale to fit”, the Host video display will fit into the size and shape of the window for the Remote Console, no matter how this window is resized by the Remote-side user.

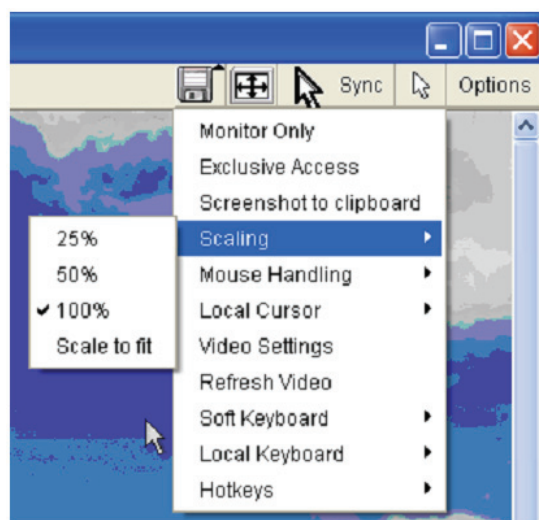
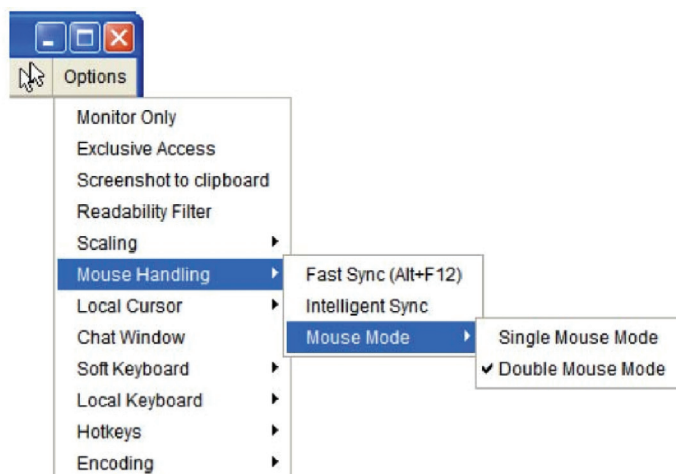


Figure 37: Remote Console Options Menu: Scaling

- **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.

- **Local Cursor**

This submenu offers a list of different cursor shapes for the mouse pointer visible by the Remote user. 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 pointer shapes depends on the version of the Java Virtual Machine installed on the Remote computer; version 1.5 or above will offer the full list.

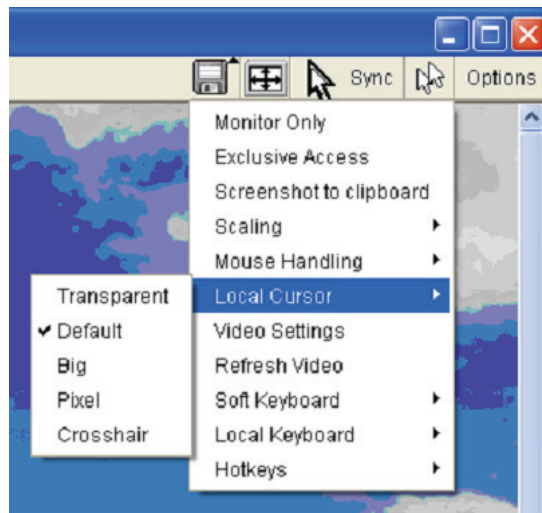


Figure 38: Remote Console Options Menu

- **Video Settings**

This submenu opens a panel for changing the CAT5 8-POR/16-POR IP-KVM video settings. The CAT5 8-POR/16-POR IP-KVM has two separate areas where different video settings can be configured. One area is the Remote Console window's Options menu, the other area is in the CAT5 8-POR/16-POR IP-KVM's web interface configuration menus.

Video Settings via the Remote Console's "Options > Video Settings"

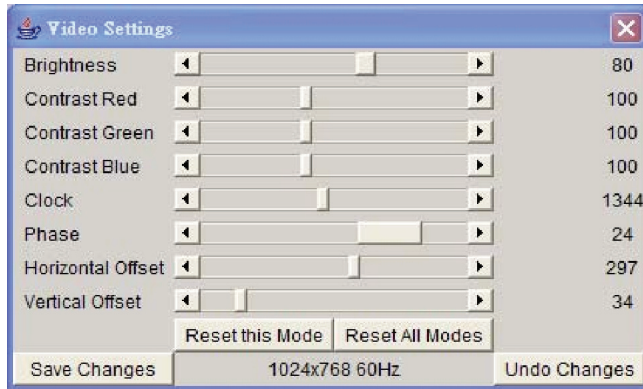


Figure 39: Video Settings Panel

Brightness - Controls the brightness of the picture

Contrast Red/Green/Blue - Controls the contrast of the picture

Clock - Defines the horizontal frequency for 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 most configurations. If the picture quality still has problems after auto adjustment, you can try to adjust this setting together and the Phase setting, as mentioned below.

Phase - Defines the phase for video sampling. This is used with the above-mentioned Clock setting to control the display quality.

Horizontal Position - Defines the horizontal positioning of the video.

Vertical Position - Defines the vertical positioning of the video.

Reset this Mode - Resets video mode-specific settings (Clock , Phase and Position) to the factory defaults.

Reset all Modes - Reset all settings to the factory defaults.

Save changes - Save changes permanently

Undo Changes - Restore last settings

Video Settings via the Web Management GUI

To set the video feed's "Noise Filter", use the CAT5 8-PORT/16-PORT IP-KVM's web management GUI. In the left-hand column, click on KVM Settings > Video. This will open the Miscellaneous Video Settings screen.

The "Noise Filter" option defines how the CAT5 8-PORT/16-PORT 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 interference, and can help lower unnecessary bandwidth consumption. A large filter setting needs less network data traffic and enables a faster

video display, but some small changes in the display may not be recognized immediately. A small filter setting displays all changes instantly, but may lead to a constant stream of network traffic, even if the display content is not actually changing (depending on the quality of the video input signal). In general, the default setting should be suitable for most situations.

Click the “Force Composite Sync” button if you are using a SUN computer or server on the Host-side.

After adjusting any settings, click the **Apply** button to save your changes.

- **Refresh Video**

Click this menu item in the Options menu list of the Remote Console to refresh the video stream coming from the Host system. Usually, only the parts of the video feed that have changed will be sent from the CAT5 8-PORT/16-PORT IP-KVM in order to save network bandwidth. This function is mainly for troubleshooting issues that may occur when old video fragments are not updated quickly for some reason. One of the reasons for this could be that the “Noise Filter” setting for video has been set too high. To adjust the Noise Filter setting, please refer to the previous section.

- **Soft Keyboard**

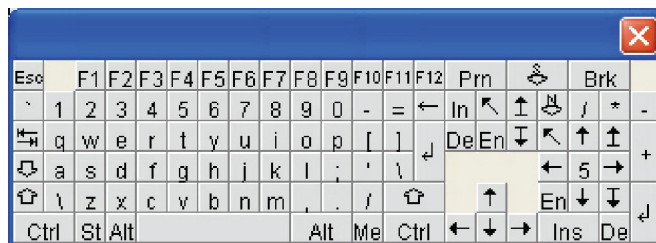


Figure 40: Soft Keyboard

Click this menu item to open up the submenu for the Soft Keyboard.

Show

Clicking this item brings up the Soft Keyboard. The Soft Keyboard may be necessary if your Host system runs a completely different language and country mapping than your Remote computer.

Mapping

This menu item is used for choosing the specific language and country mapping of the Soft Keyboard.

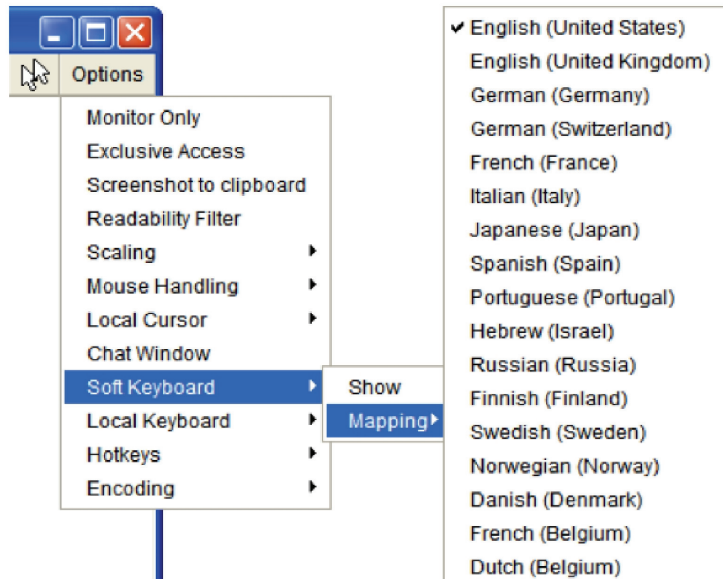


Figure 41: Soft Keyboard Mapping

- **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**

This menu item opens a list of pre-defined hotkeys, which is useful for hotkey combinations that may be difficult to send, such as CTRL+ALT+DEL. Click any entry and that specific command will be sent to the Host system.

A confirmation dialog will appear before the system sends the selected command to the Host system. Click the OK button execute the key combination on the Host system.

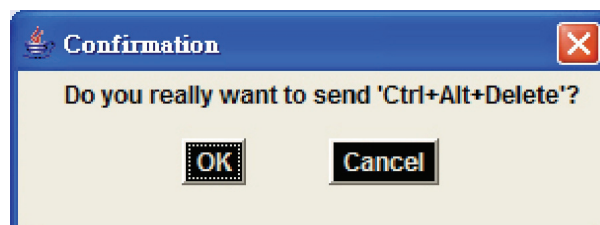
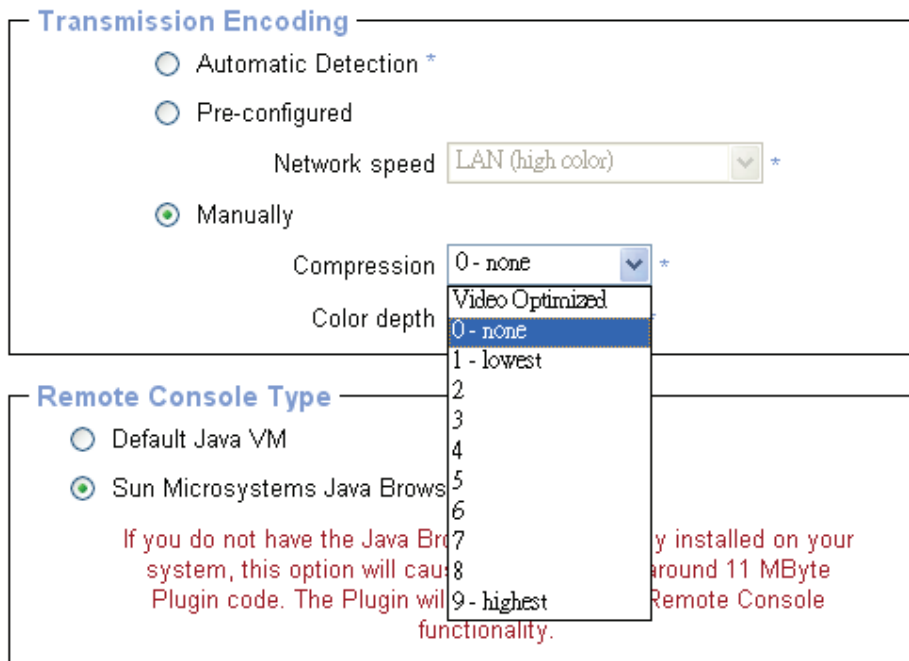


Figure 42: Remote Console Confirmation Dialog

- **Encoding**

These options are used to adjust the encoding level in terms of compression and color depth. They are available only when "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 to use 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.

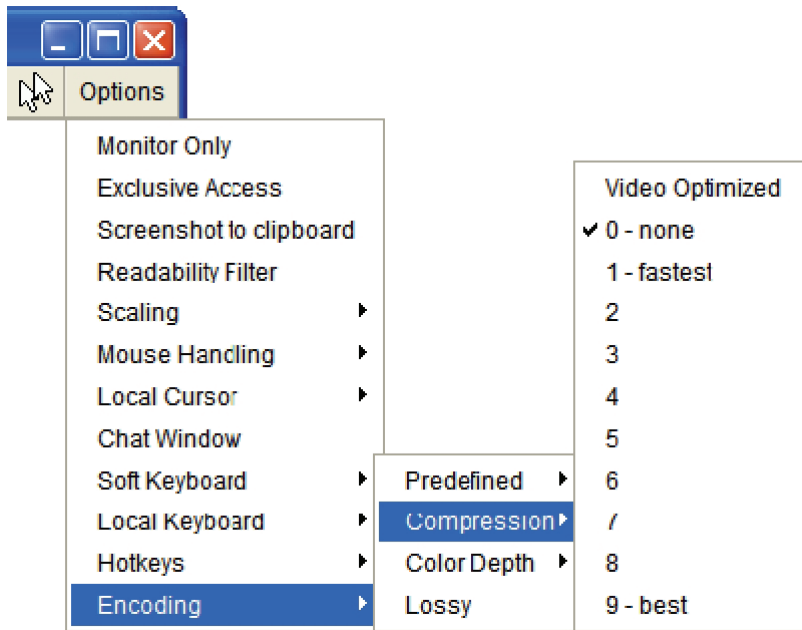


Figure 43: Encoding Compression

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.

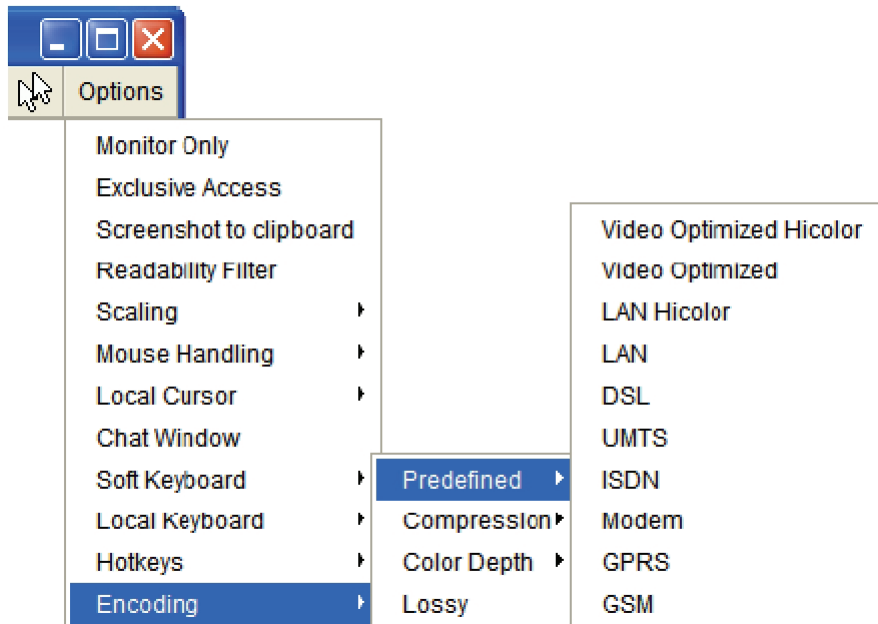


Figure 44: Predefined Compression

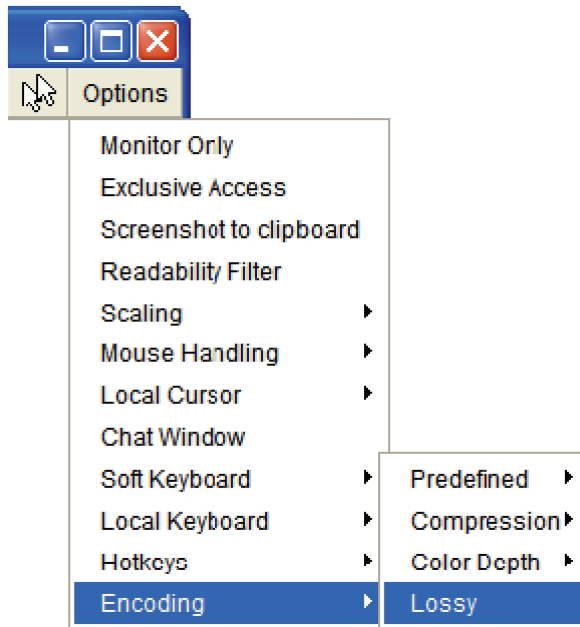


Figure 45: Lossy Compression

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.

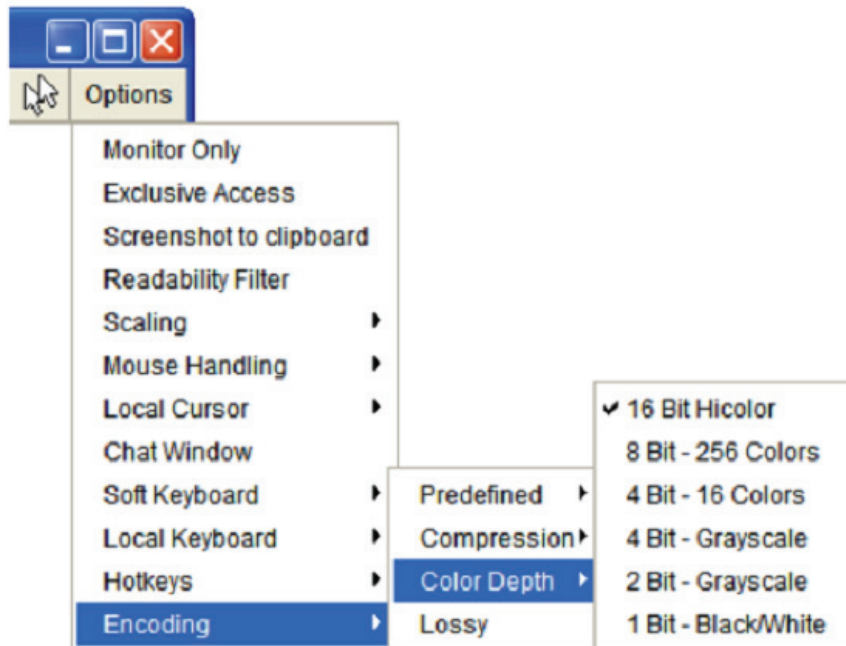


Figure 46: Encoding Color depth

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 CAT5 8-POR/16-POR IP-KVM will not have to do any video compression. In total, this will lead to less transfer time of the motion picture.

10.3.3 Status Line of Remote Console

Status line

The status bar shows the status of the Remote Console as well as the status of the connection between the Host system and the Remote system. The size of the remote screen is displayed. Figure below was taken from a Remote Console with a resolution of 1024x768 pixels. The value in brackets describes the connection to the Remote Console. “Norm” means a standard connection without encryption; “SSL” means a secure connection.



Figure 47: Status line

The right-hand side of the Status Bar may show the frame rate of the video in frames per second (Fps), and the current incoming (In) and outgoing (Out) transmission rates. If compressed encoding is enabled, the compressed transfer rate will be displayed in bracket

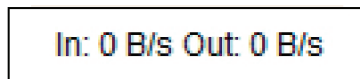


Figure 48: Status line transfer rate

For more information about Monitor Only and Exclusive Access settings, see related sections

11 Menu Option

11.1 Remote Control



The Remote Console is the redirected screen, keyboard and mouse of the remote host system that CAT5 8-POR/16-POR IP-KVM controls. The Remote Console window is a Java Applet that tries to establish its own TCP connection to the CAT5 8-POR/16-POR 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.

11.1.1 KVM Console

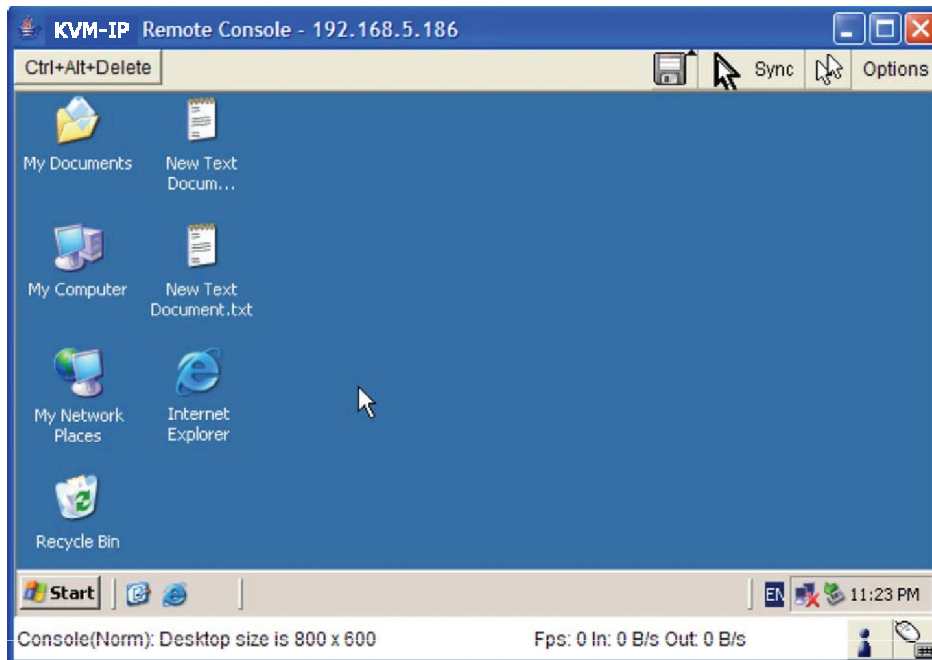


Figure 49: KVM Console

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.

11.1.2 Telnet Console/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 and outputs are redirected to the device via the serial port, and its answers are displayed on the Telnet interface.

In order to log in with Telnet or SSH, you have to enable the access settings from

Device Settings > Network.

Network Miscellaneous Settings

Remote Console & HTTPS port *

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 CAT5 8-PORT/16-PORT 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 CAT5 8-PORT/16-PORT IP-KVM host machine is using a text mode screen resolution.

To log in Telnet Console by one of the following way:

1. clicking **Remote Control > telnet Console**

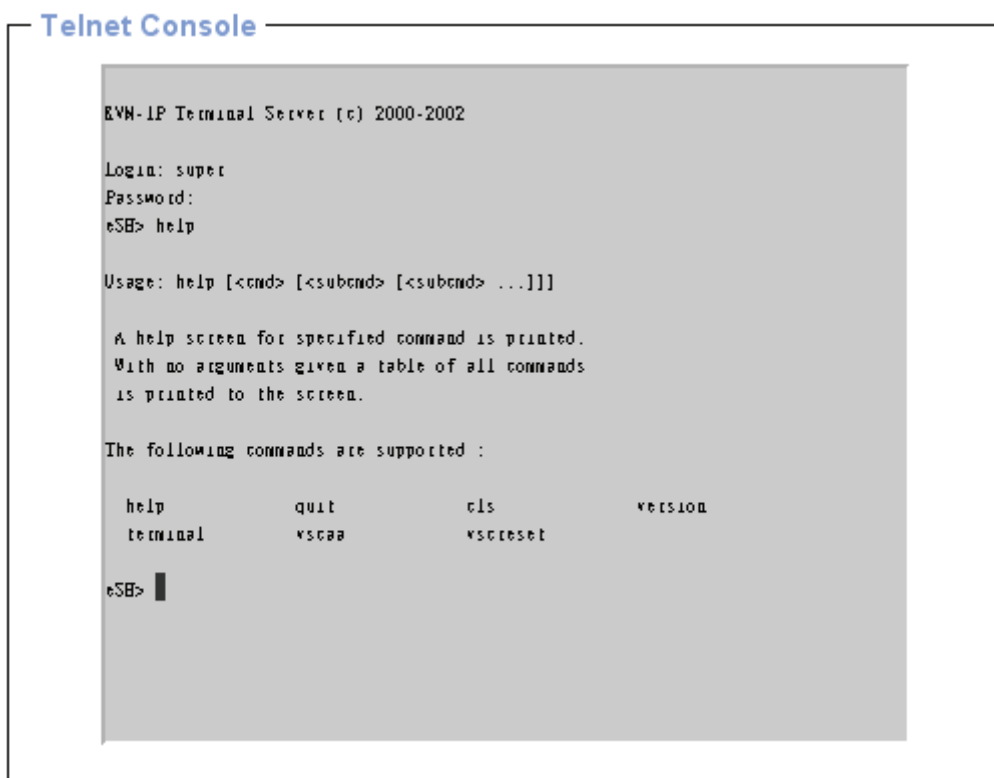


Figure 50: Telnet Console

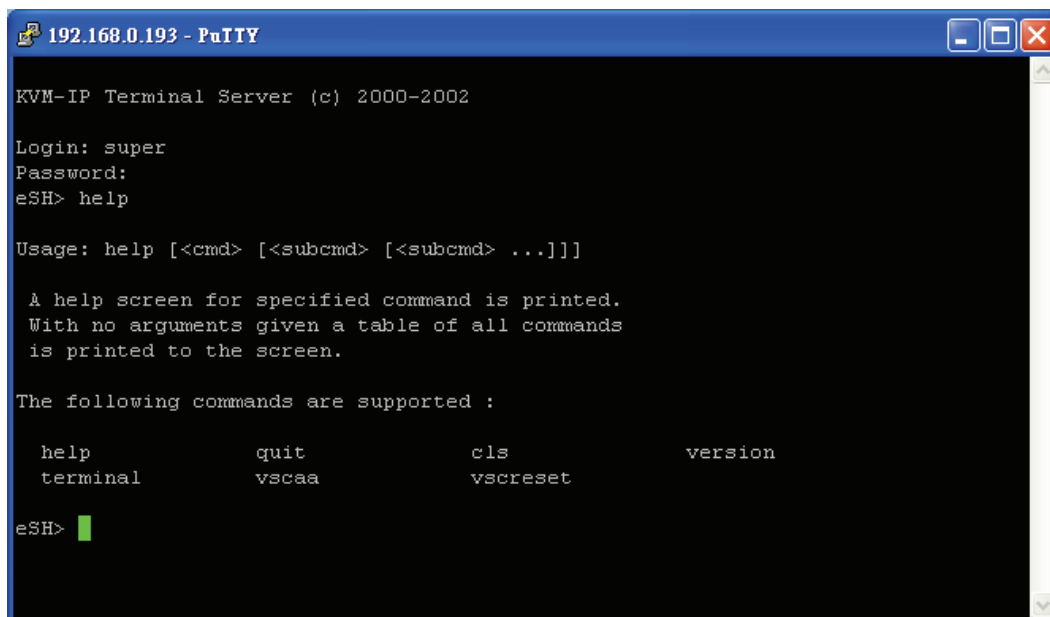
2. or telnet command as required by the Telnet client, for instance in a UNIX shell:

```
telnet 192.168.0.70
```

3. or run the SSH-supported terminal emulation program (such as **PuTTY**).

Replace the IP address by the one that is actually assigned to the CAT5 8-PORT/16-PORT 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. That means, 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 CAT5 8-PORT/16-PORT IP-KVM a command line will be presented and you can enter according management



```
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         vscreset

eSH> █
```

commands.

Key in **help** to list all available commands.

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

Activate the terminal **passthrough** mode for RS-232 serial port. This mode provides **Serial over IP** function. The hotkey sequence “ESC + e-x-i-t” (type “exit” while holding the ESC key) will switch the screen back to command mode.

vscaa

Auto-adjust of the Remote Console.

vsreset [modes/allmodes/all]

Reset the video modes like in the remote console under option “Video Settings”.

vsreset modes: reset settings for the current video mode.

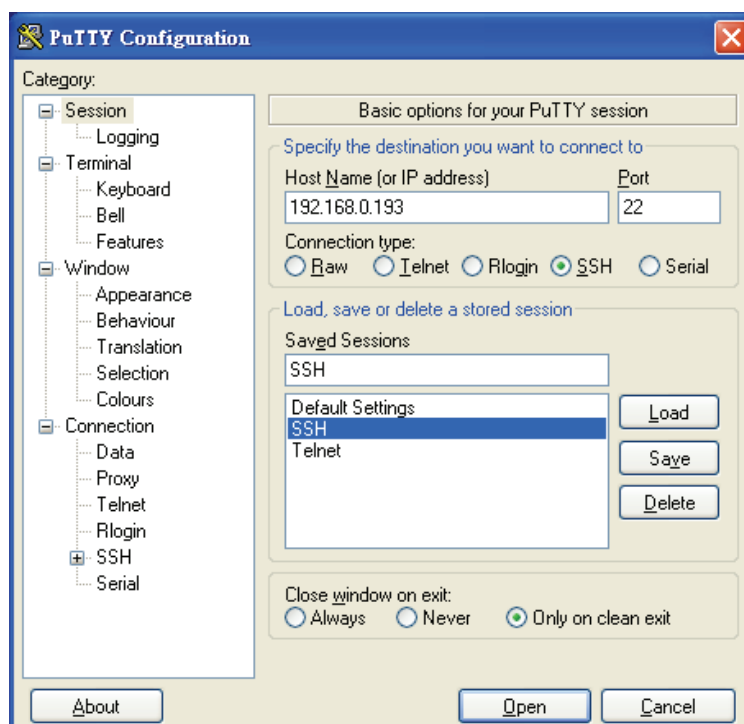
vsreset allmodes: reset settings for all video modes.

vsreset all: reset all video modes and global settings (Brightness and Contrast).

SSH Console

The CAT5 8-PORT/16-PORT IP-KVM supports the SSH security protocol. The device uses version 2 of the SSH protocol (SSH2) to encrypt the transferred data and secure transmissions. The SSH configuration interface is the same as that of Telnet, except for the fact that SSH is encrypted and therefore more secure.

Please run the SSH-supported terminal emulation program (such as **PuTTY**).



11.1.3 Remote Wakeup

Operation completed successfully.

Remote Wakeup Server List

	Wake Up	Server Description	Server IP	Server MAC
Server 1	<input type="checkbox"/>	E-mail Server	192.168.0.90	00:1F:D0:40:D7:2A
Server 2	<input type="checkbox"/>	Web Server	192.168.0.74	00:16:E6:DF:C1:72

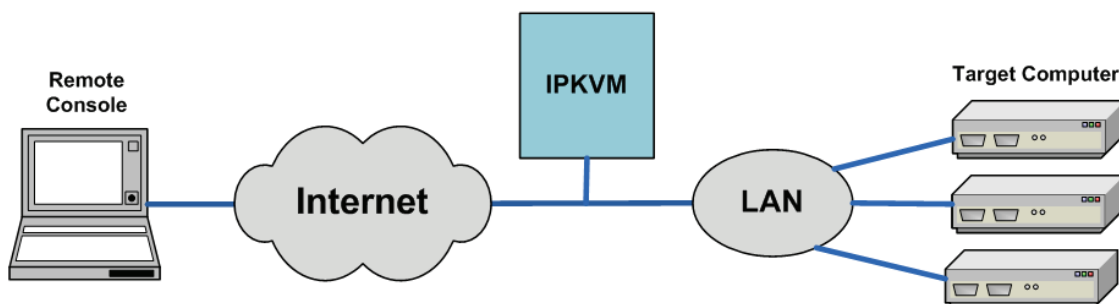
Buttons: Wake Up, Clear

Remote Wakeup Server Settings

	Server Description	Server IP	Server MAC	
Server 1	E-mail Server	192.168.0.90	00:1F:D0:40:D7:2A	Get MAC
Server 2	Web Server	192.168.0.74	00:16:E6:DF:C1:72	Get MAC

Buttons: More entries, Apply, Reset to defaults

The CAT5 8-PORT/16-PORT IP-KVM provides the remote power wakeup function, which can remotely wake up the sleeping computer. With this feature, the computers that are not in use for now can be shut down and remotely wake up the computer when want to use it, and thus save the power energy.



Settings on target computer:

To wake up a remotely located computer via the CAT5 8-PORT/16-PORT IP-KVM, some settings have to be pre-configured on the target computer:

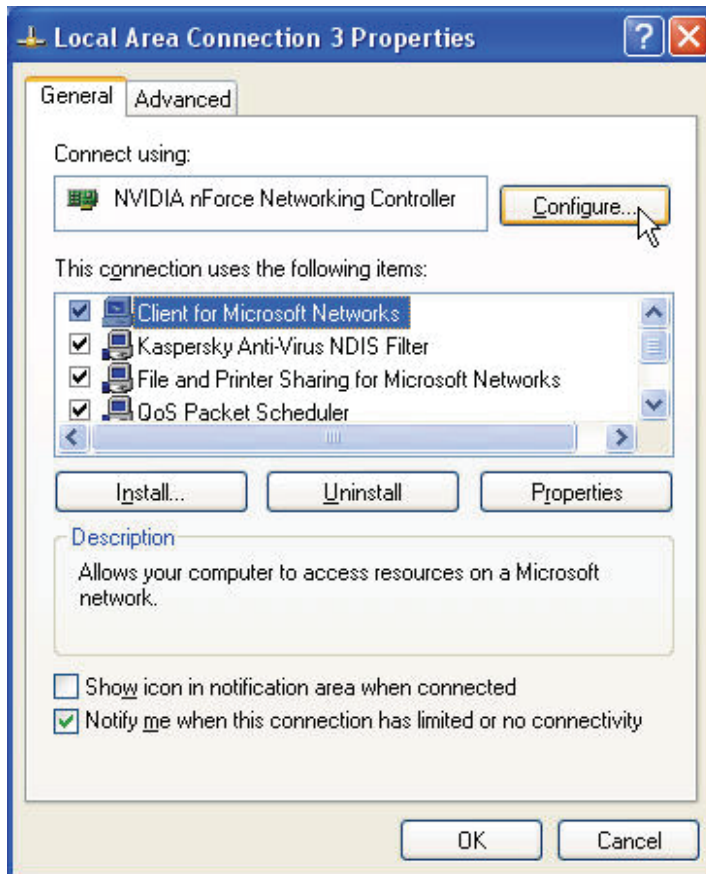
1. BIOS setting:

Enable the wakeup function in the BIOS of the target system.

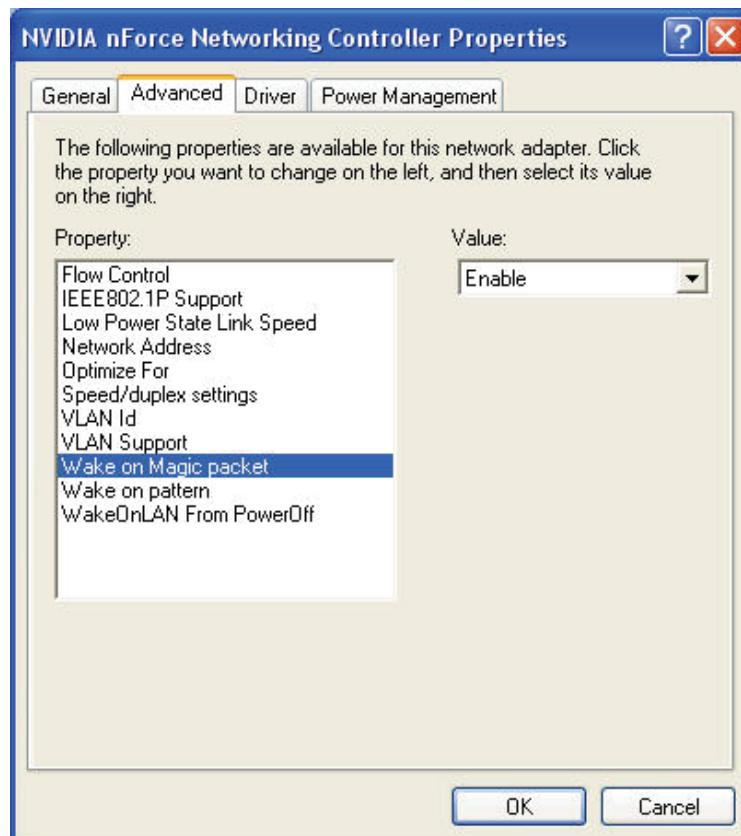
Note: The naming of the wakeup function in BIOS varies depending on the type of BIOS. It may be listed as **Wake On LAN/PME**, **PME Event Wake Up**, or **Power On By PCI Device**.

2. Windows Settings:

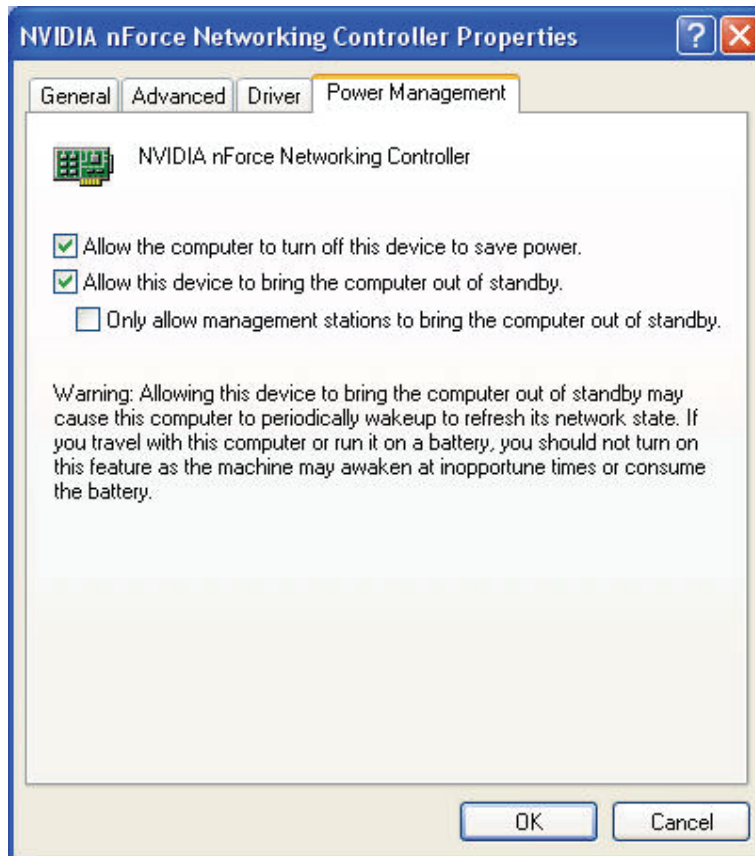
Enter the Properties of Local Area Connection.



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



Make sure the following two items are selected.



Settings on CAT5 8-PORT/16-PORT IP-KVM:

The control can be easily configured via web GUI.

1. Click on **Remote Control > Remote Wakeup** to bring up the configuration page.
2. Type in the computer/server description and the computer/server's IP address.
3. Click on the **Get MAC** button to obtain and automatically add the corresponding MAC address of the selected computer.
4. Click on the **Apply** button to save the entry.
5. Click on the **Reset to defaults** button if you want to clear all entries
6. If you want to configure multiple target systems, click on the **More entries** button to add more target computers. Repeat steps 2 to 4 for all target systems

11.2 Virtual Media

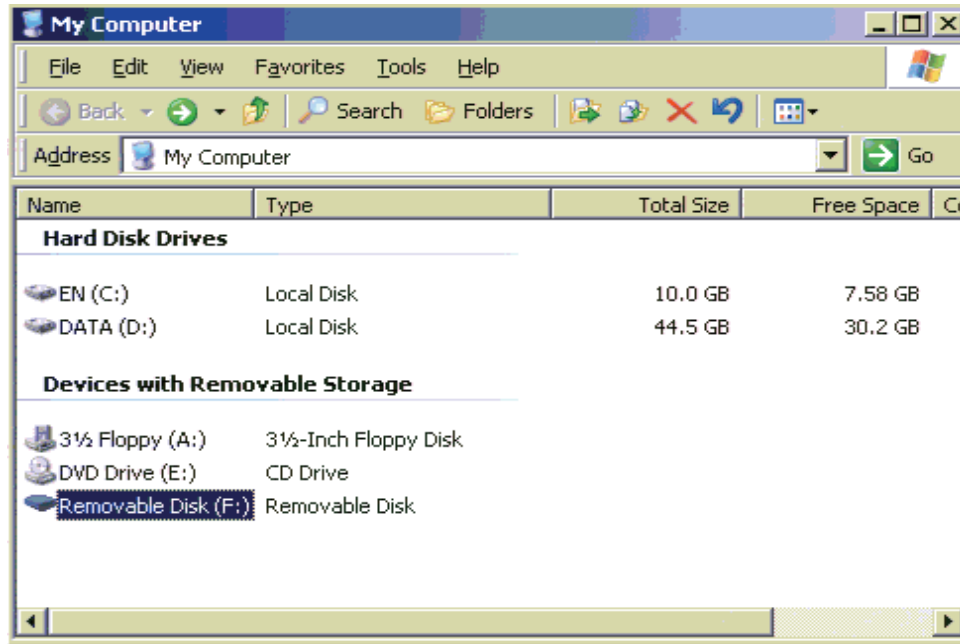
The CAT5 8-POR/16-POR IP-KVM provides a powerful feature called Virtual Media (or Virtual Disk). The CAT5 8-POR/16-POR IP-KVM can present either a local floppy disk image (stored on the CAT5 8-POR/16-POR IP-KVM) or a redirected remote CD/DVD-ROM image (redirected from the Remote computer) to the target computer through the built-in USB port. This can allow for system recovery in conditions including disk failure or no primary network connection on the target computer.

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 disk.



Before go ahead with this setup, both remote user computer and local computer (the one connected with the CAT5 8-POR/16-POR IP-KVM unit) would have to have Operating System Win2000, XP or above. This function would not work on other platforms at this moment.

Before using Virtual Media, please connect the USB cable from CAT5 8-POR/16-POR IP-KVM to host computer. After connecting the USB cable, you can see a "Removable Disk" on the host computer. Below is the host computer screen (the computer which connected with CAT5 8-POR/16-POR IP-KVM).



11.2.1 Drive Redirection

The Drive Redirection function gives the administrator another virtual disk drive on the Host computer. With Drive Redirection, you do not have to use an image file. Instead, the Remote-side user can open a drive on his or her local computer and use it on the Host machine. Thus, the drive is shared over a TCP network connection. Devices that can be redirected are floppy drives, hard disks, CD-ROM drives, and other removable devices such as USB storage drives.

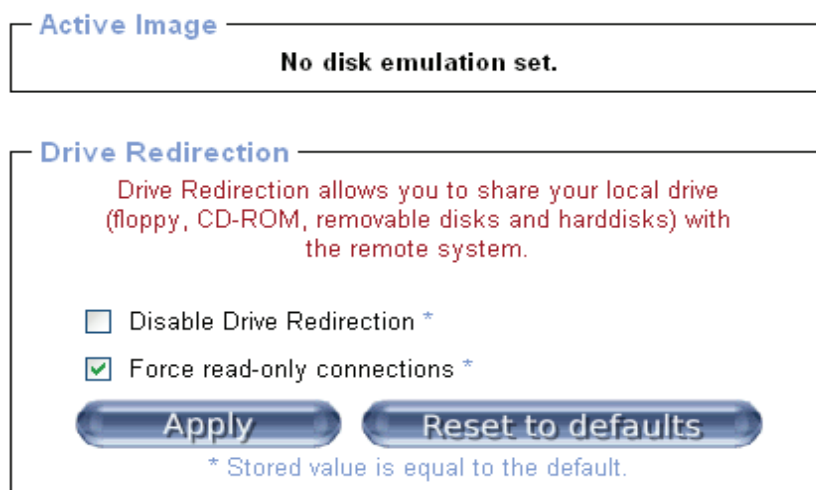


Figure 51: Options of Drive Redirection

It is even possible to enable write support so that the Remote-side user can write data to his or her local disk from the Host machine. However, if write support is enabled, care should be taken that the two systems do not write onto the same disk at the same time, as computer operating systems cannot distinguish a local system from a redirected system.

WARNING: If both the Host system and the Remote system try to write data on the same device at the same time, data may be damaged and/or lost. Please use this feature only if you know what you are doing.

Please be noted that Drive Redirection works on a more basic level than the operating systems of the computers. This means that neither the Remote-side nor the Host-side operating system is aware that the drive is being redirected. This may lead to inconsistent data when the operating system (either on the Remote-side or Host-side machine) is writing data on the device. If write support is enabled, the Host computer might damage the data and the file system on the redirected device. On the other hand, if the Remote-side operating system tries to write data to the redirected device, the drive cache of the Host's operating system might contain older data.

Because the operating systems are not aware that the drive is being redirected, they could try to write data at the same time and therefore cause error messages to pop up. We therefore recommend that the Remote user uses the Drive Redirection function with care, especially if write support is enabled.

Disable Drive Redirection

To disable the Drive Redirection function.

Force read-only connections

If you enable the **Force read-only connections** function, write support for the Drive Redirection feature will be switched off once you click **Apply**. This will make it impossible to write on a redirected device, which is a safer option if you don't want to take the risk of file-system-destroying write-over collisions between the Remote and.

Click **Apply** to submit your changes.

11.2.2 Virtual Drive

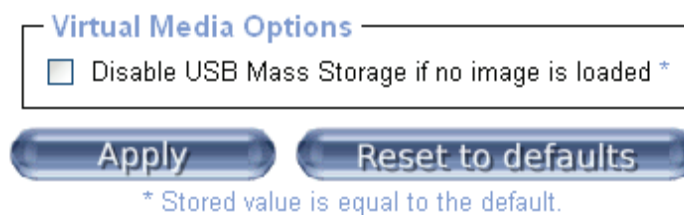


Figure 52: USB mass storage option

Enable this option to disable the mass storage emulation (and hide the virtual drive) if you are not presenting (or "mounting") a disk image file or drive to the Host system. After ticking or unticking the checkbox, click the **Apply** button to save your changes.

Note: If the above setting is not enabled, and if no disk image file is detected, the Host

system could possibly hang in boot mode due to changes in the boot order or the boot manager (LILO, GRUB). Such incidents were reported for some Windows versions (Windows 2000 and Windows XP), and other operating systems might behave in the same way. The actual OS behavior will depend on the BIOS version used in the specific machine.

11.2.3 CD/DVD Image

Use Image on Windows Share (via SAMBA)

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

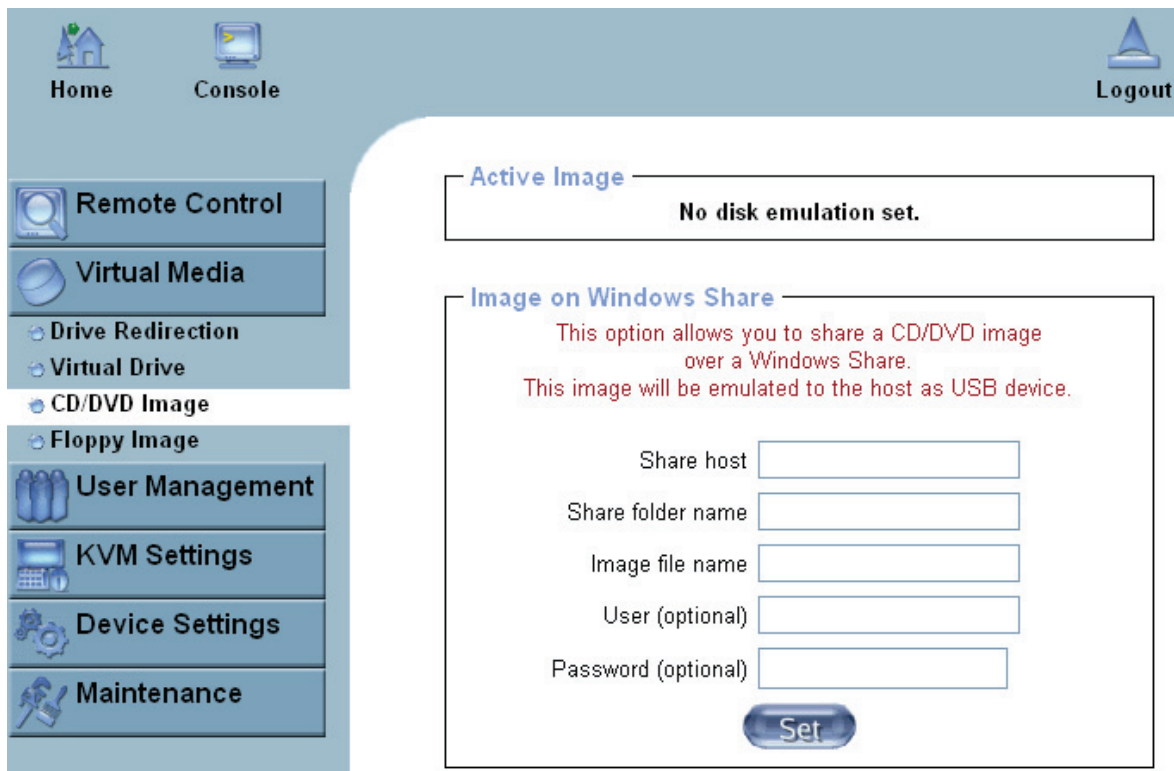


Figure 53: Virtual Media - CD-ROM Image

Share host

Enter the server name or its IP address (the computer/server that shares out the image file).

Note: For Windows 95, 98 and Windows ME, do not enter the IP address; enter the server name (e.g. “NetBIOS Name”).

Share folder name

Enter the name of the relevant share folder.

Image file name

Enter the name of the image file as it is on the share folder.

User (optional)

If necessary, specify the username for the share named before. If unspecified and a guest account is activated, this guest account information will be used as your login.

Password (optional)

If necessary, specify the password for the given user name.

Notes:

1. The output image extension file must be an ISO image file, and the file name extension must be 'iso', e.g. CD-Rom_vir.iso.
2. You can create an ISO file up to 650 MB in size (CD-ROM size). This drive will be accessible only in read-only mode, you will not be able to write any information to it. This drive can act as a boot drive if the motherboard/BIOS on the Host computer supports the USB BOOTABLE function. For emulating a DVD Drive, please use **Drive Redirection** function.
3. The information required for the steps above has to be given from the point of view of the CAT5 8-PORT/16-PORT IP-KVM. Please enter IP addresses and device names accordingly. Administrative permission is required for this, as regular users may not have access rights. Please log in as a system administrator (or as "root" on UNIX systems). It is also important to specify the correct IP-KVM IP addresses and device names. Otherwise, the CAT5 8-PORT/16-PORT IP-KVM may not be able to access the referenced image file properly. This will cause the CAT5 8-PORT/16-PORT IP-KVM to leave the given file unmounted, and instead display an error message.
4. The specified share has to be configured correctly. Administrative permission is required for this. Normal user may not have a high enough level of authorization. You should either login in as a system administrator (or as "root" on UNIX systems), or ask your system administrator for help to complete this task.

Operation Procedures:

1. Please run Nero or any CD/DVD imaging tool to create CD/DVD ISO image.
2. Please create a folder and share this folder **on the PC that shares out the image file**. Copy the CD/DVD ISO image file to this sharing folder. (Please make sure password has to be setup with the authorized user during Sharing => Permission settings)

MS 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

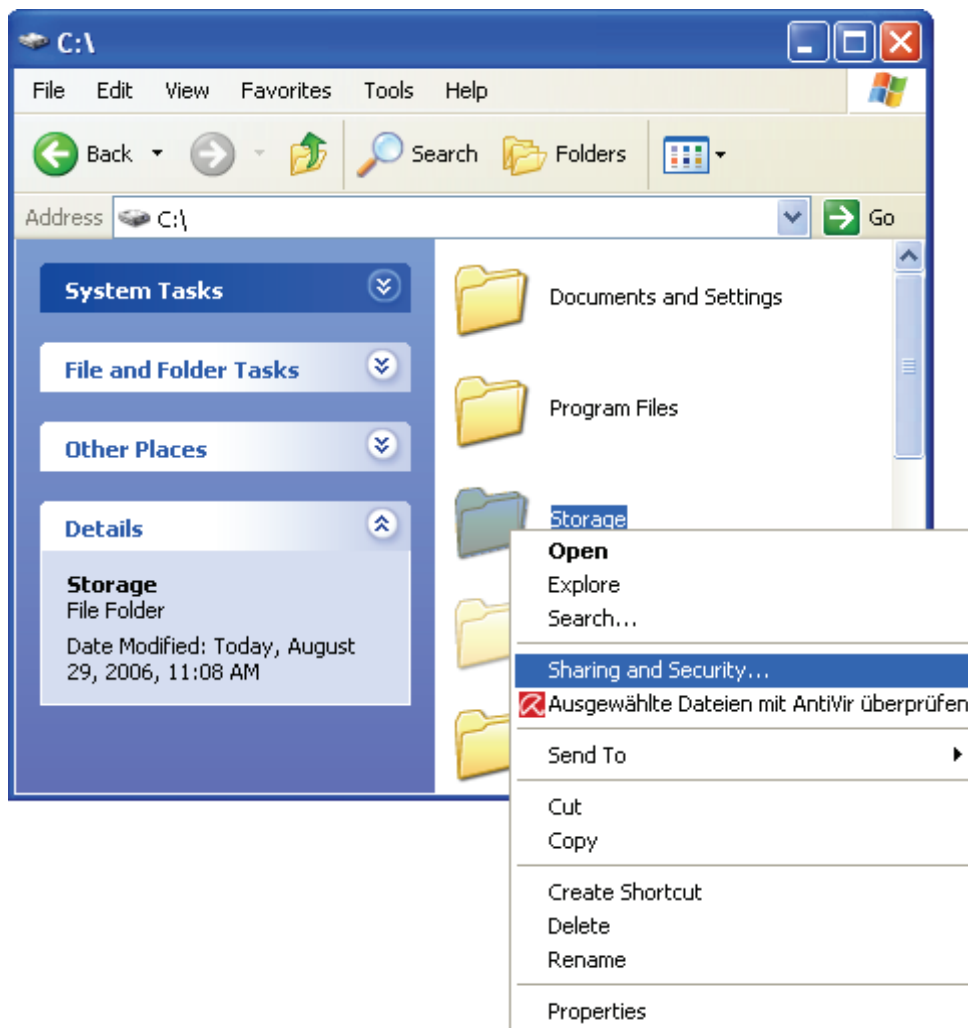


Figure 54: Explorer Context Menu

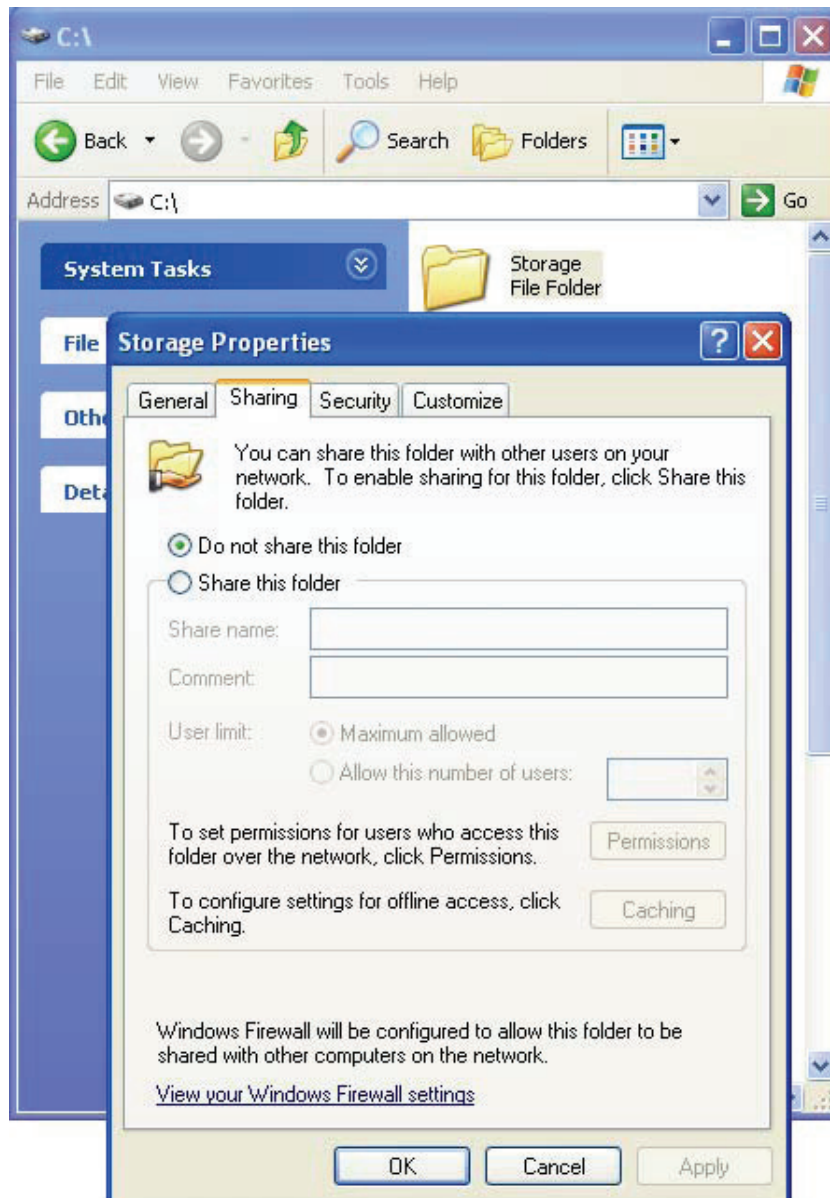


Figure 55: Share Configuration Dialog

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.

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.

Viewing the **man**-entry of **smb.conf** may also provide additional help.

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

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, a screen like the one below will appear.

Image file set successfully

Active Image

CD-ROM Image

Share Host: 59.120.208.56

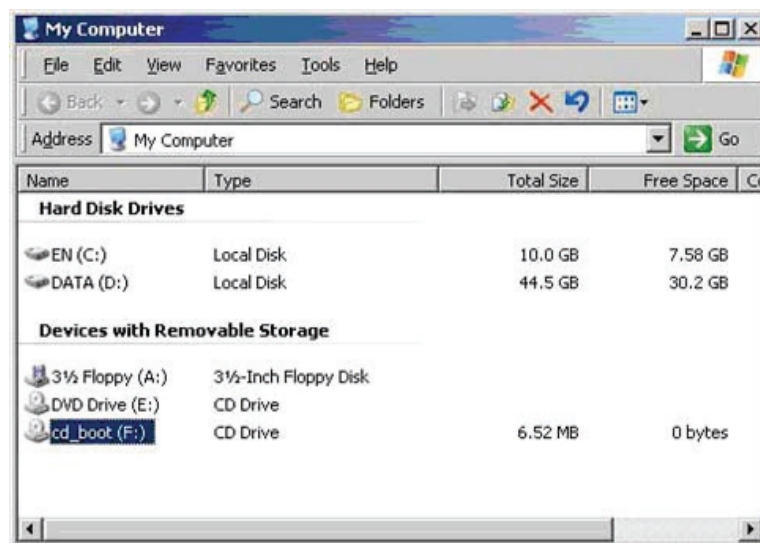
Share folder name: storage

Image file name: Cdrom_image.iso

User name: fae

Password: not displayed

- Open the remote console and you can see the virtual CD as shown below.



11.2.4 Floppy Disk

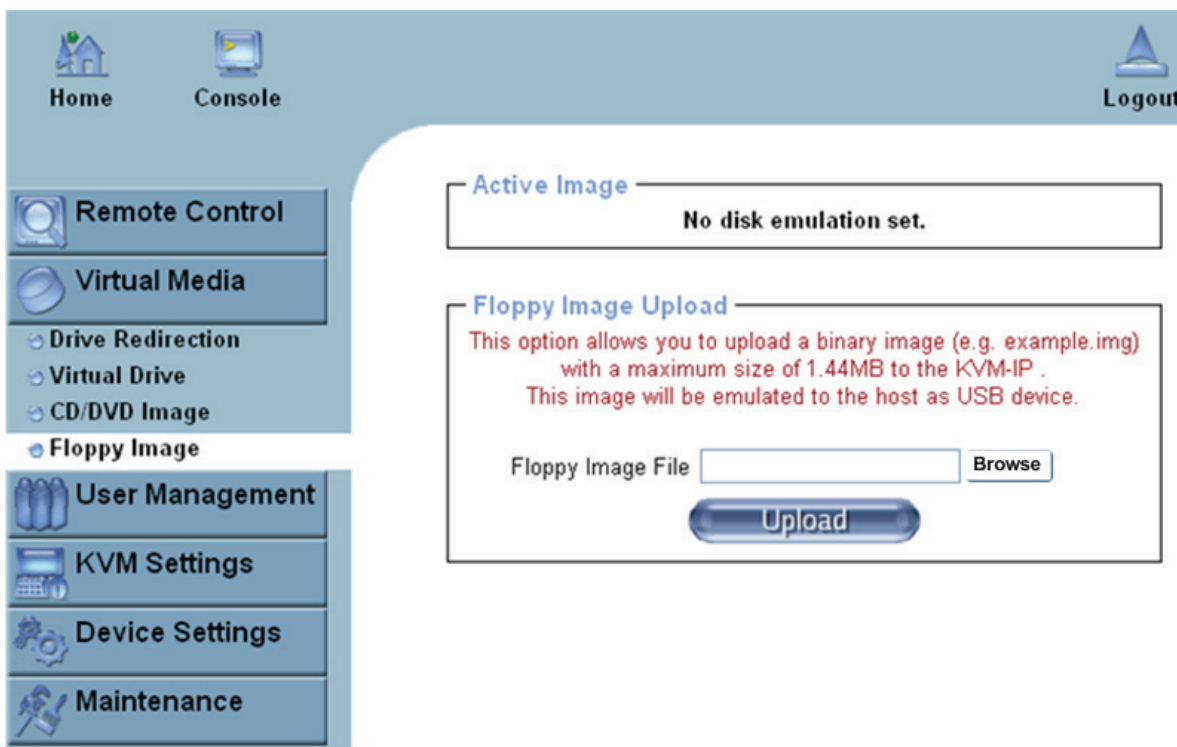
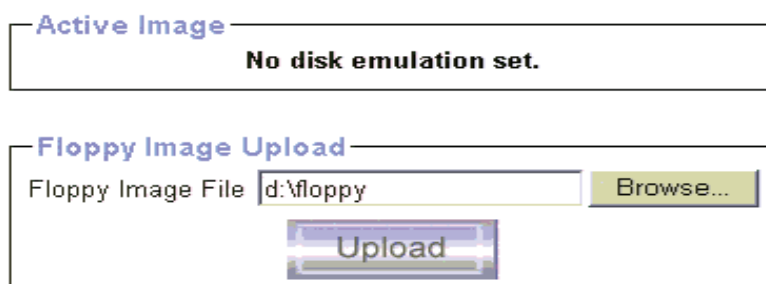


Figure 56: Virtual Media - Floppy Disk

The maximum image size is limited to 1.44MB. To use a larger image, mount this image via Windows Share (or SAMBA) (see the Section called Use Image on Windows Share (via SAMBA) for details)

Operation Procedures:

1. You need to create the floppy image file first (Please refer to the section “Creating a floppy image”). For this example, we used Raw Write program (or any other image-creator software) to create the floppy image. Please use licensed software for this purpose.
2. You can find an image file saved at desire destination after you created it with Raw Write.
3. Open the browser to log into the CAT5 8-POR/16-POR IP-KVM. Click **Virtual Media > Floppy Disk**. Click the Browse button to choose the image file.

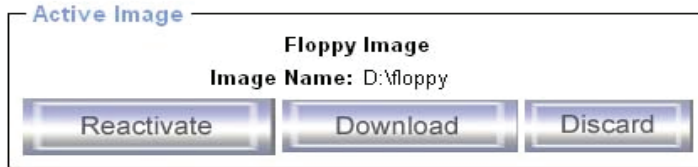


Click on the button **Upload** to initiate the transfer of the chosen image file into the CAT5

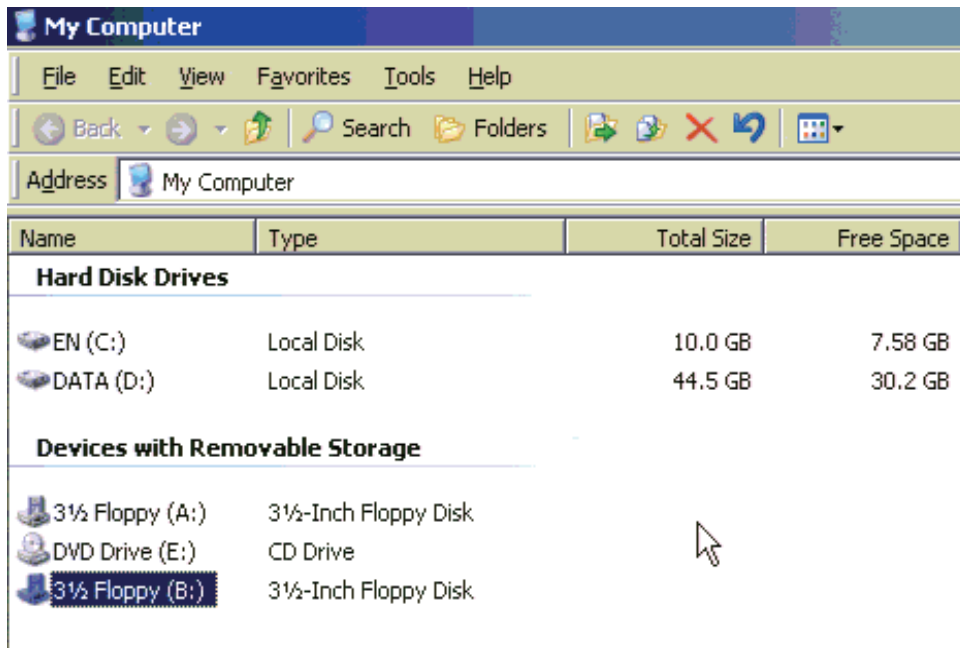
8-PART/16-PART IP-KVM module's on-board memory

4. After you uploading the image file, you will see the information below.

Floppy image uploaded successfully.



5. Open the remote console and you will see a virtual Floppy drive is created on the host computer that connected to CAT5 8-PART/16-PART IP-KVM.



The maximum size of the floppy image disk is 1.44MB. This drive is in read-only mode and does not allow you to write any information on the drive. This drive can act as a boot drive if the motherboard/BIOS on the Host computer supports the USB BOOTABLE function.

Notes:

1. For any image-creating software, the output image's file extension must be ".img", e.g. "floppy_vir.img".
2. The uploaded image file will be kept in the onboard memory of the CAT5 8-PART/16-PART IP-KVM until the end of the current session. A session ends when you log out or initiate a reboot of the CAT5 8-PART/16-PART IP-KVM.

11.2.5 Creating an Image

11.2.5.1. Creating a Floppy Image

MS Windows

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

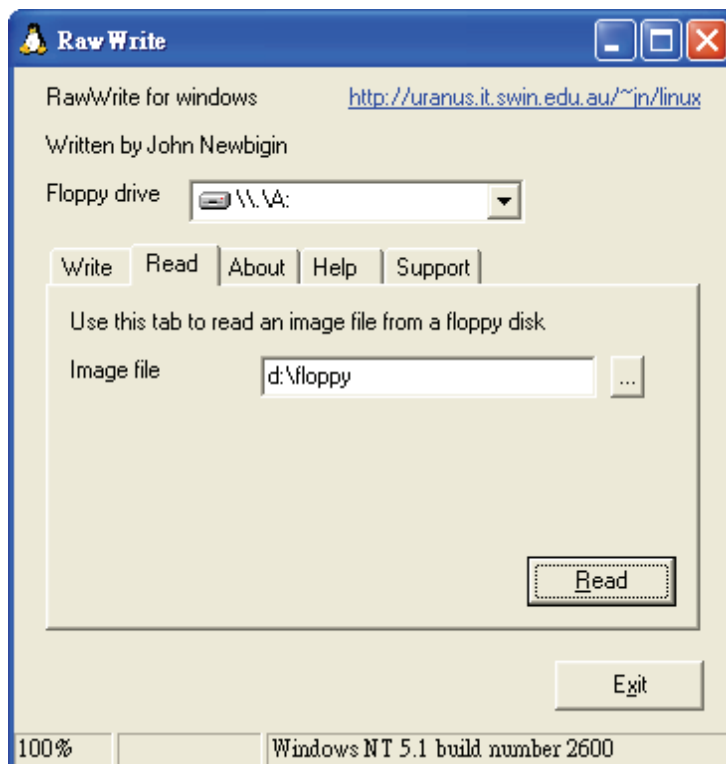


Figure 57: Raw Write for Windows selection dialog

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 “Read” to initiate the image creation process.

UNIX and UNIX-like OS

To create an image file, you can use the “dd” command. 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 disk 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.).

11.2.5.2. Creating a CD/DVD ISO Image

MS Windows

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

For example, with “Nero” you should select “Copy and Backup”. Then, click on 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 58: Nero selection dialog

UNIX and UNIX-like OS

To create an image file, you can use “dd” command. 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:

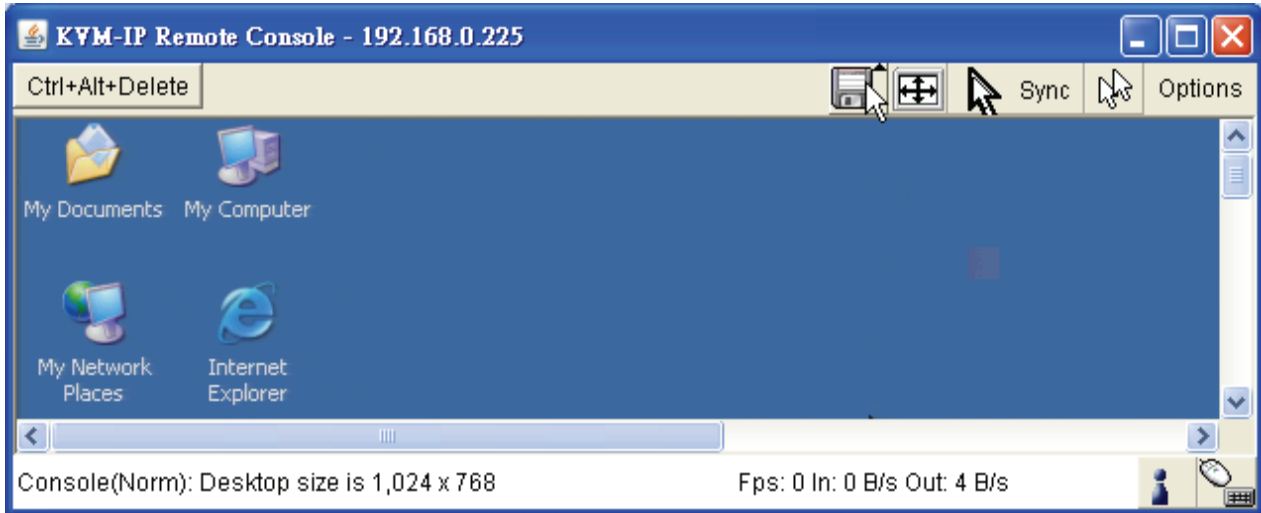
```
dd [ if=/dev/cdrom ] [ of=/tmp/cdrom.image ]
```

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.).

11.2.6 Making a Drive Redirection

The operation for making a Drive Redirection as below:

1. Click **Remote Control > KVM Console**.
2. Click on the “Floppy” icon 



You will see the Driver Redirection window as below

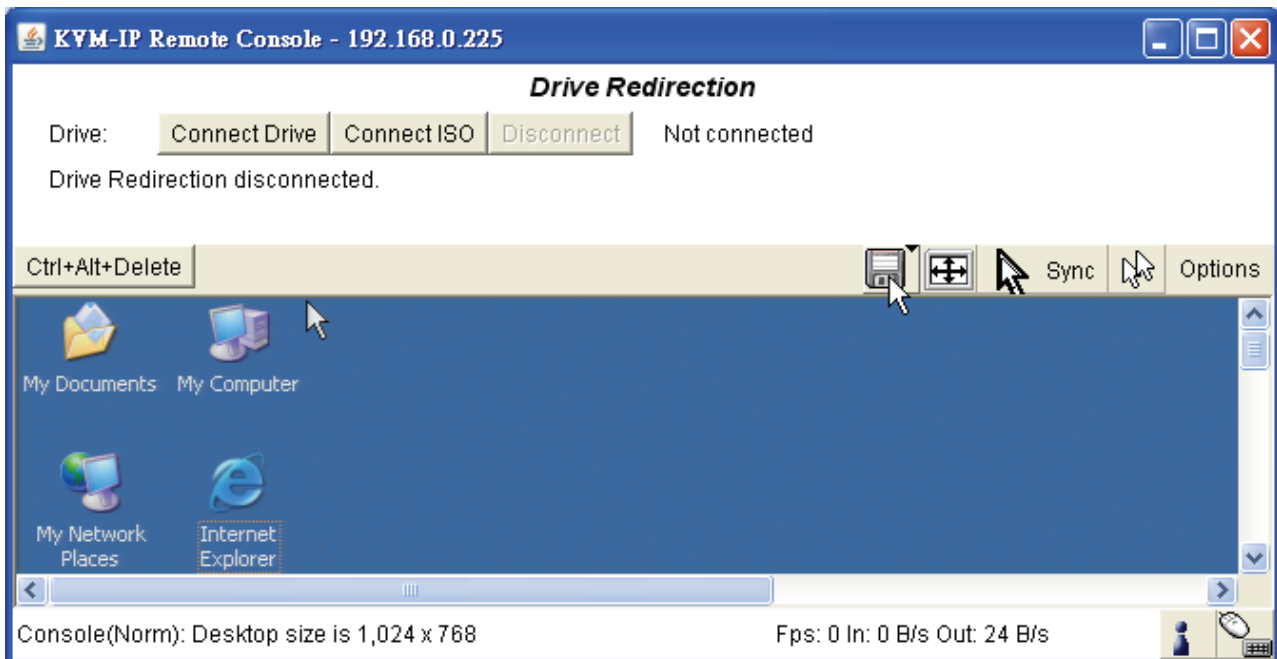
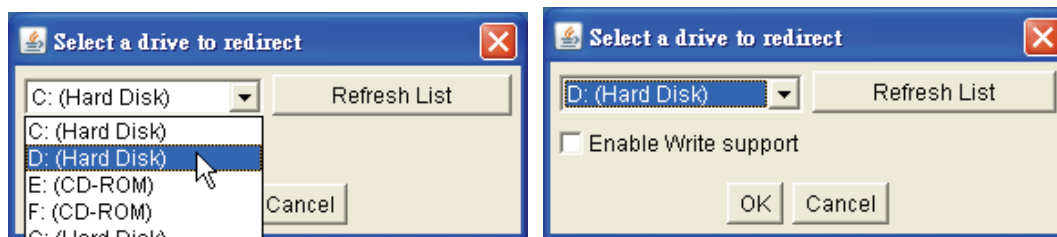


Figure 59: Built-in Java Drive Redirection

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

3a. If you click the **Connect Drive** button in the Drive Redirection field, the following issues need to be taken into consideration:



Select the drive to be redirected and click **OK**.

Select the drive that should be redirected. All available devices (drive letters) are shown here. Please be noted that the entire hard disk that the drive belongs to will be shared with the Remote computer, not only one partition. If you have a hard disk with more than one partition, all partitions that belong to this disk will be redirected. The "Refresh" button can be used to regenerate the list of drive initials. This is especially handy when working with a USB stick.

Warning

Please be cautious that if "Allow Write Support" is selected, all data on the shred media might be destroyed.

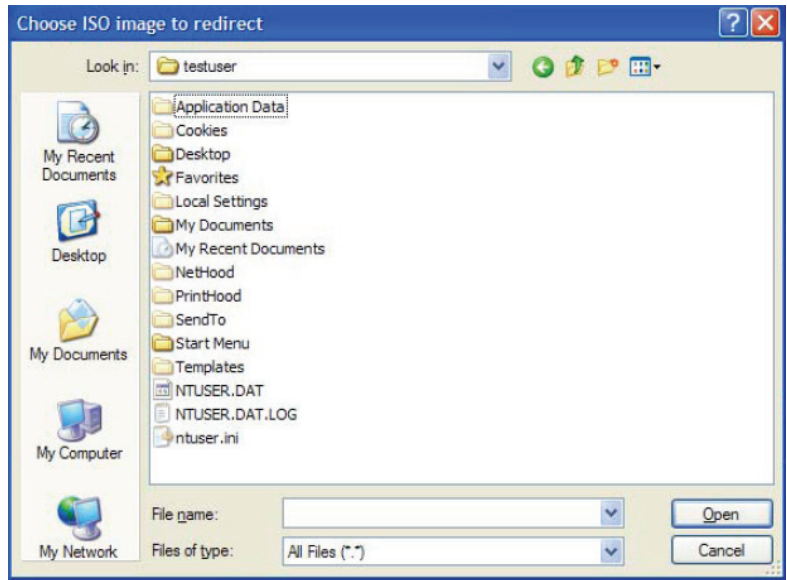
Write Support

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 feature only if you exactly know what you are doing.

Warning

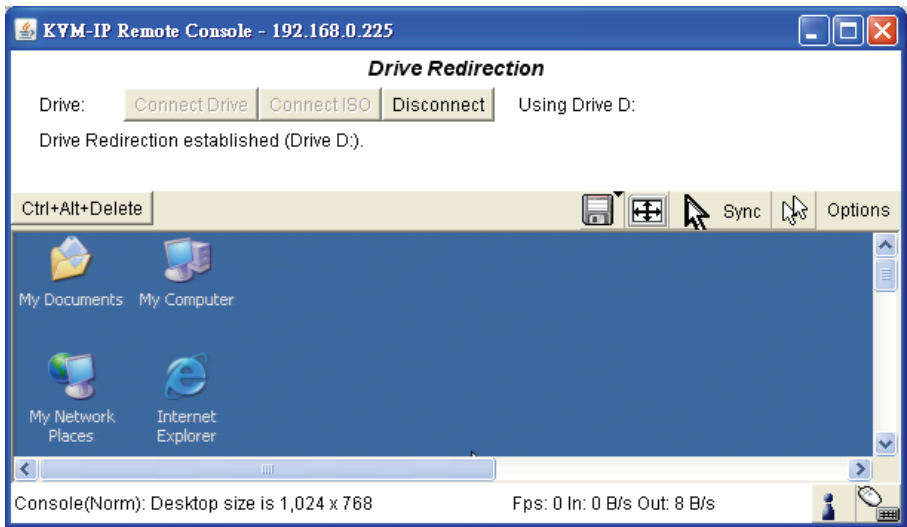
1. Drive Redirection is only possible with Windows 2000 or later versions.
2. The Drive Redirection works on a low SCSI level and the SCSI protocol cannot recognize partitions; therefore the whole drive selected will be shared instead of any particular partition.

3b. If click on **Connect ISO**

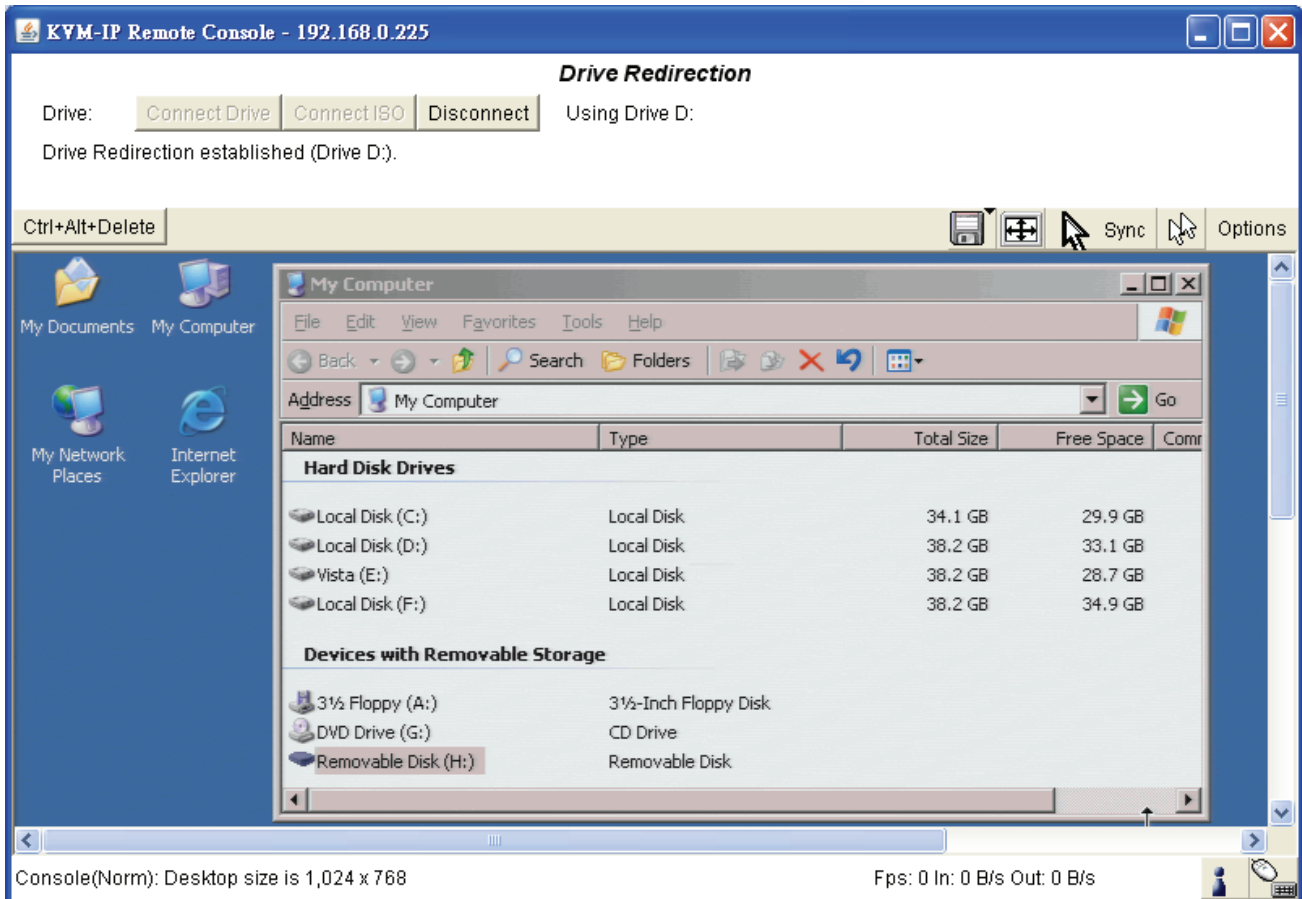


Select the ISO image file and click **Open**

4. Finally the established Drive Redirection connection will be displayed



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



The drive redirection software will try to lock the Remote-side local drive before it is redirected. That means that it will try to prevent the local operating system from accessing the drive as long as it is redirected. This attempt may fail, especially if a file on the drive is open when the attempt is made. In the case of such a locking failure, you will be prompted if you want to establish the connection anyway. If Write Support is enabled, a drive which is not locked may be damaged by the Drive Redirection. This should not be a serious problem if the Write Support is disabled.

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

Please note that the Virtual Drive is created on the “device level”, not the “partition level”, which means that the computer looks for I/O at the BIOS level and sends the corresponding data to the Host computer. This means that it sends the entire hard drive (which may consist of multiple partitions) and emulates all of those partitions on the Host computer. A DVD drive can be emulated in the same way. However, such a “virtual” DVD drive **cannot** act as a boot drive like floppy and CD-ROM images can.

11.3 User Management

On an CAT5 8-PORT/16-PORT IP-KVM, each username has permission levels that are assigned to it. These permission settings affect how the user interfaces with the Remote Console. Permissions allow or forbid the user from performing various actions on the CAT5 8-PORT/16-PORT IP-KVM's web pages. There are three permission "ranks" that can be assigned to any user at any time by any user that has the relevant permission "rank". The highest permission rank is "super user", then "administrator", then "user" at the bottom of the rank hierarchy.



11.3.1 Change Password

Change Password

Old Password

New Password

Confirm New Password

Apply

Figure 60: Setting Password

Click on User Management > Change Password to change the password for the currently logged in user account. Enter the relevant old and new passwords, and then click the **Apply** button to save your changes.

11.3.2 Users and Groups

The screenshot shows a 'User Management' form with the following elements:

- Existing users:** A dropdown menu with '--- select ---' and a 'Lookup' button.
- New user name:** A text input field.
- Full user name:** A text input field.
- Password:** A text input field.
- Confirm Password:** A text input field.
- Email address:** A text input field.
- Mobile number:** A text input field.
- Role:** A dropdown menu with 'Administrator' selected.
- Enforce user to change password on next login *:** An unchecked checkbox.
- Buttons:** 'Create', 'Modify', and 'Delete' buttons at the bottom.

Figure 61: Users and Groups

There are three permission levels of user accounts:

- **Super** -- Has permission to change all configurations and use all functions.
 - **Administrator** -- Has permission to change most configurations and use most functions
 - **User** -- Has permission to access only the basic functions of the Remote Console
- You can choose the desired level from the selection box **role**.

The CAT5 8-POR/16-POR IP-KVM comes pre-configured with a factory default “super user” account that is permitted to make all possible configuration changes and use all the device’s functions.

The factory default username and password for this super user is “super” and “pass”. **Make sure you change the password immediately after you have installed your CAT5 8-POR/16-POR IP-KVM.**

Existing users

Select an existing user for modification. Once a user has been selected, click the **Lookup** button to display the user’s information.

New User name

Enter a name for the new user account.

Password

Enter a password for the selected user. It must be at least three characters long.

Confirm password

Re-enter the password for the selected user for confirmation.

Email address

Enter the user's e-mail address here. (optional)

Mobile number

Enter the user's mobile phone number here. (optional)

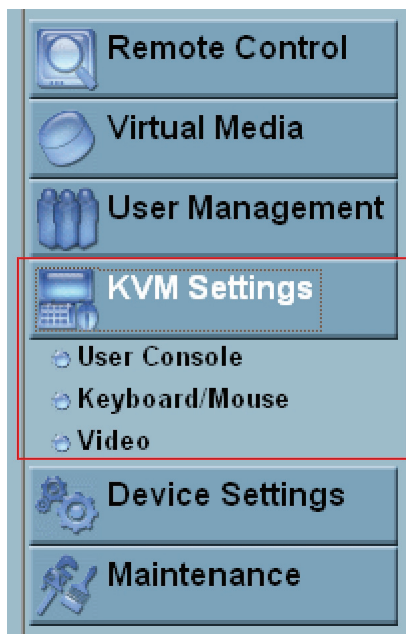
Role

Assign a permission level, or role, to the selected user.

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

Note: The CAT5 8-PORT/16-PORT IP-KVM is equipped with a built-in processor and memory unit, which both have limitations in terms of the processing instructions and memory space. To guarantee an acceptable response time, we recommend that you do not let more than 15 users connect to the CAT5 8-PORT/16-PORT IP-KVM at the same time. The memory space available on the CAT5 8-PORT/16-PORT IP-KVM mainly depends on the configuration and usage of the CAT5 8-PORT/16-PORT IP-KVM (log file entries, etc.). For this reason, we recommend that you do not store more than 63 user profiles.

11.4 KVM Settings



11.4.1 User Console

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

Remote Console Settings for User

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

super

Transmission Encoding

Automatic Detection *

Pre-configured

Network speed

Manually

Compression *

Color depth *

Remote Console Type

Default Java VM *

Sun Microsystems Java Browser Plugin

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

Miscellaneous Remote Console Settings

Start in Monitor Mode *

Start in Exclusive Access Mode *

Mouse Hotkey

Hotkey (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 62: User Console Setting

Remote Console Settings for User (user select box)

This selection box displays the username whose configuration values are displayed and for which any changes will take effect. You may change the settings of other users if you have the required permission level. Use the dropdown box to select the user whose configuration settings you want change, then click the Update button.

Transmission Encoding

The Transmission Encoding setting allows you to change 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 logged in at the same time and the network bandwidth of the connection line (Modem, ISDN, DSL, LAN, etc.).

- Automatic detection
The encoding and the compression level are determined automatically from the available bandwidth and the current content of the video image.
- Pre-configured
Use the dropdown box to select the network speed that most closely matches the CAT5 8-PORT/16-PORT IP-KVM's connection speed to automatically choose the best settings for compression and color depth for the indicated network speed.
- Manually
This field lets you adjust both the compression rate and the color depth individually. Depending on the selected compression rate, the data stream between the CAT5 8-PORT/16-PORT IP-KVM and the Remote Console will be compressed in order to save bandwidth. Since high compression rates use more of the CAT5 8-PORT/16-PORT IP-KVM's computing power, they should not be used while several users are accessing the CAT5 8-PORT/16-PORT IP-KVM simultaneously.

The standard color depth is 16 -bit (65536 colors). Other color depths are intended for slower network connections in order to allow for faster transmission of data. Compression level 0 (no compression) uses only 16-bit color. For low bandwidth connections, 4-bit (16 colors) and 2-bit (4-color grayscale) are recommended for typical desktop interfaces. To retain a high-quality image on a low bandwidth connection, such as when viewing photos, try 4-bit (16-color grayscale). 1-bit color depth (black/white) should only be used for extremely slow network connections.

Remote Console Type

This field specifies which Remote Console viewer the selected user will use.

- Default Java-VM
This viewer uses the default Java Virtual Machine (JVM) of your Browser. This may be the Microsoft JVM for Internet Explorer, or the Sun JVM if the browser is configured to use it by default. Use of the Sun JVM may also be forced manually

(see below).

- **Sun Microsystems Java Browser Plugin**

This viewer instructs the web browser that your GUI is running on to use the Sun Microsystems Java Virtual Machine (JVM). 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 if 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 instruct your browser to download and install the plugin, usually through prompts that will appear, and an 11 MB plugin will need to be downloaded. (The CAT5 8-PORT/16-PORT IP-KVM will provide a link to the JVM plugin if the Remote computer does not already have it installed. The user could also install the latest Java software later, if needed.)

The advantage of downloading Sun's JVM is that it provides a stable and identical experience across different platforms. The Remote Console software is optimized for this JVM version and offers a wider range of functionality when run in Sun's JVM. Please make sure that you install Sun JVM 1.5 or above in your client system.

Miscellaneous Remote Console Settings

- **Start in Monitor Mode**

This setting sets the initial value for the Monitor Only mode. By default, Monitor Only mode is off. If you enable this setting, the Remote Console window will open in view-only mode.

- **Start in Exclusive Access Mode**

If you enable this setting, the Remote Console will start in Exclusive Access mode. This means that the Remote Console windows of all other users will be forced to close if this user opens the Remote Console for the CAT5 8-PORT/16-PORT IP-KVM on his or her computer. No one else can open the CAT5 8-PORT/16-PORT IP-KVM's Remote Console window until this user disables Exclusive Access mode or logs off..

Mouse hotkey

This lets you specify a hotkey combination for this user that will either start the mouse synchronization process when Double Mouse Mode is active, or will free the mouse pointer from being captured by the Remote Console when Single Mouse Mode is active.

Remote Console Button Keys

Button Keys allow keystroke combinations to be sent to the Host computer that normally cannot be generated on the Remote computer. The reason for this might be a missing key, or the fact that the local operating system of the Remote computer is

unconditionally catching this key combination already. Typical examples are “Control+Alt+Delete” in Windows and DOS, or “Control+Alt+Backspace” on Unix or Unix-like operating systems for restarting X-Server.

The syntax to define a new Button Key is as follows:

```
[confirm] <keycode>[+|-*]<keycode>]*
```

“confirm” programs the system to display a confirmation dialog box (Yes/No) before a keystroke sequence is sent to the remote host.

“keycode” is the key sequence that will be sent. Multiple key codes can be concatenated with a plus or a minus sign. The plus sign builds key combinations where all keys listed will be pressed until a minus sign or the end of the combination is encountered, where all pressed keys will 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.

11.4.2 Keyboard/Mouse

Keyboard/Mouse Settings

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 *

Apply **Reset to defaults**

* Stored value is equal to the default.

Figure 63: Keyboard and Mouse Settings

- **Keyboard Model**

Select the keyboard configuration that matches the one that will be used by the Remote user. This will help ensure that keystrokes received by the Host computer match the ones sent by the Remote computer. 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**

We recommend that you enable this setting if the Host system runs on a UNIX or UNIX-like OS.

- **Mouse Speed**

- **Auto mouse speed**

Use this option if the mouse settings on the Host system use an additional acceleration setting. The CAT5 8-POR/16-POR IP-KVM tries to detect the acceleration and speed of the mouse during the mouse sync process.

- **Fixed mouse speed**

This option uses a direct translation of mouse movements between the local and the remote pointer. You may also adjust the fixed scaling which determines number of pixels to move the remote mouse pointer when the local mouse pointer is moved 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 that any mouse acceleration settings of the OS should be disabled. Also, the Remote Console's Intelligent Sync function will not be available when fixed scaling is selected.

- **Absolute mouse scaling for MAC server**
Enable this option if the Host computer uses Mac OS.

After making any changes, click the **Apply** button to save your settings.

11.4.3 Video

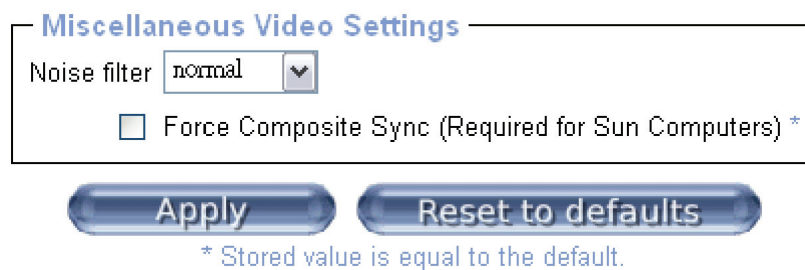


Figure 64: Video Settings

Miscellaneous Video Settings

- **Noise filter**

This option defines how the CAT5 8-POR/16-POR 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 interference, and can help lower unnecessary bandwidth consumption. A large filter setting needs less network data traffic and enables a faster video display, but some small changes in the display may not be recognized immediately. A small filter setting displays all changes instantly, but may lead to a constant stream of network traffic, even if the display content is not actually changing (depending on the quality of the video input signal). In general, the default setting should be suitable for most situations.

- **Force Composite Sync (Required for Sun Computers)**

When connecting the device directly to a legacy Sun computer that uses composite sync as the video output, the CAT5 8-POR/16-POR IP-KVM may not recognize the composite sync video output automatically. To support signal transmission from a Sun machine, enable this option. If this is not enabled, the video feed of the Remote Console may not be visible.

After making any changes, click the **Apply** button to save your settings.

11.5 Device Settings



11.5.1 Network

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

Network Basic Settings

IP auto configuration *

Preferred host name (DHCP only)

IP address

Subnet mask *

Gateway IP address

Primary DNS server IP address *

Secondary DNS server IP address *

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 *

LAN Interface Settings

Current LAN interface parameters: autonegotiation on, 100 Mbps, full duplex, link ok

LAN interface speed *

LAN interface duplex mode *

* Stored value is equal to the default.

Figure 65: Network Settings

Warning

Changing the network settings of the 8-PORT/16-PORT IP-KVM might result in losing your connection to it. In case you change the settings remotely make sure that all the values are correct and that you still have a way to access the 8-PORT/16-PORT IP-KVM if the connection is lost, such as though a local network.

- IP auto configuration
 With this option you can control whether the CAT5 8-PORT/16-PORT IP-KVM should fetch its network settings from a DHCP or BOOTP server. For DHCP, select “dhcp”, and for BOOTP select “bootp”. If you choose “none” then IP auto configuration is disabled and you will need to set a static IP.

- Preferred host name
This sets the preferred host name to request from DHCP server. Whether the DHCP server takes the CAT5 8-PORT/16-PORT IP-KVM suggestion into account or not depends on the DHCP server's configuration.
- IP address
Here you can set the CAT5 8-PORT/16-PORT IP-KVM's IP address.
- Subnet Mask
Here you can set the subnet mask for the CAT5 8-PORT/16-PORT IP-KVM.
- Gateway IP address
Here you can set the gateway for the CAT5 8-PORT/16-PORT IP-KVM. In case the CAT5 8-PORT/16-PORT IP-KVM needs to 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
Here you can set the primary DNS server for the CAT5 8-PORT/16-PORT IP-KVM. This option may be left blank, but the CAT5 8-PORT/16-PORT IP-KVM will then be unable to perform name resolution.
- Secondary DNS Server IP Address
Here you can set the secondary DNS server for the CAT5 8-PORT/16-PORT IP-KVM. It will be used in case the Primary DNS Server cannot be contacted.
- Remote Console And HTTPS port
Here you can set the port the CAT5 8-PORT/16-PORT IP-KVM will use for the Remote Console server and HTTPS server. If this is blank, the default port of 443 will be used.
- HTTP port
Here you can set the port the CAT5 8-PORT/16-PORT IP-KVM will use for the HTTP server. If this is blank, the default port of 80 will be used.
- Telnet port
Here you can set the port the CAT5 8-PORT/16-PORT IP-KVM will use for the Telnet server. If this is blank, the default port of 23 will be used.
- SSH port
Here you can set the port the CAT5 8-PORT/16-PORT IP-KVM will use for the SSH server. If this is blank, the default port of 22 will be used.

- **Bandwidth limitation**
This lets you limit the bandwidth used by the CAT5 8-PORT/16-PORT IP-KVM. If this is blank, no bandwidth limit will be applied.
- **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 CAT5 8-PORT/16-PORT IP-KVM from the setup protocol. Setup protocol is a proprietary layer-2 MAC-based protocol to allow some configuration software to detect CAT5 8-PORT/16-PORT IP-KVM devices in the network, even without IP address, and then configure network related settings for the CAT5 8-PORT/16-PORT IP-KVM.

11.5.2 Dynamic DNS

Dynamic DNS Settings

Enable Dynamic DNS *

Dynamic DNS server www.dyndns.org

DNS System

Hostname (eg. yourhost.dyndns.com)

Username

Password

Check time (HH:MM) *

Check interval *

Delete saved external IP

* Stored value is equal to the default.

Figure 66: Dynamic DNS

Dynamic DNS allows you to use a Dynamic DNS service to reach your CAT5 8-PORT/16-PORT IP-KVM by an easy to remember domain name rather than by its IP address. This can also be useful if your IP address changes frequently, such as when using a DSL connection. When Dynamic DNS is enabled, the CAT5 8-PORT/16-PORT IP-KVM will connect to a DDNS service at regular intervals to update it with its current IP address. The Remote user can then simply open a web browser to go to the easy to remember address (e.g. mykvm.dyndns.org) provided by the DDNS service. There are many freely available DDNS services available, such as www.dyndns.org, which is used in the example diagram below.

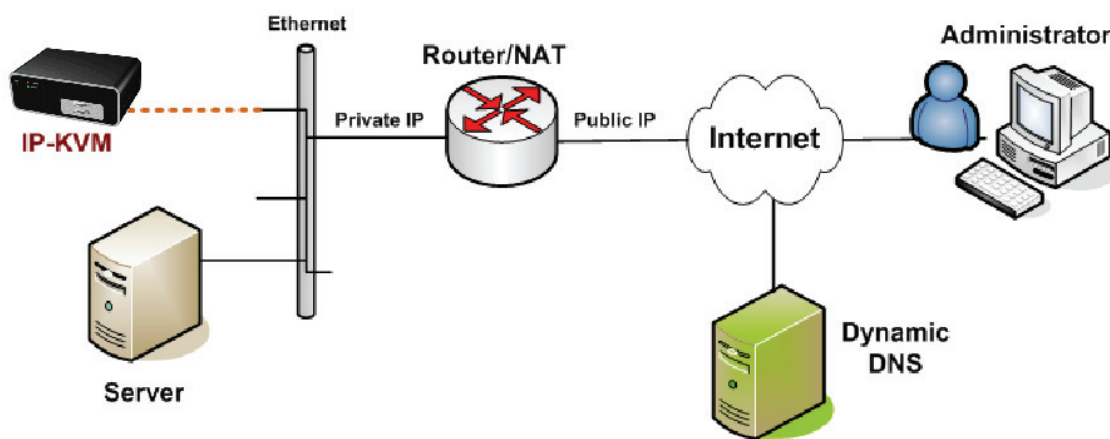


Figure 67: Dynamic DNS Scenario

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

- Make sure that the LAN interface of the CAT5 8-PORT/16-PORT IP-KVM is properly configured.
- Create an account with a DDNS service provider and set up a hostname for the CAT5 8-PORT/16-PORT IP-KVM to use. You will need the username and password for your DDNS account as well as the hostname you will use.
- Enable Dynamic DNS and enter the required settings, as described below. After making your changes, click the **Apply** button to save your changes.

Enable Dynamic DNS

This enables the Dynamic DNS service. This requires you to have configured a DNS server's IP address.

Dynamic DNS server

This is the address of the DDNS service the CAT5 8-PORT/16-PORT IP-KVM will use. Currently, this is a fixed setting as only dyndns.org is currently supported.

DNS System

Choose Dynamic for free DNS service. Customize this for your own domain.

Hostname

Enter the hostname of the CAT5 8-PORT/16-PORT IP-KVM that is provided by the

Dynamic DNS service. Make sure you enter the entire hostname, including the domain. (e.g. testserver.dyndns.org)

Username

Enter the username for your DDNS service account. The username may not contain any spaces.

Password

Enter the password for your DDNS service account.

Check time

The CAT5 8-POR/16-POR IP-KVM registers itself for initiating the IP address of CAT5 8-POR/16-POR 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 CAT5 8-POR/16-POR IP-KVM.

Warning

The CAT5 8-POR/16-POR IP-KVM has its own independent real time clock. Make sure the time setting of the CAT5 8-POR/16-POR IP-KVM is correct. (see the Section *Date And Time*)

11.5.3 Security

HTTP Encryption

Force HTTPS for Web access *

KVM Encryption

KVM Encryption Off * Try Force

Group based System Access Control

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

Enable Group based System Access Control *

Default Action *

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

* Stored value is equal to the default.

Figure 68: Device Security

Force HTTPS

If this option is enabled, access to the web GUI is only possible using an HTTPS connection. The CAT5 8-PORT/16-PORT IP-KVM will not listen on the HTTP port for incoming connections.

KVM encryption

This option controls the encryption of the RFB protocol. RFB is used by the Remote Console to transmit screen data from the Host computer to the Remote computer, and keyboard and mouse data from the Remote computer back to the Host. If this option is set to “Off”, no encryption will be used. If set to “Try” the applet will try to make an encrypted connection. In case the encrypted connection fails for any reason, an unencrypted connection will be used.

If KVM encryption is set to “Force”, the applet will only make an encrypted connection with a certificate. An error will be reported in case an encrypted connection cannot be made.

Group-based System Access Control

This lets you control what IP addresses can connect to the CAT5 8-PORT/16-PORT IP-KVM by creating IP filtering rules. You can choose to allow or block IP addresses to/from accessing the CAT5 8-PORT/16-PORT IP-KVM.

Note: If you set the IP filtering rules incorrectly, it is possible to block your computer from accessing the CAT5 8-PORT/16-PORT IP-KVM. For assistance in creating IP filtering rules, please contact your network administrator.

Chain rule

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

- ACCEPT : access allowed
- DROP : access not allowed

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

When the CAT5 8-PORT/16-PORT IP-KVM receives a TCP packet, it will process the packet with the chain rule depicted below. The process ordering is important; the packet will enter the chain rule 1 first, if meet the rule then take action directly, otherwise go to chain rule 2.

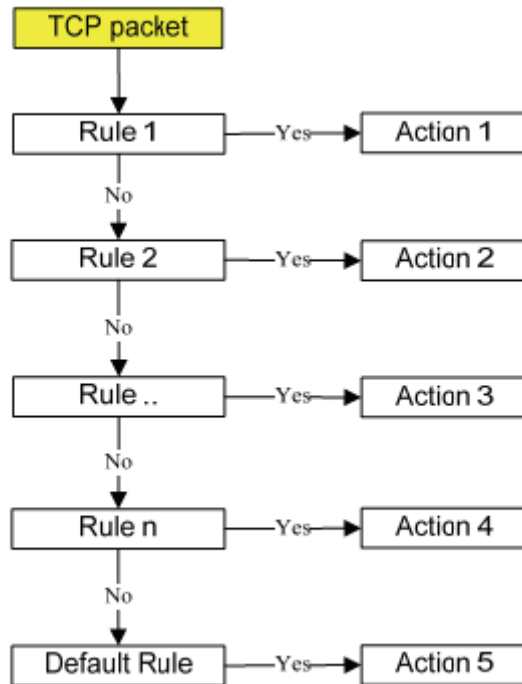


Figure 69: Chain Rules of IP Filtering

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

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

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 70: IP Filter Setting

11.5.4 Certificate

Certificate Signing Request (CSR)

Common name

Organizational unit

Organization

Locality/City

State/Province

Country (ISO code)

Email

Challenge password

Confirm Challenge password

Key length (bits) *

* Stored value is equal to the default.

Figure 71: Certificate Settings

The CAT5 8-PORT/16-PORT IP-KVM uses the Secure Socket Layer (SSL) protocol for any encrypted network traffic between itself and a connected client. While establishing a connection, the CAT5 8-PORT/16-PORT IP-KVM has to expose its identity to a client using a cryptographic certificate. The default certificate that comes with the CAT5 8-PORT/16-PORT IP-KVM device upon delivery is for testing purpose only. The system administrator should not rely on this default certificate as a secured global access mechanism for access via the Internet.

It is possible to generate and install a new base64 X.509 certificate that is unique for a particular CAT5 8-PORT/16-PORT IP-KVM. In order to do this, the CAT5 8-PORT/16-PORT IP-KVM can generate a new cryptographic key and the associated Certificate Signing Request (CSR) that will need to be certified by a certification authority (CA). A CA verifies that you are the person who you claim you are, and signs and issues a SSL certificate to you.

The following steps are necessary to create and install a SSL certificate for the CAT5 8-PORT/16-PORT IP-KVM:

- Create a SSL Certificate Signing Request using the panel shown as above. You need to fill out a number of fields that are explained below. 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.
- Save the file of the CSR string (if it is not displayed in a file, copy and paste it onto a word processing program file before you save it) and send it to a Certification Authority(CA) for certification. You will get the new certificate from the CA after an authentication process (the process will depending on the CA).
- Upload the certificate to the CAT5 8-PORT/16-PORT 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
```

Certificate Upload

SSL Certificate File

Figure 72: SSL Certificate Upload

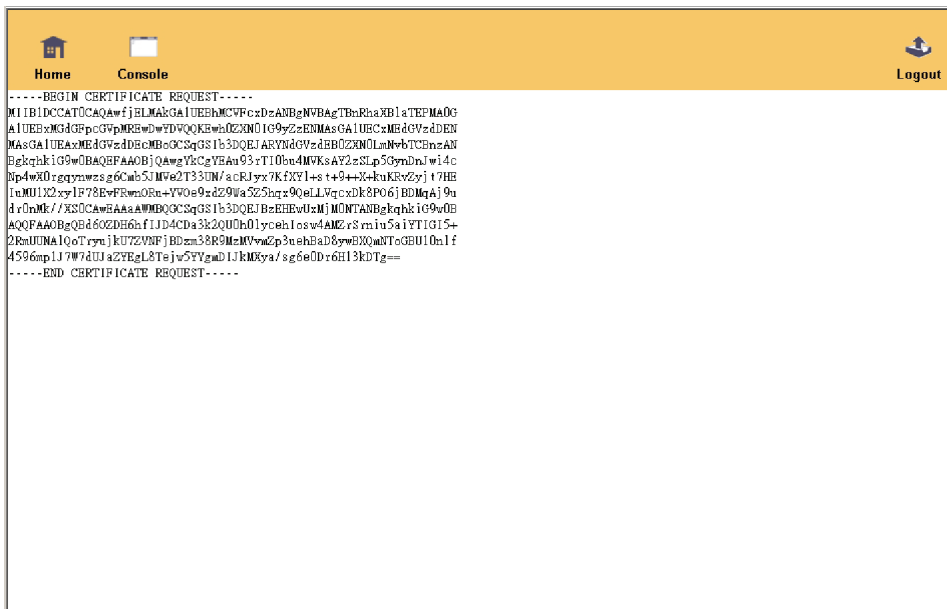


Figure 73: CSR string

After completing these three steps, the CAT5 8-PORT/16-PORT IP-KVM has its own certificate that is used for identifying the card to its clients.

Warning

If you destroy the CSR on the CAT5 8-PORT/16-PORT 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.

Common name

Enter the network name of the CAT5 8-PORT/16-PORT IP-KVM (usually the fully qualified domain name). It is identical to the name that is used to access the CAT5 8-PORT/16-PORT 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 CAT5 8-PORT/16-PORT IP-KVM is accessed using HTTPS.

Organizational unit

Enter the department within your organization the CAT5 8-PORT/16-PORT IP-KVM belongs to.

Organization

Enter the name of the organization to which the CAT5 8-PORT/16-PORT IP-KVM belongs.

Locality/City

Enter the city where your organization is located.

State/Province

Enter the state or province where your organization is located.

Country (ISO code)

Enter the country where your organization is located. This is the two-letter ISO code, e.g. DE for Germany, or US for the USA. (Note: the country code must 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

Reenter the challenge password for confirmation.

Email

Enter the email address of a contact person that is responsible for the CAT5 8-PORT/16-PORT IP-KVM and its security.

Key length

Enter the length of the generated key in bits. 1024 Bits are supposed to be sufficient in most cases. Longer keys may result in slower response time when establishing a connection to the CAT5 8-PORT/16-PORT IP-KVM.

11.5.5 Serial Port

Serial Port Settings

Configuration login *

Modem

Serial line speed: 115200 bits/s *

Modem init string: ATZH0 OK ATL0M0&K3X1 *

Modem server IP address: 192.168.3.1 *

Modem client IP address: 192.168.3.2 *

Passthrough access to serial port 1 via Telnet/SSH

Speed	Data bits	Parity	Stop Bits	Handshake
115200 *	8 *	none *	1 *	None *

Serial Port Log

Key Word 1: Key Word

[More entries](#)

[Apply](#) [Reset to defaults](#)

* Stored value is equal to the default.

Figure 74: Serial Port

The CAT5 8-POR/16-POR IP-KVM Serial Settings allows you to specify what device is connected to the serial port and how to use it.

Configuration or console login

If this is selected, the CAT5 8-POR/16-POR IP-KVM will not use the serial port for any advanced functions; it will only be used for initial configuration.

Modem

If this is selected, the serial port will support an Internet modem connection. The CAT5 8-POR/16-POR IP-KVM offers remote access using a telephone line in addition to the standard built-in Ethernet adapter. The modem needs to be connected to the serial interface of the CAT5 8-POR/16-POR IP-KVM.

Logically, connecting to the CAT5 8-POR/16-POR IP-KVM using a telephone line means nothing more than creating a dedicated point-to-point connection from your Remote computer to the CAT5 8-POR/16-POR IP-KVM. In other words, the CAT5 8-POR/16-POR 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 CAT5 8-POR/16-POR IP-KVM, make sure to configure your Remote computer accordingly. For instance, on Windows based operating systems you can configure a dial-up network connection (which is set to PPP by default).

The Modem Settings panel allows you to configure the remote access to the CAT5 8-PORT/16-PORT IP-KVM using a modem. The meaning of each parameter is described below. For further assistance with these settings, please contact your network administrator.

Serial line speed

Enter the speed the CAT5 8-PORT/16-PORT IP-KVM will communicate with the modem. Most modems available today will support the default value of 115200 bps. In case you are using an old modem and having connection issues, try to lowering this speed.

Modem Init String

Enter the initialization string used by the CAT5 8-PORT/16-PORT IP-KVM to initialize the modem. The default value will work with most standard modems directly connected to a telephone line. In case you have a special modem, or if 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 entering a new string. Refer to the modem's manual for the modem init string syntax.

Modem server IP address

Enter the IP address will be assigned to the CAT5 8-PORT/16-PORT 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 CAT5 8-PORT/16-PORT IP-KVM and your console computer. The default value will work in most cases.

Modem client IP address

Enter IP address that 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 CAT5 8-PORT/16-PORT 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 CAT5 8-PORT/16-PORT IP-KVM.

Serial Port Log

“Key Word 1”: The Serial Port Log function is used for console server applications. The data received from the selected serial port can be buffered in the CAT5 8-PORT/16-PORT IP-KVM’s memory or in an NFS server. The user can also define Key Words for that serial port, which will then trigger email notifications or SNMP traps that will be sent to an administrator if the keyword is found in the logged data.

11.5.6 Date/Time

Date/Time Settings

UTC Offset

User specified time *

Date / / (mm/dd/yyyy)

Time : : (hh:mm:ss)

Synchronize with NTP Server

Primary Time server *

Secondary Time server *

Apply **Reset to defaults**

* Stored value is equal to the default.

Figure 75: Date / Time

On this screen, the internal clock of the CAT5 8-PORT/16-PORT IP-KVM can be set. You can adjust the clock manually, or use an NTP time server. Without a time server, the time setting will be lost if the CAT5 8-PORT/16-PORT IP-KVM loses power for more than a few minutes. To avoid this, you can use an NTP time server, which sets the internal clock automatically according to the current UTC time. After making any changes, click **Apply** button to save your changes. You can click the **Reset to defaults** button to change settings back to the factory defaults.

UTC Offset: When using an NTP server to set the time automatically, use this setting to determine the offset for your time zone.

User Specified Time: Select this option to set the time manually. Enter the date and time using the formats specified.

Synchronize with NTP Server: Select this option to use an NTP server to set the time automatically. Enter the address of the NTP server you want to use in the **Primary Time server** text box. You can enter another NTP server in the **Secondary Time server** text box in the event that the Primary Time server is unavailable. Also, make sure you set the UTC Offset for your time zone by using the **UTC Offset** dropdown box at the top of the window.

Warning

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.

11.5.7 Event Log

Home Console Logout

Remote Control
Virtual Media
User Management
KVM Settings
Device Settings
Network
Dynamic DNS
Security
Certificate
Serial Port
Date/Time
Event Log
Authentication
USB
Config File
Maintenance

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

Figure 76: Event Log

Important events like a login failure or a firmware update are logged to several different destinations. Each type of event belongs to an event group for which logging can be separately activated or deactivated.

On the CAT5 8-POR/16-POR IP-KVM's web GUI, click **Device Settings > Event Log** to open the Event Log Targets and Event Log Assignments page. You can see the current event log by going to **Maintenance > Event Log**.

The following is a description of each of the fields on the **Device Settings > Event Log** screen:

- **List logging enabled**

The usual way to log events is to use the internal log list of the CAT5 8-POR/16-POR IP-KVM. To enable this internal log, tick the “List Logging Enabled” checkbox in **Device Settings > Event Log**. To view the actual log list, go to **Maintenance > Event Log**.

Since the CAT5 8-POR/16-POR IP-KVM's system memory is used to save the event log, the maximum number of saved log list entries is restricted to 1000 events. After this maximum is reached, older log entries will be deleted to make room for newer ones.

You can clear the internal log by clicking the **Clear** button.

Warning

If the reset button on the web GUI is used to restart the CAT5 8-POR/16-POR IP-KVM, all log data will be saved and will be available after the CAT5 8-POR/16-POR IP-KVM has been restarted. However, if the CAT5 8-POR/16-POR IP-KVM loses power or a hard reset is performed, all log data will be lost. To avoid this, use one of the following log methods.

- **NFS Logging enabled**

This allows you to log events to a file on an NFS server. To use NFS Logging, tick the **NFS Logging Enabled** checkbox and enter the **NFS Server**, **NFS Share**, and **NFS Log File** to use. To write log data from more than one CAT5 8-POR/16-POR IP-KVM devices to only one NFS share, you will need to use a unique NFS Log File name for each CAT5 8-POR/16-POR IP-KVM. After making your changes, click the **Apply** button. After applying the settings, the CAT5 8-POR/16-POR IP-KVM will try to mount the NFS share immediately, so make sure that the NFS share is online and accessible to the CAT5 8-POR/16-POR IP-KVM.

- **SMTP Logging enabled**

This allows the CAT5 8-POR/16-POR IP-KVM is able to send event e-mails to the specified e-mail address. These mails contain the same description strings as the internal log file, and the mail subject will contain the event group of the log event. In order to use SMTP Logging, tick the **SMTP Logging Enabled** checkbox, enter the **SMTP Server** (<server IP>: <port>), **Receiver Email Address**, and **Sender Email Address**, then click the **Apply** button to save your changes.

Note: The SMTP Server must be reachable by the CAT5 8-PORT/16-PORT IP-KVM, and must require no authentication.

- **SNMP Logging enabled**

If this is activated, the CAT5 8-PORT/16-PORT 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 the information about the log event. Only authentication and host power events have their own trap class that consists of several fields with detailed information about the event. To receive this SNMP traps, any SNMP trap listener may be used.

Here is an example of all generated event and its event group.

Loggable Events and their Event Groups	
Events	Event Group
Device successfully 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

Warning

In contrast to the internal log file on the CAT5 8-PORT/16-PORT 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.

11.5.8 Authentication

Authentication Settings

Local Authentication *

LDAP

User LDAP Server *

Base DN of User LDAP Server *

Type of external LDAP Server *

Name of login-name attribute *

Name of user-entry objectclass *

User search subfilter *

Active Directory Domain *

RADIUS

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

* Stored value is equal to the default.

Figure 77: Authentication Setting

On this screen, you can specify how the CAT5 8-POR/16-POR IP-KVM will look to authenticate the users. By default, Local Authentication is enabled, which means users will need to use a user account configured on the CAT5 8-POR/16-POR IP-KVM.

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 CAT5 8-POR/16-POR 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 there is always a "back door" to the CAT5 8-POR/16-POR IP-KVM.

LDAP Access

The CAT5 8-PORT/16-PORT IP-KVM uses LDAP only for authentication (password verification). User privileges and private settings are still stored locally at the CAT5 8-PORT/16-PORT IP-KVM. That's why a user account has to be created on the CAT5 8-PORT/16-PORT IP-KVM before this user can login via LDAP. Also, all privilege configurations have to be done within the CAT5 8-PORT/16-PORT IP-KVM user management.

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

- **SMTP Logging enabled**

This allows the CAT5 8-PORT/16-PORT IP-KVM is able to send event e-mails to the specified e-mail address. These mails contain the same description strings as the internal log file, and the mail subject will contain the event group of the log event. In order to use SMTP Logging, tick the SMTP Logging Enabled checkbox, enter the SMTP Server (<server IP>: <port>), Receiver Email Address, and Sender Email Address, then click the Apply button to save your changes.

- **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 subfilter**

Here you can refine the search for users that should be known to the CAT5 8-PORT/16-PORT 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

Using the RADIUS Server

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. We can give a recommendation for all products listed above, especially for the free RADIUS implementation.

Note: *Currently, we do not support challenge/response. An Access Challenge response is seen and evaluated as an Access Reject.*

To access a remote device using the RADIUS protocol you have to login, first. You are asked to specify your user name and password, then. The RADIUS server reads your input data (Authentication) and the CAT5 8-PORT/16-PORT 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. In terms of the remote activity mechanism the login via RADIUS works similar to the Remote Console. If there is no activity for half an hour your connection to the CAT5 8-PORT/16-PORT IP-KVM will be aborted and closed.

Server

Enter either the IP address or the hostname of the RADIUS Server to connect to. For the hostname DNS has to be configured and enabled.

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 CAT5 8-PORT/16-PORT IP-KVM serves 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). For the shared secret you can use any standard alphanumeric and special characters. A shared secret may consist of up to 128 characters in length and may contain both lowercase and uppercase letters (A-Z,a-z), numerals (0-9) and other symbols (all characters not defined as letters or numerals) such as an exclamation mark (!) or an asterisk (*).

Authentication Port

The port the RADIUS server listens for authentication requests. The default value is #1812.

Accounting Port

The port the RADIUS server listens for accounting requests. The default value is #1813.

Timeout

Sets the request time-to-live in seconds. The time-to-live is the time to wait for the completion of the 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.

11.5.9 USB



* Stored value is equal to the default.

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

11.5.10 Config File



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

11.6 Maintenance

The administrator can perform various maintenance activities on the CAT5 8-PORT/16-PORT IP-KVM. These include viewing its status, updating its firmware, viewing the event log and resetting the unit.



11.6.1 Device Information

The Device Status page contains a table with information about the hardware and firmware of CAT5 8-PORT/16-PORT IP-KVM. 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 78: Device Information

The Data file for support allows you to download the CAT5 8-PORT/16-PORT 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 79: Connected Users

The Connected Users field at the bottom of the Device Information field(see the screenshot above) displays the status of connected users. For every user, it lists the username, the IP address of the network host that the user is connecting from, and the activity status.

RC means that the Remote Console is open and active on that user’s computer. If the Remote Console is opened in Exclusive Access mode, the term “exclusive” is added. For more information about this option, see the Section **4.3.2 Control Bar of the Remote Console**.

The column on the far right displays either the term “active” for an active user, or shows the number of minutes that the user has been inactive..

11.6.2 Event log

The Event Log displays all events that are logged by the CAT5 8-PORT/16-PORT IP-KVM (see screenshot below).

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.

[Prev] [Next]

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.

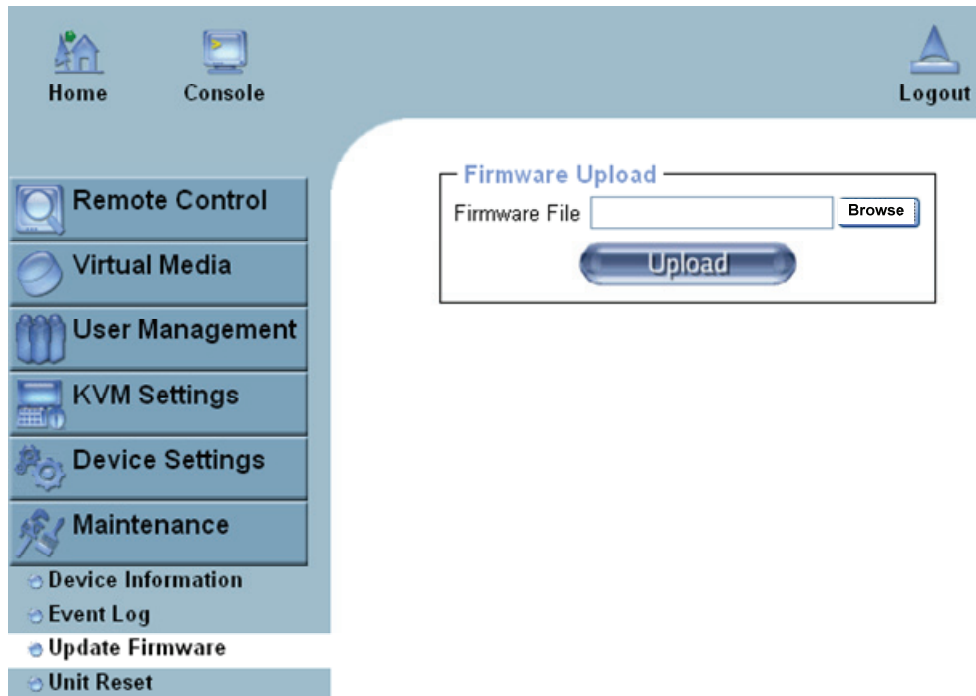
[Prev] [Next]

Figure 80: Event Log List

11.6.3 Update Firmware

Firmware can be easily upgraded via web page. This section describes the upgrade procedures.

The CAT5 8-PORT/16-PORT IP-KVM is a complete, independent, standalone computer. The software it runs is called firmware. The firmware of the CAT5 8-PORT/16-PORT



IP-KVM 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 supplier web site. If the firmware file is compressed (file suffix .zip) then you must unzip it before you can proceed. Under the Windows operating system you may use WinZip from <http://www.winzip.com/> for decompression. Other operating systems might provide a program called unzip.

Before you can start updating the firmware of your CAT5 8-PORT/16-PORT IP-KVM the new uncompressed firmware file has to be accessible on the system that you use for connecting to the CAT5 8-PORT/16-PORT IP-KVM.

Warning !!!

This process is not reversible and might take few minutes. During this upgrading process, we should not disconnect the power or the Ethernet cable, since it may causes upgrade failure and destroy the image in Flash memory.

The CAT5 8-PORT/16-PORT 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.

Warning !!!

CAT5 8-POR/16-POR IP-KVM will verify firmware checksum before proceed upgrade procedure. The mechanism help to prevent false firmware file to damage CAT5 8-POR/16-POR IP-KVM. It is crucial to keep a steady power supply during the procedure otherwise the power-off event may damage the permanent storage and disable CAT5 8-POR/16-POR IP-KVM

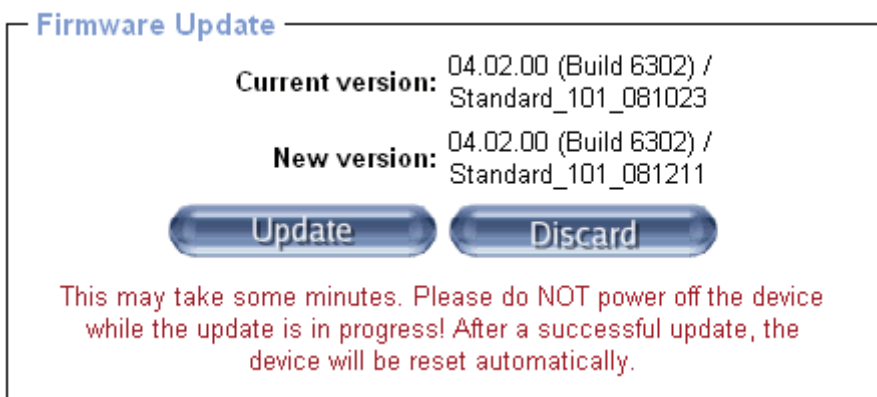
Updating the firmware is a three-stage process:

1. Upload the new firmware file onto the CAT5 8-POR/16-POR IP-KVM unit.



In order to do that you need to select the file on your local system using the button “**Browse**” of the Upload Firmware panel. 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.

2. If everything went well, you see the Update Firmware panel.

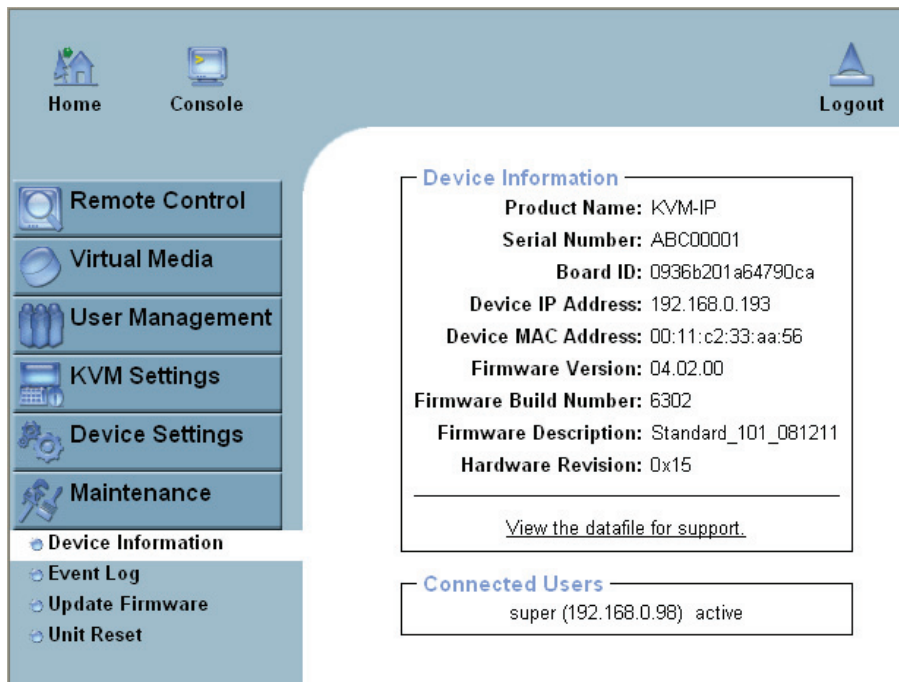


The panel shows you the version number of the currently running firmware and the version number of the uploaded firmware. Pressing **Update** will store the new version and substitute the old one completely.

3. After the firmware updated successfully, the device will be rebooted and redirected to the login web page automatically.



Check out the device information to see the updated firmware is running.



11.6.4 Unit Reset

This section allows you to reset specific parts of the device, such as the settings for the keyboard and mouse, USB, the video engine, and the entire CAT5 8-POR/16-POR IP-KVM device itself. In the event of an abnormal operation, the subsystems may be reset without resetting the entire CAT5 8-POR/16-POR IP-KVM.

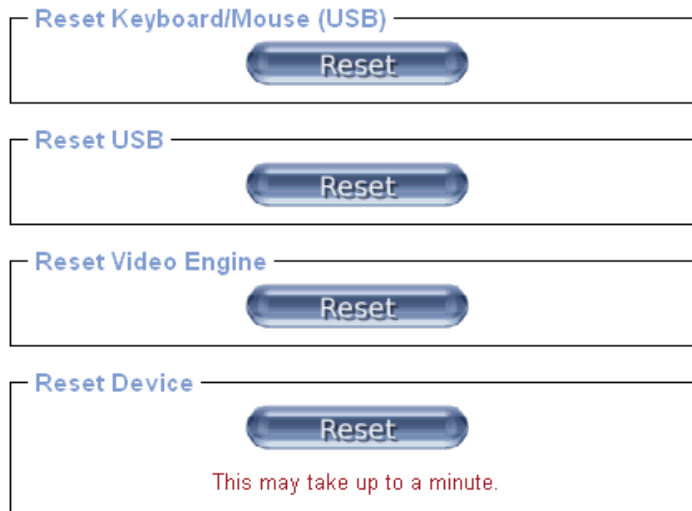


Figure 81: Unit Reset

To reset a specific functionality, click on the related **Reset** button.

Clicking on **Reset** button in the **Reset Device** field will reboot the entire CAT5 8-POR/16-POR 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 subsystems (e.g. the video engine) will take only a few seconds and will not cause the device's network connections to close.

Note: Only the super user is allowed to reset the CAT5 8-POR/16-POR IP-KVM.

11.6.5 Reset Factory Defaults

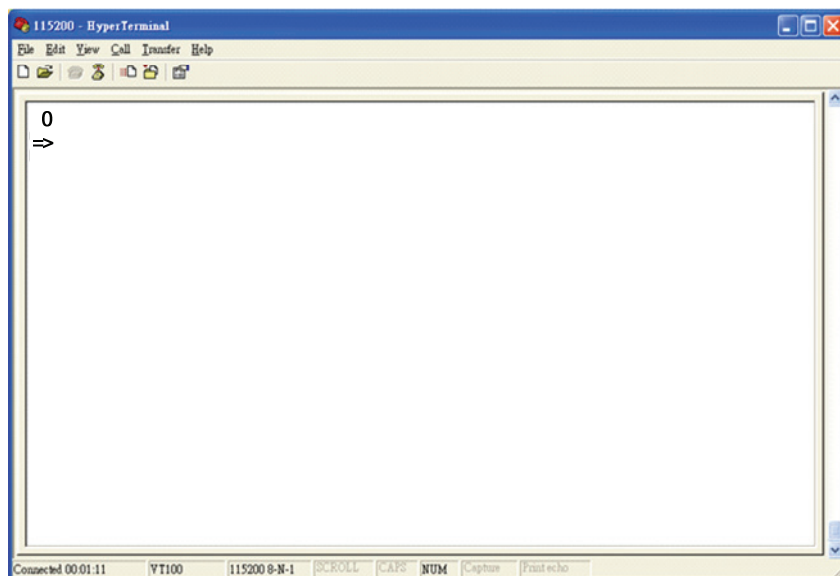
This function can be used if you forget the password for logging in to the CAT5 8-PORT/16-PORT IP-KVM, or if you want to return the CAT5 8-PORT/16-PORT IP-KVM to its factory default settings as it was when you purchased it.

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

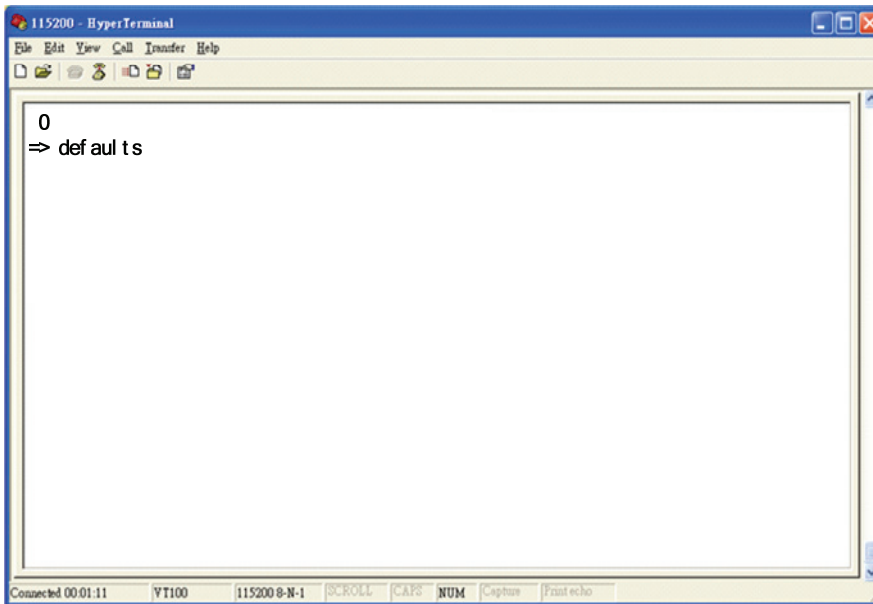
The following procedures will return the CAT5 8-PORT/16-PORT IP-KVM to factory default settings:

1. Connect a RS232 null modem cable from your local console PC to the CAT5 8-PORT/16-PORT IP-KVM Serial port. Configure your terminal emulation program (such as **HyperTerminal** or **PuTTY**) with the following settings: Baudrate **115200**, Data/stop bits **8-1**, Parity **none**, Flow control **none**.
2. Enter the debugging mode via reboot the CAT5 8-PORT/16-PORT IP-KVM system and hit the ESC key. There are two ways to enter the debugging mode:
 - (a) Reboot the CAT5 8-PORT/16-PORT IP-KVM device. During the first 2 seconds of boot-up, press the **ESC** key (on the computer that's connecting through the serial port) a few times to get to a => prompt.
 - (b) Press and hold the computer's **ESC** button **while** you push and release the CAT5 8-PORT/16-PORT IP-KVM's **Reset** button, and then release the **ESC** button after 2 seconds.

The debugging mode window will appear as shown below.

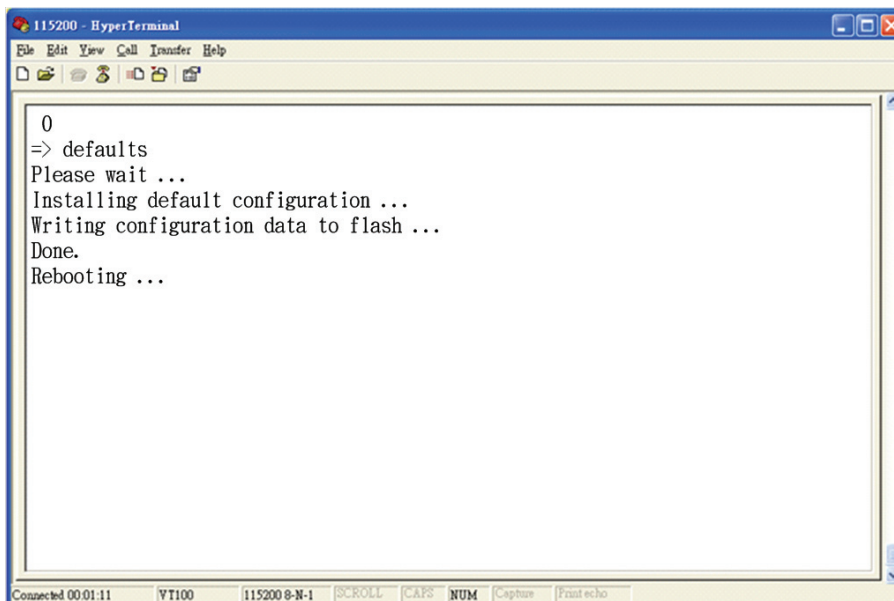


3. Key in "**defaults**" command and then **Enter**. The unit will automatically set to factory default settings and reboot the system.



Warning: Resetting the CAT5 8-PORT/16-PORT IP-KVM to factory defaults will clear all settings on the device.

4. The window will display the following information when the reset to factory defaults had been completed, and the CAT5 8-PORT/16-PORT IP-KVM will automatically reboot.



12. FAQ

1. **Does any software require on servers which connect to the CAT5 8-PORT/16-PORT IP-KVM?**

No, the CAT5 8-PORT/16-PORT IP-KVM is a 100% hardware solution. No extra software required.

2. **What operating systems does CAT5 8-PORT/16-PORT IP-KVM support?**

The CAT5 8-PORT/16-PORT IP-KVM supports Windows, Unix, Unix-like Operating System (Sun Solaris, Linux) and Mac OS.

3. **What web browsers does the CAT5 8-PORT/16-PORT IP-KVM support?**

The CAT5 8-PORT/16-PORT IP-KVM support Microsoft Internet Explorer 6 and above, Netscape, Mozilla, Safari, Firefox, Avant, World, Opera, and other web browsers.

4. **What Java version should the user install?**

We need to install Java Runtime Environment (version 1.5 or above) on the remote console PC.

5. **Does the CAT5 8-PORT/16-PORT IP-KVM work with KVM switches made by other companies?**

Yes, the CAT5 8-PORT/16-PORT IP-KVM can work with most of standard KVMs.

6. **When you set up the username and password, what is the maximum number of letters and digits that can be used?**

The CAT5 8-PORT/16-PORT IP-KVM accepts up to 32 letters and digits for the username and password.

7. **How many users can access the CAT5 8-PORT/16-PORT IP-KVM at the same time?**

The CAT5 8-PORT/16-PORT IP-KVM can accommodate up to 15 concurrent users.

8. **What level of data encryption does the CAT5 8-PORT/16-PORT IP-KVM provide?**

The CAT5 8-PORT/16-PORT IP-KVM provides RSA 2048-bit encryption for authentication, and AES 256-bit encryption for data.

9. **How do I set up keystroke hotkeys for commands such as CTRL+ALT+DEL?**

Remote Console Button Keys allow you to send keystroke combinations to the Host computer that normally cannot be generated on the Remote computer. Typical examples are "CTRL+ALT+DEL" on Windows and DOS, or "CTRL+ALT+Backspace" on Unix or Unix-like operating systems for rebooting X-Server. Please refer to section **11.4.1 User Console** for more information on creating Remote Console Button Keys.

13. Troubleshooting

1. I can't bring up the login page of CAT5 8-PORT/16-PORT IP-KVM web server.

Check to make sure that the CAT5 8-PORT/16-PORT IP-KVM is powered on, and that your network configuration (IP address, subnet mask, router, firewall, etc.) is correct. Try to ping the IP address of the CAT5 8-PORT/16-PORT IP-KVM to find out whether the CAT5 8-PORT/16-PORT IP-KVM is reachable. If you cannot reach the CAT5 8-PORT/16-PORT IP-KVM, you will not be able to go to its login page.

2. I forgot my password. How can I reset the CAT5 8-PORT/16-PORT IP-KVM to factory defaults?

For a detailed description of this process, see the Section **11.6.5 Reset Factory Defaults**.

3. I can't log in to the CAT5 8-PORT/16-PORT IP-KVM.

Was the correct combination of user and password given? On delivery, the user "super" has the password "pass". Moreover your browser must be configured to accept cookies.


4. When a PC connects to the Host via USB and runs the PSetup utility, an error message occurred: "Exception processing message ..."

This may be due to improper BIOS settings. If the Host system is not equipped with a floppy disk drive, check the BIOS to make sure it is set to "No floppy drive installed".

5. The CAT5 8-PORT/16-PORT IP-KVM web GUI are inconsistent or chaotic.

Make sure your browser cache settings are not set to "never check for newer pages" or something similar. Otherwise, web pages may be loaded from your browser cache and not from the CAT5 8-PORT/16-PORT IP-KVM device itself.

6. The Remote Console window of CAT5 8-PORT/16-PORT IP-KVM can not be opened.

(1) Please make sure that the Remote computer has Java Runtime Environment v1.5 or above installed. When trying to open the Remote Console, the  icon will appear at the top right corner of the screen if the Java Runtime Environment is not installed.

Notes:

1. In order to run this function, the Remote system need support JRE (Java Runtime Environment) version 5.0 (v1.5) or above. You can get the Java Software from the website <http://www.java.com/en/download/>
2. It's recommended to install newer Java version (e.g., version 6 update 11 or above) for better performance.

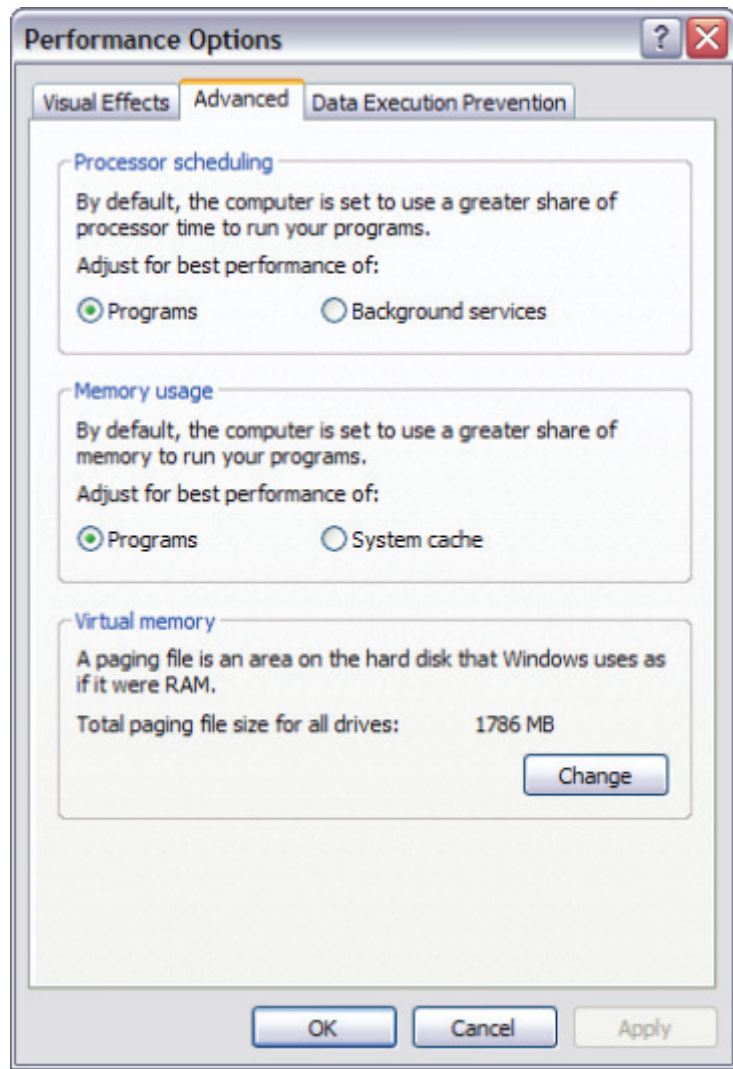
(2) It is also possible that a firewall is preventing access to the Remote Console. Make sure the TCP port **443** (for both HTTPS and RFB) and port 80 (for HTTP) are open for the CAT5 8-PORT/16-PORT IP-KVM to receive incoming TCP connection attempts.

7. The Remote Console (Java Applet) hanged.

The reason for this may be related to your Windows memory management configuration. Often, the issue is that Windows has allocated more memory to system cache than to applications.

Try the following steps to solve this issue:

- (a) Go to **Control Panel > System**.
- (b) In the **Advanced** tab, click **Performance Settings**.
- (c) Click the Advanced tab.
- (d) If **System cache** is selected in **Memory Usage**, change it to **Programs** and click the **OK** button to save your changes. (See the screenshot below.)
- (e) Restart the computer. The problem should be solved now.



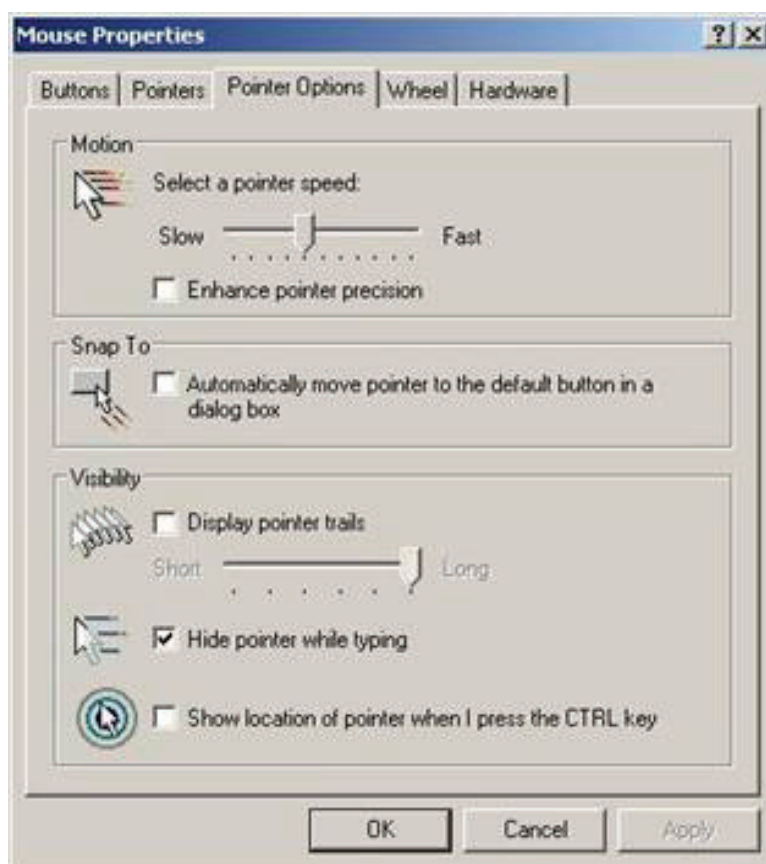
8. Local mouse and remote mouse are not in sync after doing mouse Intelligent Sync.

Please don't place the pointer on the upper left-hand corner of Remote Console window. Intelligent Sync (Options > Mouse handling) will re-calculate the coordinate of

the pointer from upper left-hand corner of Remote Console window. If still not in sync, please ensure that the “Enhance pointer precision” tab is not checked in the Windows Control Panel of the Host system. (For Windows XP, the click sequence to this setting is **Control Panel > Printers and Other Hardware > Mouse > Pointer Options**). See page 20 for detailed information.

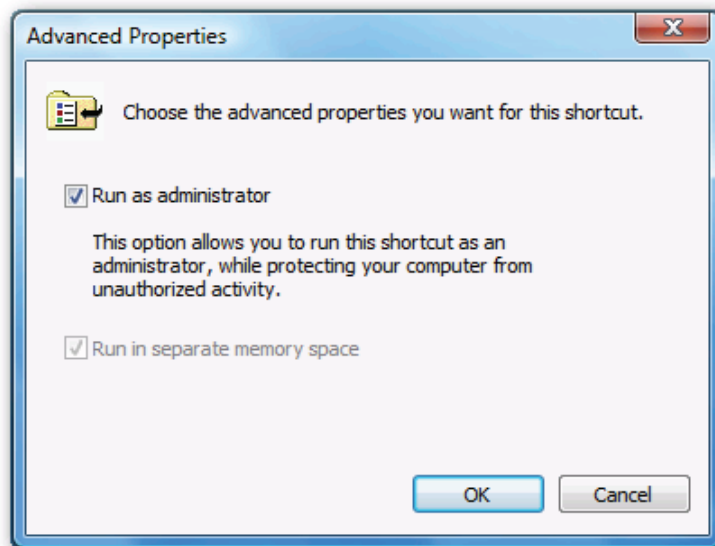
9. **In Double mouse mode, the Host and Remote mouse pointers are not in sync, even after clicking the “Sync” button.**

Check to make sure that the mouse settings on your Host computer have the options “Enhance pointer precision” or “Automatically move mouse pointer to the default button in a dialog box” disabled. (For Windows XP, go to **Control Panel > Printers and Other Hardware > Mouse > Pointer Options**). See page 20 for detailed information



10. **In Windows Vista, the mouse won’t work in the Remote Console window, and Drive Redirection also doesn’t work.**

Try running Internet Explorer in Administrator mode. To do this, right-click on a shortcut to IE, and tick the checkbox next to "Run as administrator". Alternatively, right-click on the IE shortcut, select Properties, Shortcut-Advanced Properties, and tick the checkbox next to "Run as administrator".



11. The Virtual Media (Drive Redirection) fails to connect to a USB drive

This may be due to improper BIOS settings. If the PC is not equipped with a floppy disk drive, check the BIOS to make sure it is set to “No floppy drive installed”.


12. When connecting Local console, the computer VGA resolution does not match the monitor’s resolution.

Make sure VGA resolution works fine if directly connect the monitor to the computer. Please turn off the computer, wait few seconds then turn on again. Notice that during computer startup, it will try to obtain the information of the connected monitor resolution from its VGA port. So before computer startup, the monitor and KVM switch should be already ON and running.

Please follow the power up procedures: power on monitor, power on CAT5 8-PORT/16-PORT IP-KVM, wait for CAT5 8-PORT/16-PORT IP-KVM startup complete (about 60 seconds), and then power on the Host (Target) computer.

13. The video quality is bad or the picture is grainy

Adjust the brightness and contrast settings (in Options > Video Settings) until

satisfaction, or click on the “Auto Adjust Video” button  to correct a flickering video.

14. The video on the Remote Console window is surrounded by a black border.

The black bars may be caused by a fixed video mode where the resolution of the video is smaller than the window size. The video mode can be changed in the video settings of the CAT5 8-PORT/16-PORT IP-KVM. Refer to Section called **Control Bar of Remote Console** in Chapter 4 for more information.

15. The Remote-side monitor shows video, but the Remote Console window remains blank.

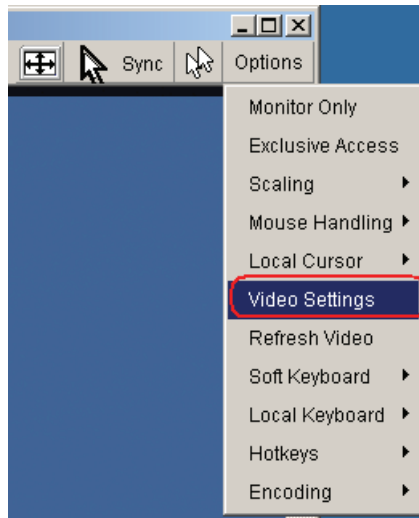
Check to make sure that the Remote Console is connected by checking the Status Bar at the bottom of the Remote Console window. If the connection is active, you should verify that the flat panel interface (VGA interface) is not switched off by the video driver

of your operating system.

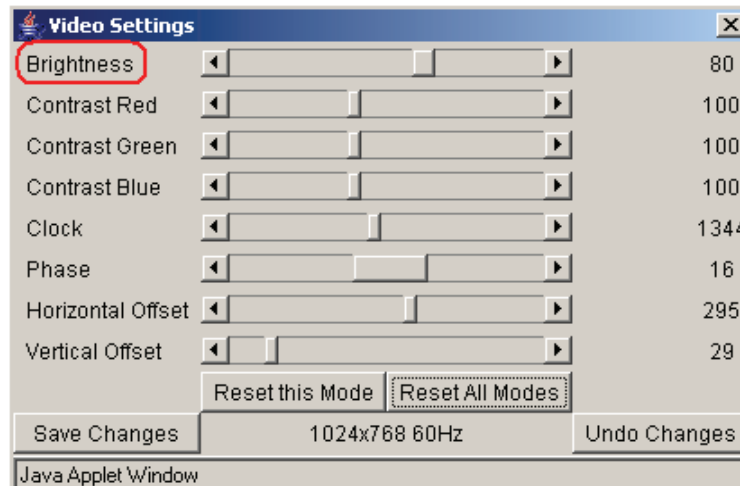
16. Video in the Remote Console window has a pinkish tint.

Try adjusting the brightness of the Host Console window by following these steps:

(a) Click **Video Settings** in Options menu of the Remote Console.



(b) Adjust the **Brightness** setting until the pinkish tint is reduced or eliminated.



17. Special key combinations, e.g. ALT+F2, ALT+F3 are intercepted by the console system and not transmitted to the host.

You can create a Remote Console Button Key to send the keystroke combination for you. This can be done in the **KVM Settings > User Console** screen of the CAT5 8-PORT/16-PORT IP-KVM's web GUI. For more information, refer to section **11.4.1 User Console**.

18. I can't upload the signed certificate in Mac OS X

If an "internal error" occurs while uploading the signed certificate, either change the extension of the file to .txt or add a file helper using the Internet Explorer preferences for this type of file. Make sure that the encoding is plain text and the checkbox "use for outgoing" is checked. Alternatively, try using a Mozilla-based browser such as Firefox.

19. The Remote Console does not open with Opera in Linux.

Some versions of Opera do not grant enough permission if the signature of the applet cannot be verified. To solve the problem, add the following lines to the java policy file of

Opera (e.g. /usr/share/opera/java/opera.policy):

```
grant codeBase "nn.pp.rc.RemoteConsoleApplet" { permission java.lang.RuntimePermission  
"accessClassInPackage.sun.*";}
```

to the java policy file of opera (e.g. /usr/share/opera/java/opera.policy).

14. KVM Firmware Upgrade Procedures

The KVM switch provides the firmware update for the following functions:

- **USB console:** Update for USB console keyboard/mouse compatibility.
The firmware filename for USB console is like **OTG_CAT5KVM_SCAN_Vx.xx.300**.
- **PORT0:** Update for 1~8 Port communication.
The firmware filename for PORT0 is like **CK_PortCOM_Vxxx.300**.
- **PORT1:** Update for 9~16 Port communication.
The firmware filename for PORT1 is like **CK_PortCOM_Vxxx.300**
- **CSL1:** Update for PS/2 console and on-screen-display.
The firmware filename for CSL1 is like **CK_CSLOSD_Vxxx.300**.
- **CSL2:** Update for PS/2 console keyboard/mouse compatibility.
The firmware filename for CSL2 is like **CK_CSL2_Vxxx.300**.

To update the firmware, please do the followings:

1. Disconnect all the KVM cable between KVM and computer.
2. Disconnect all the keyboard and mouse plugged on KVM.
3. Disconnect the VGA cable between KVM and monitor.
4. Apply DC 12V adapter to the KVM.
5. Execute the firmware update utility “Prog182S.EXE”.

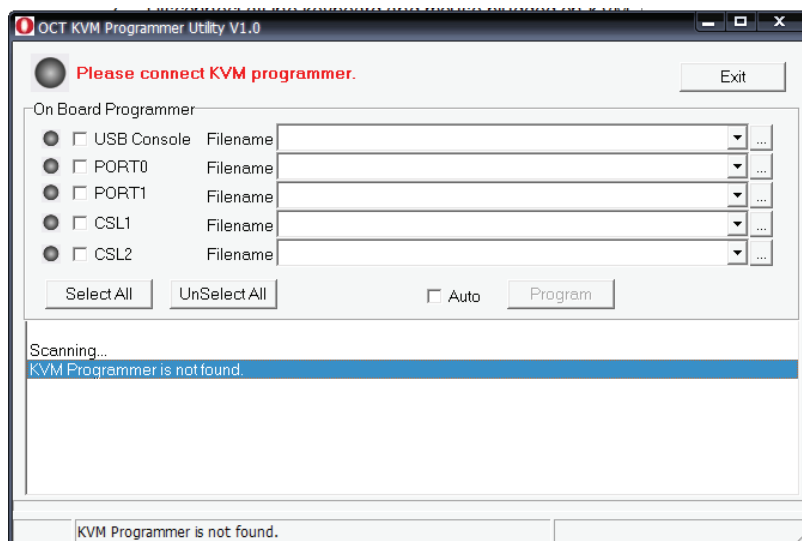


Figure 82: Firmware Upgrade Utility

6. Use the mini-USB cable to connect KVM firmware update port and the USB port of computer which runs the firmware update utility.



Figure 83: Connect KVM and PC by mini-USB cable

7. The utility will scan the KVM programmer automatically.

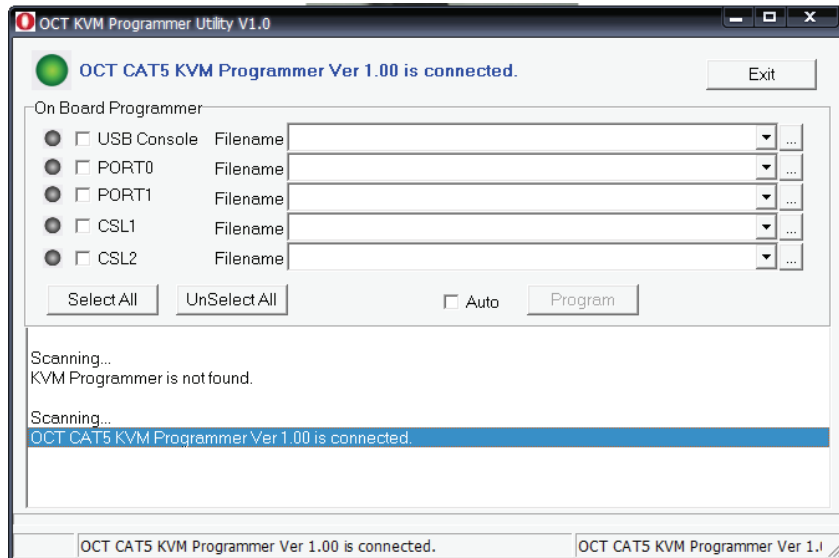


Figure 84: Programmer Connection Status

8. Please select the target by enabling the check box, for example “USB Console”, and click the file browsing button to select the firmware file to update.

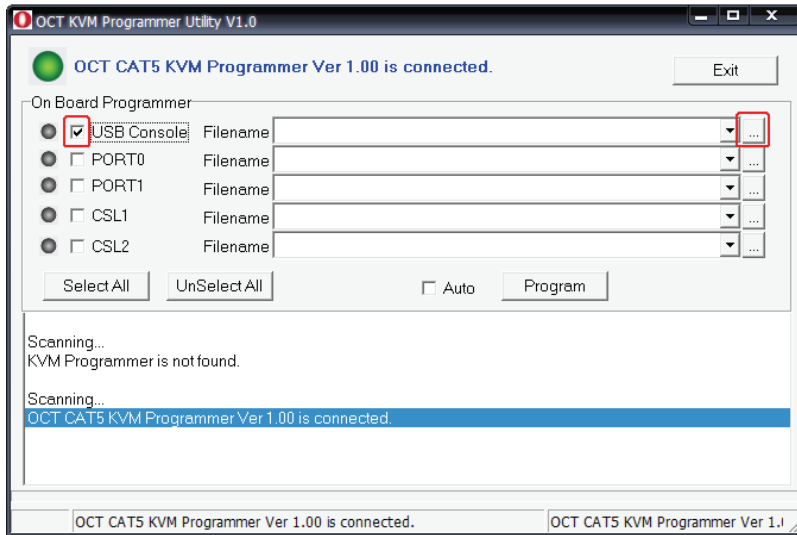


Figure 85: Check Updated Port

9. Select the firmware file to update.

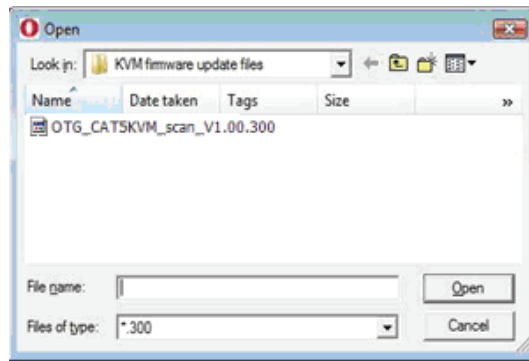


Figure 86: Select Firmware File

10. Click the "Program" button to start firmware programming.

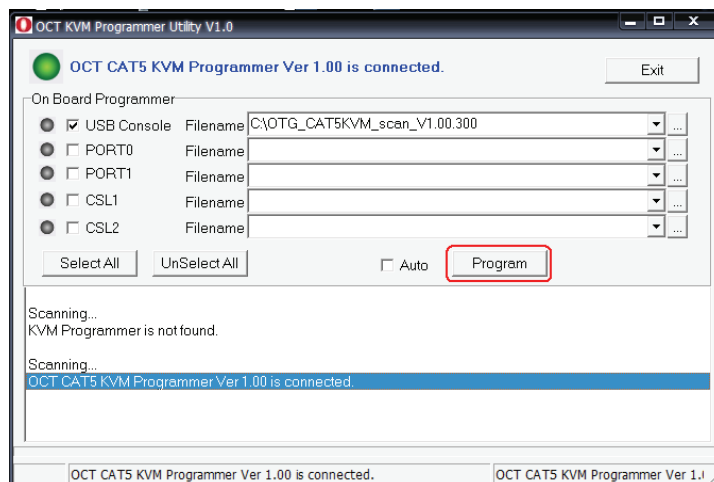


Figure 87: Click "Program" button

11. A status bar is shown under the panel to indicate the update progress.

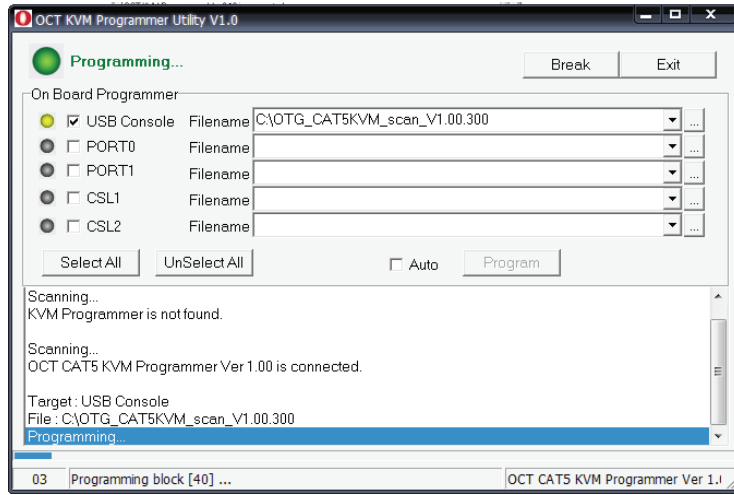


Figure 88: Programming Progress

12. The firmware is updated successfully.

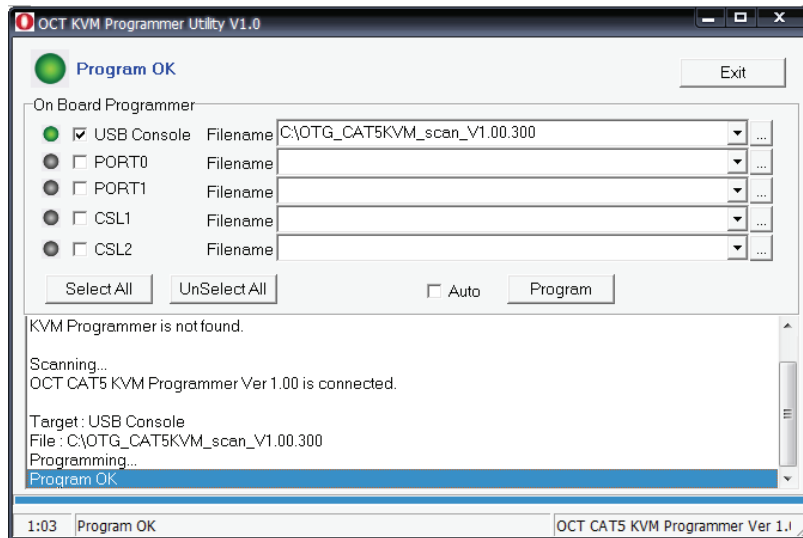


Figure 89: Programming Finished

B. Video Modes

The table below lists the video modes that the CAT5 8-PORT/16-PORT IP-KVM supports. Please don't use other custom video settings. If you do, the CAT5 8-PORT/16-PORT IP-KVM may not be able to detect them.

Resolution (x, y)	Refresh Rates (Hz)
640 x 480	60, 72, 75
800 x 600	56, 60, 70, 72
1024 x 768	60, 70, 72
1152 x 864	75
1280 x 960	60
1280 x 1024	60, 75
1600 x 1200	60
1920 x 1200 (local console)	60

C. User Role Permissions

The table below lists the user authorization permissions granted for the three user authority categories: "Super User", "Administrator", and "User"

Function	User	Administrator	Super
Remote Control: KVM	x	x	x
Remote Power Wakeup	-	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 a different Compression and Color Depth configuration in order to match the different bandwidth limitations of the network type (UMTS, ISDN, etc.)

The following suggested network bandwidth planning table for CAT5 8-PORT/16-PORT 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. Well-Known 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. The 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

H. Protocol Glossary

BOOTP (Bootstrap Protocol)

Similar to DHCP, but for smaller networks. Automatically assigns the IP address for a specific duration of time.

CHAP (Challenge Handshake Authentication Protocol)

A secure protocol for connecting to a system; it is more secure than the PAP.

DHCP (Dynamic Host Configuration Protocol)

Internet protocol that automating the configuration of computers that use TCP/IP.

DNS (Domain Name Servers)

A system that allows a network name server to translate text host names into numeric IP addresses.

LDAP (Lightweight Directory Access Protocol)

A protocol for accessing directory information.

NAT (Network Address Translation)

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)

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)

A protocol used to synchronize time on networked computers and equipment.

PAP (Password Authentication Protocol)

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)

A protocol for creating and running IP and other network protocols over a serial link.

RADIUS (Remote Authentication Dial-In User Service)

An authentication and accounting protocol. It 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)

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)

TCP/IP protocol for sending email between servers.

SSL (Secure Sockets Layer)

A protocol that provides authentication and encryption services between a web server and a web browser.

SSH (Secure Shell)

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.

Disclaimer

Information in this document is subject to change without notice. The manufacturer does not make any representations or warranties (implied or otherwise) regarding the accuracy and completeness of this document and shall in no event be liable for any loss of profit or any other commercial damage, including but not limited to special, incidental, consequential, or other damages.

No part of this document may be reproduced or transmitted in any form by any means, electronic or mechanical, including photocopying, recording or information recording and retrieval systems without the express written permission of the manufacturer.

All brand names and product names used in this document are trademarks, or registered trademarks of their respective holders.

FCC Statement

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

- Reorient or relocate the receiving antenna.
- Increase the separation between the device and receiver.
- Connect the computer into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

