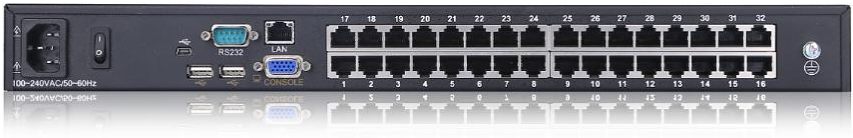
CAT5 KVM over IP Switch

(8 Port / 16 Port / 32 Port)

User Manual



Printing date: 2018/03

Version: V3.0

Contents

1. Product Overview

1.1 Brief Introduction

KVM – over – IP (Hereinafter refers to IP-KVM) reloads the local keyboard, mouse and video to a remote management console. Operator can safely get the BIOS level access, maintenance, support and recover system fault by using the standard Internet browser. It has passed SLL security certification and has been encrypted.

IP-KVM can easily access and control the remote KVM via LAN or Internet. It gathers the compressed video signal and the keyboard/mouse signal, then converts them into digital signal and transmits to the remote computer. IP-KVM supports remote access and provides solutions for control non-invasion remote.

It is easy and fast to install the KVM console; you just need to connect corresponding cables to the right ports of KVM and its module without software configuration. Connect multiple computers with RJ-45 connector and CAT5 cable, transmitting distance is up to 150M without a KVM extender.

1.2 Features

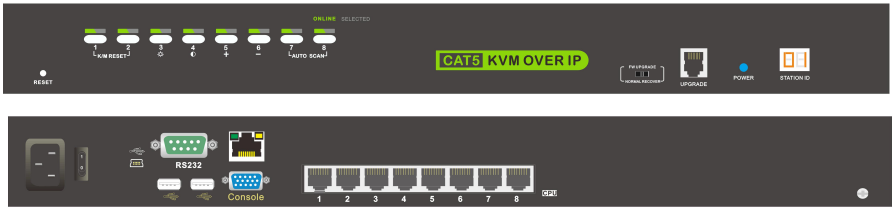
- Access and control up to 8/16/32 computers
- Supports USB keyboard and mouse console
- Two level password security--only authorized users view and control computers; up to four users and an administrator with a separate profile for each
- Convenient computer switching via front panel LEDs, hotkeys and OSD menu
- Auto scan feature for monitoring user-selected computers

- Hot pluggable --add or remove computers without having to power down the switch
- Broadcast mode--operations simultaneously performed on all selected computers
- Easily select port via mouse
- Manage server all around the world
- Remote access to the KVM(Keyboard, video and mouse) through modem
- Support any operating system even in BIOS level, during start up or in blue screen
- Support virtual media and hardware redirection
- Supports JAVA browser remote control
- All transmitting data are encrypted with SSL 265 bits
- SSL certificate management
- Automatically senses video resolution for best possible screen capture
- High-performance mouse tracking and synchronization

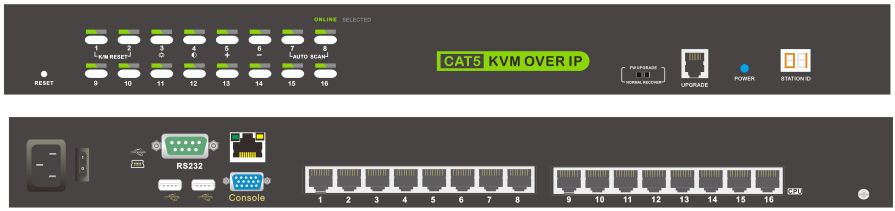
2. Installation and Start-up

2.1 Panel View

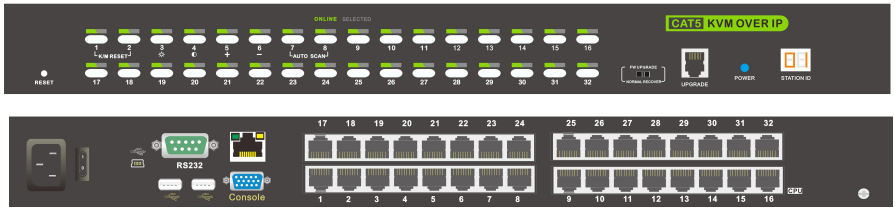
8 Port KVM



16 Port KVM



32 Port KVM



2.2 System requirement

Hardware

Item	Description
Local Host	8 or 16 PC/server
Local Console	One USB keyboard, one USB mouse and one monitor
Remote Console	1 PC or multiple computers connected to the network

Software

Item	Description
Local Host	No required extra software
Remote Console	(1)Java operating environment:version1.4.2 or higher (2)Browser: Microsoft Internet Explorer (version6.0 and above or Netscape or Mozilla or Safari)

2.3 When the server is up and running

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

1.Restart the system.
2. Watch the boot process.
3. Boot the system from a separate partition to load the diagnostic environment.
4. Run special diagnostic program.

2.4 When the server is dead

Obviously, fixing hardware defects is not possible through a remote management device.

Nevertheless KVM-over-IP gives the administrator valuable information about the type of a hardware failure. Serious hardware failures can be categorized into five different categories with different chances to happen:

1.Hard disk failure 50%
2.Power cable detached, power supply failure 28%
3.CPU, controller, main board failure 10%
4.CPU fan failure 8%
5.RAM failure 4%

Using KVM-over-IP, administrators can determine which kind of serious hardware failure has occurred

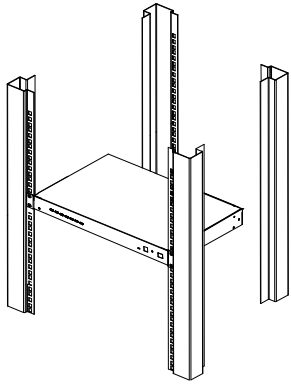
Type of Failure	Detected by
Hard disk failure	Console screen, CMOS set-up information
Power cable detached, power supply failure	Server remains in power off state after power on command has been given.
CPU Controller, main board failure.	Power supply is on, but there is no video output.
CPU fan failure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

2.5 Rack Mounting

The IP-KVM can be put on the desktop or rack mounted in standard 19” /1U rack:

Make sure all the connecting computers and external device are shut down before installation.

Put the KVM switch in a fit place, screw the brackets to the two sides of the switch, then screw the switch to the 19” rack. Keep a certain distance between the host computer, switch, monitor, keyboard and mouse when installation.



2.6 Single Station Installation

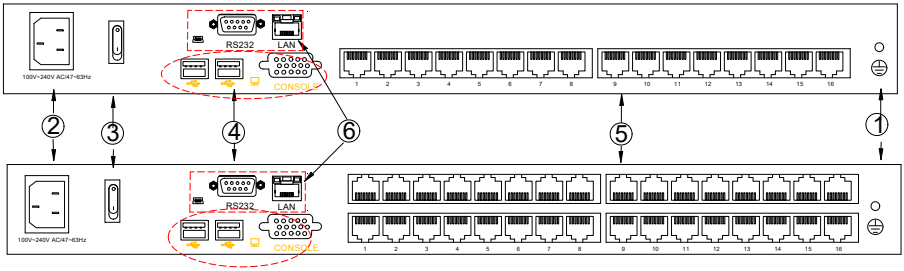
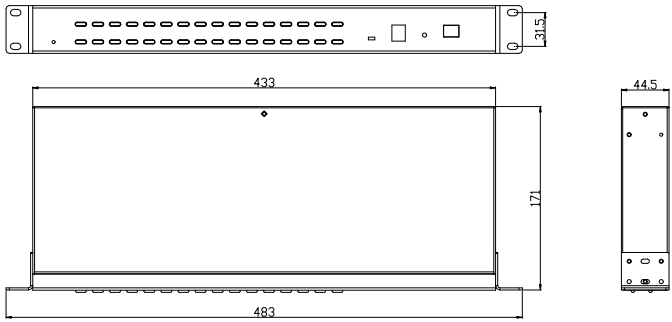


Diagram 2.1 Install KVM components

Table 1.1

No.	Explanation
1	Ground Connection Screw
2	Power Input(AC or DC)
3	Power Switch
4	Local Console
5	PC Connection Port
6	IP Port

Structure and Size



Single Station Installation:

1) Make sure the IP KVM has been connected to the ground.
2) Connect PC or server to KVM with KVM adapter and CAT5 cable according to number ② and③ in below diagram.
3) Connect IP KVM's LAN port to the Internet (see number ⑤ in below diagram).
4) Connect 220V AC power(see number ④ in below diagram), then turn on power switch ⑦ and the KVM start auto-checking and make "beep" sound.
5) Connect the local console (keyboard, monitor and mouse) to the console port. (see number ⑥ in below diagram),
6) Power on PC or server.

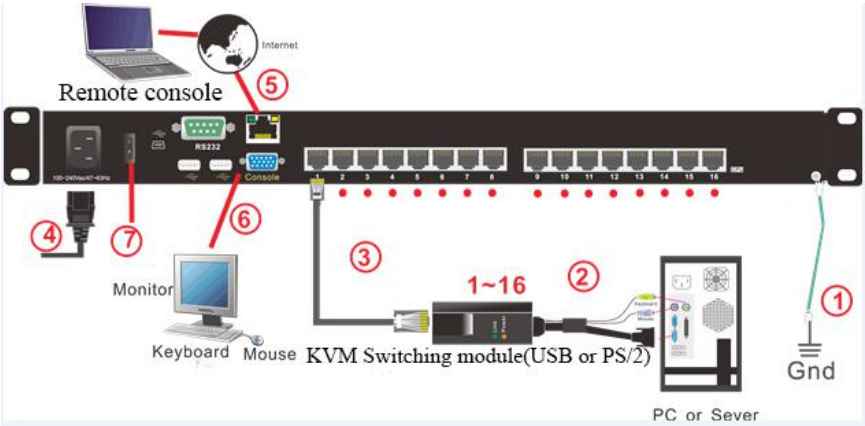
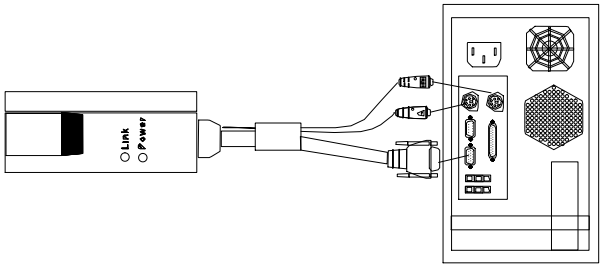


Diagram 2.3 Installation diagram

Module

PS/2 CPU module



USB CPU module

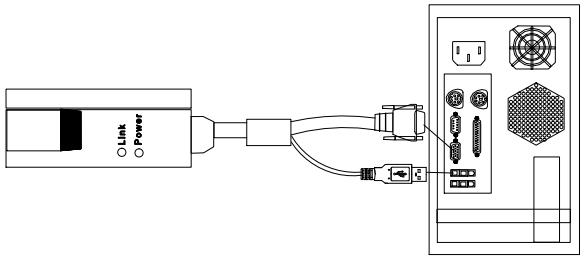


Table 1.3: Module LEDs

Components	Function	
Power LED	Flashing green light	The module is power on
	Green light keeps on	The module has been connected to the KVM
Link LED	Quickly flashing	The module is communicating with the host
	Orange light keeps on	The module has been selected by the KVM switch

2.7 Cascade Installation

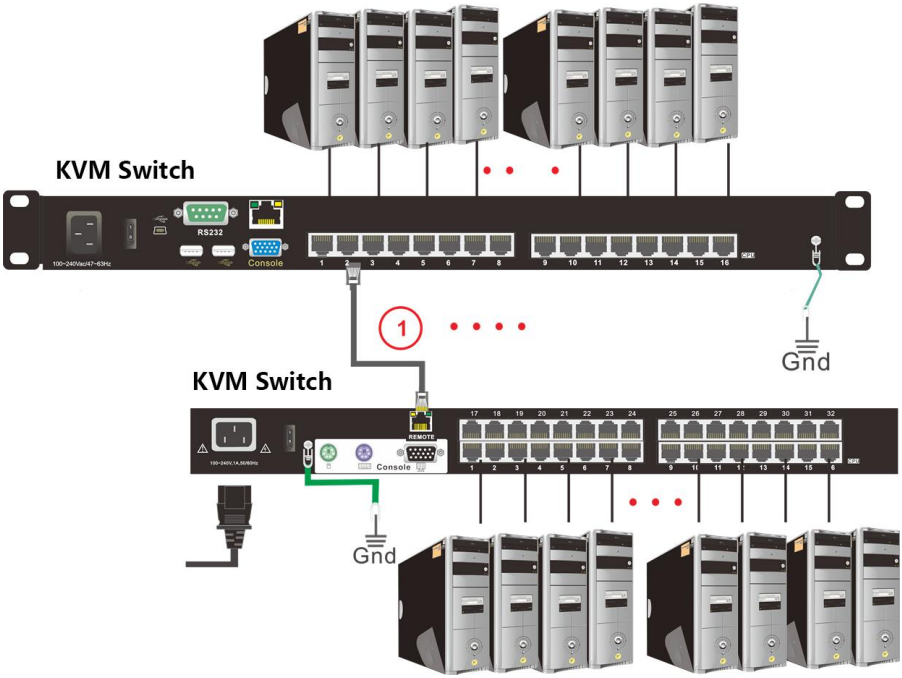


Diagram 2.4 Cascade installation

Explanation:

1. Connect one port of the CAT5 cable to any RJ45 port of the KVM, and connect the other port to the RJ45 port with “Chain in” of another KVM.
2. Repeat above operation to cascade more KVM switches.

   8 Port: max cascade 8 KVM Switch (256)

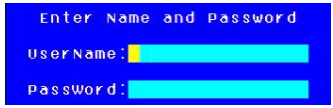
   16 Port: max cascade 16 KVM Switch (512)

   32 Port: max cascade 32 KVM Switch (1024)
3. Connect host computers according to 2–4.

2.8 Opening the console

1) The KVM makes two “beep” sounds after power on; an OSD window appears for you to input user name and password.

2) Below password window appears:



The default user name and pass word is blank, double click 【Enter】 to login and the OSD menu pops up, it’s ready to use the KVM switch.

2.9 LED OSD configuration

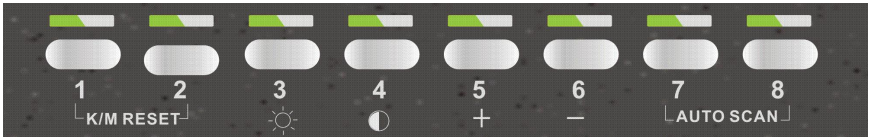
Diagram 2.5 KVM front views

Table 1.2

No.	Components	Function
1	Port selecting switch	Press LED buttons to select computer and the LED tube showing the selected port number
2	Port Selection Buttons& LEDs	Indicator LEDs are built into the switches, the online LED light is on the left and the selected LED light is on the right. 1) An online LED light(orange) indicates that the KVM has connected to its corresponding computer and power on.

		2) A selected LED light(green) indicates that the computer attached to its corresponding port is up and running.
3	Reset KVM	Reset KVM switch
4	Upgrading switch	Pull this switch to upgrade inner IC
5	Software upgrading	This upgrading can only be done by the supplier, it is not support customer upgrading
6	Power LED	It shows the KVM has been power on and ready
7	Station ID	It shows the current port, when cascade to next bank, it will show the bank number

Number key operation



1. Press 【1】and【2】 at the same time for three seconds resets the keyboard and mouse.
2. Press【7】 and【8】at the same time for three seconds enters the auto scan mode.
3. Press【3】 for three seconds enters brightness adjusting mode.
   - 33 are flashing on the LED tube.
   - Then press 【5】,【6】to adjust.
   - Press【3】exits or waits for five seconds and it will auto-exit.
4. Press 【4】 for three seconds enters definition adjusting mode.
   - 44 are flashing on the LED tube.

- Then press 【5】, 【6】 to adjust.
- Press 【4】 exits or waits for five seconds and it will auto-exit.

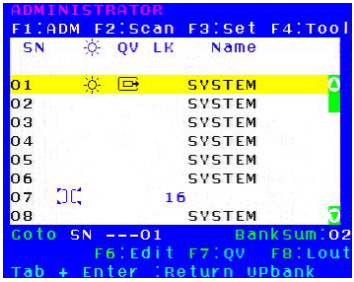
5. Press 【5】 enters port selecting mode.
   - 55 is flashing on the LED tube.
   - Exits after select a port or wait for five seconds and it will auto-exit.

6. Press 【6】 for three seconds will initialize the brightness and definition of each

3. OSD Operation

3.1 OSD Menu Operation

Double click the right button of the mouse or double click hotkey【Scroll Lock】 to invoke below OSD main menu. You can customize the OSD hotkeys; find more details in OSD function instructions.



Heading	Explanation
SN	Port numbers
	Chain in KVM
	On line
	System on
	Quick view
	BRC Port
	Channel is only be seen
Name	Port name

To access the OSD menu through keyboard:

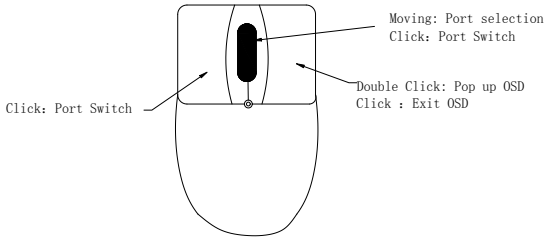
1.In the submenus that appears, moving the highlight bar to your selected port and then press Enter.

2.Press【Page Up】or【Page Down】quickly moves to next BANK

3. Press any key from 【0-9】to enter any port of current station

To access the OSD menu through mouse:

1. Use the scroll wheel to switch from one port to another.
2. Click the right or middle button to confirm your selected port and close the OSD main menu at the same time.
3. Click the right button to exit the OSD main menu.



*Note: Operate via keyboard after invoke the OSD menu via the touchpad.

3.2 OSD functions

Menu	Keys	Submenu/Explanation
ADM	F1	Set User login-Set User login account and password Set accessible-Set access permissions BRC Mode -monitor multiple computers at the same time Load Default-reset the menu to the original factory default settings
SCAN	F2	All-Lists all the ports on the installation Power On-lists only powered on ports that have attached computers. Quick View-Lists only the ports that have been selected as Quick View ports

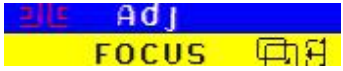
SET	F3	Auto Scan–set scanning time period Port ID–set how long a port displays on the monitor OSD Hotkey–set OSD hotkeys Lout Time off– to set the time out value
TOOL	F4	Reset RGB–Press Enter reset RGB Beeper【On】–press Enter switch Bee sounds Mouse Hot【On】–press Enter to close touchpad operating on OSD. Restore Values–press Enter restore the current user default value. About KVM– press Enter shows the KVM version
Edit	F6	Edits port names
QV	F7	Start or close Quick View
Lout	F8	Log out/lock the KVM
Exit	Esc	Press this key exits OSD menu
	Scroll Lock	Press this key exits OSD menu
	Num Lock	Press this key exits OSD menu

Table 1.5

The display screen will be distorted if the CAT5 cable is too long, for this case, you can adjust according to below steps:

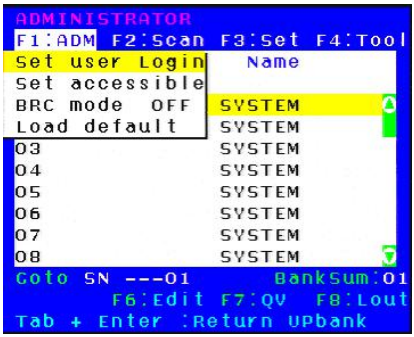
1. Press【+】 and ADJ FOCUS will pop up, then press【+】,【–】to adjust definition.

2. Press【,】and ADJ BRIGHT will pop up, then press【,】【.】to adjust brightness.



F1–ADM

- **Menu Overview**



Operating instructions

1) Press【F1】or 【←】【→】enters the F1 submenus.

2) Press 【↑】【↓】moves the highlight bar to select the submenu.

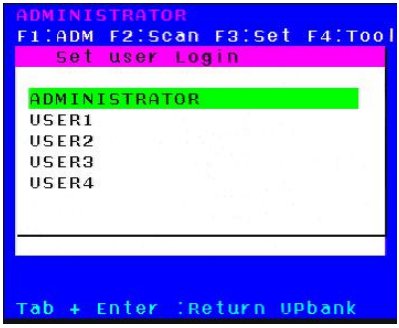
3) Press 【Enter】 selects and exits ADM menu.

4) Press【Esc】cancels the operation and exits ADM menu.

- **Menu Explanation**

1. Set User Login—Press【Enter】 selects Set User Login and a screen as below diagram 4–1.1 appears:

One administrator and four users account can be set (the account and the password are no more than 16 characters)



Enter

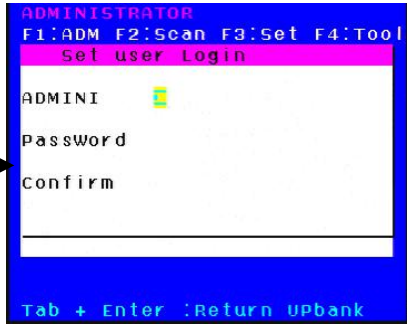


Diagram 4–1.1 Diagram 4–1.2

Note: You can set up an account and password according to diagram 4–1.2, then " User setup ok" pops up showing that you have done your set," and if "Password Not Match" pops up, you need to type in your password again as you did in your first type.

2. Set Accessible—press 【Enter】 to select Set Accessible, then below menu appears: (diagram 4-1.3)

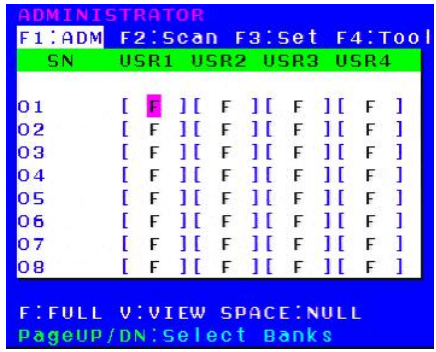
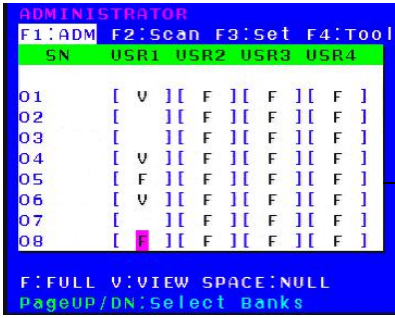


Diagram 4-1.3

Menu	Explanation
FULL	Full access function to the station and can do any operation to the ports
VIEW	Read only function, you can only read the port but you can't operate it if set this function.
NULL	If you set this function, the port will be not displayed on the user's OSD menu

Note: The administrator always has full access to all the ports.



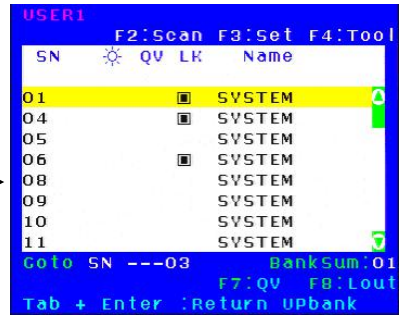


Diagram 4-1.4 Diagram 4-1.5

E.g.: 1) If you want to set access permission of [User1], press【Space】to select the permission options you need to set.

2) If you want to set access permission of cascade port, press【Page Down】moves to next level, and the SN changes into Bank — Port(e.g.: 02–01), then press【Space】to select the permission options you need to set.

3) [User1] log in OSD menu, below diagram 4–1.5.

3. BRC Mode Off – Press 【Enter】to enter the BRC mode, enter the main menu, press 【F7】 to add or delete a port that need broadcast function. When BRC mode is effect, a speaker symbol appears in QV column. (See below diagrams). While BRC mode is in effect, we can synchronous operate multiple computer ports.

Note: While BRC mode is in effect, the mouse is forbidden to use.

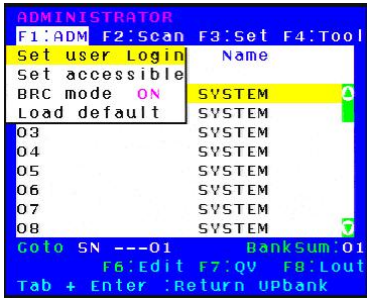


Diagram 4–1.6

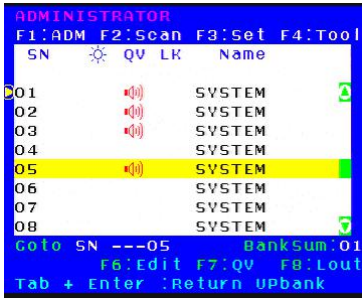


Diagram 4–1.7

1)Open BRC mode

【F1】–>BRC Mode OFF–> 【Enter】 –->BRC Mode ON (diagram 4–1.6)

2) Open the port that need broadcast function

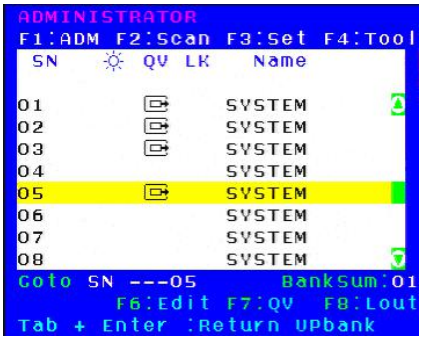
Press【↑】【↓】key—>select the port that need broadcast function → 【F7】 →a speaker symbol appears in the QV column which shows the port has entered broadcast mode.

3) Close the broadcasting port

press【↑】【↓】key—>select the port→ 【F7】→exit BRC mode and the speaker symbol disappears

4) Exit BRC mode

Invoke OSD main menu → 【F1】–>BRC Mode ON –> 【Enter】 ––> BRC Mode OFF, KVM exit BRC mode (diagram 4–1.8)



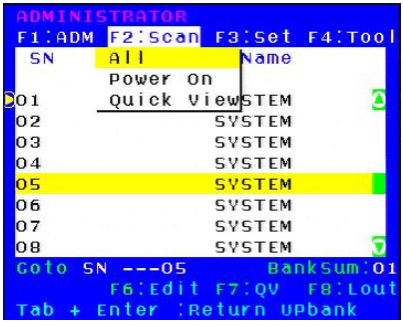
【F1】–>BRC Mode OFF –> 【Enter】 ,enter the main menu, all symbols turn

Diagram 4–1.8

4. Load Default––– press 【Enter】 to select the submenu, all the set values are restoring to original factory default settings.

F2–Scan

- Menu Overview



Operating instruction

1) Press【F2】or 【←】【→】enters the F2 submenus.

2) Press 【↑】【↓】moves the highlight bar to select the submenu.

3) Press 【Enter】 selects and exits Scan menu.

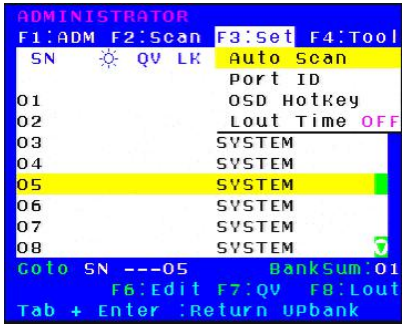
4) Press【Esc】cancels the operation

- **Menu Explanation**

Submenu	Explanation
All	Use this function to scan all ports according to the set scanning interval.
Power On	Use this function to scan all signal ports with according to the set scanning interval.
Quick View	Use this function to scan all ports with quick view symbols according to the set scanning interval.

F3-Set

- **Menu Overview**



Operating instructions

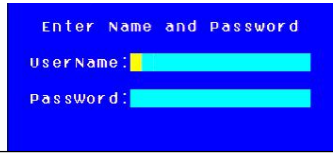
1) Press【F3】or 【←】【→】enters the F3 submenus.

2) Press 【↑】【↓】moves the highlight bar to select the submenu.

3) Press【Enter】selects and exits Set menu.

4) Press【Esc】cancels the operation

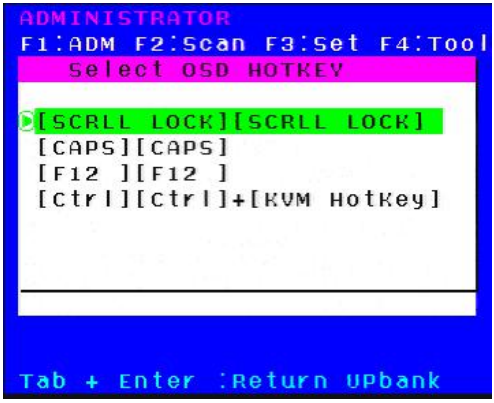
- **Menu Explanation**

Submenu	Default value
Auto Scan	5S（effective range 5–99）
Port ID	0S: not display the port ID 1–98S: display the seconds, maximum 98s 99S: permanent display
OSD Hotkey	【Scroll Lock 】+ 【Scroll Lock 】 【Caps Lock】 +【Caps Lock】 【F12】 +【F12】 【Ctrl】+ 【Ctrl】+ 【KVM Hotkey】
Lout Time off	0: off 01–99M:set the screen saver timeout, it is automatically log out if the current operator is no longer operate for a while, then the KVM will be locked and you need to enter user name and password to operate again 

OSD Hotkey Operation

Operating instruction

1. Press 【F3】and move the highlight bar with【↓】 to select "OSD Hotkey" submenu. Press 【Enter】and below screen appears:
2. KVM default hotkey:【Scroll Lock】



2.Select the" 【 Ctrl 】【 Ctrl 】 + 【 KVM Hotkey 】 " and press 【Enter】, and then the 【Ctrl】hotkey is available in this hotkey mode, the mouse hotkey can't enter the

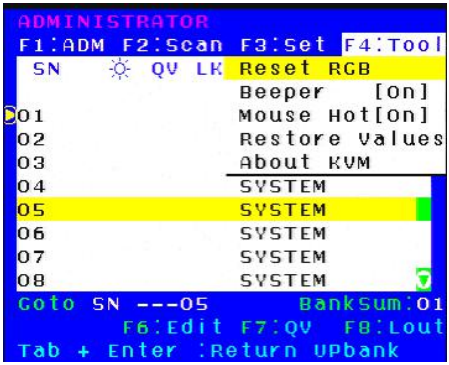
OSD menu

Invoke hotkey: double click 【L_Ctrl】 + the corresponding function key

Function	Operating	Function description
Switching port	+2 number keys	Eg.: switch to port 4 by hotkeys 【L_Ctrl】+【L_Ctrl】+【0】+【4】
	+ F1~ F8	Skip ports from 1–8
Invoke OSD main menu	+ "space "	This allows you to invoke OSD main menu (see OSD menu operation)

F4–Tool

- **Menu Overview**



Operating instructions

1) Press【F4】or 【←】【→】enters the F4 submenus.

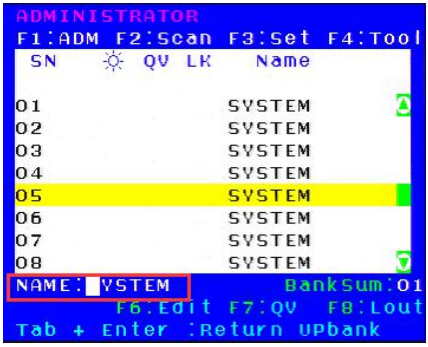
2) Press 【↑】【 ↓】moves the highlight bar to select the submenu.

3) Press【Enter】 selects and exits Tool menu.

- **Menu Explanation**

Submenu	Instruction
Reset RGB	Restore the video signal to the default value.
Beeper【On】	The beeper can be turned on or off with this function.
Mouse Hot【On】	To open and close the mouse with this function. We can't operate the OSD when it is【Off】.
Restore Values	Restore to original factory default values.
About KVM	It shows the KVM version information.

F6–Edit port names

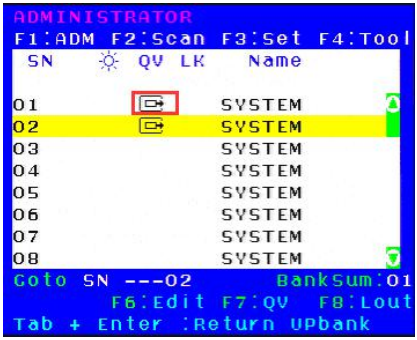


- Select the port with【↑】【↓】 key;
- Press F6 and key in the new name or modify the old one, then press Enter to save the name and exit editing.
- Press 【Esc】to cancel and exit the editing.

Note:

The NAME characters include:

F7–Set Quick View port



- Select ports with【↑】【↓】keys;
- Press【F7】to include current port as Quick View, then an arrowhead appears in the QV column to indicate so;

Note:

Press 【F7】 to cancel the QV symbol if the current port has already have a QV arrowhead symbol in its QV column; if you want to cancel all the QV function, press Restore Values under F4:Tool.(The port name restores to default setting at the same time.)

【default value】All the ports exit QV.

F8–LOUT

- Press【F8】exits the OSD main menu and fully exits current port, then the log in window appears:

- Users must log in all over again to regain access to the OSD.

3.3 Cascade Function

1. Operate the host computer under cascade

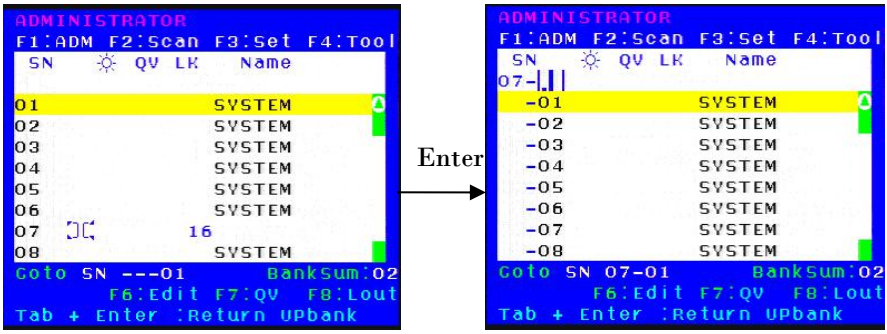


Diagram 4–1.5 Diagram 4–1.6

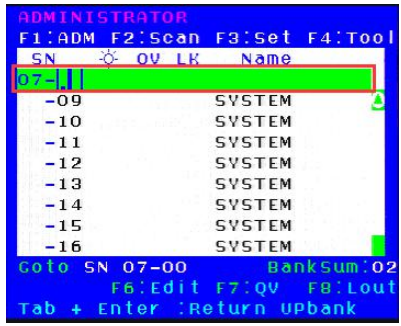
Explanation:

Shows that we have already connected an 8 port KVM to port 2(see diagram 4–1.5), we can connect 8 computers to the 8 port KVM. Press【 Pa UP】to select port on current station, then press 【Enter】to operate the port.

Enter

2. Return to OSD main menu

Tab



OSD Menu

Note:

1. Press【Tab】, then 02 — in column SN changes into green, which indicates the port has been selected. Then press【Enter】to return to main menu to operate other ports.
2. Press【Pa DN】returns to the OSD main menu.

4.IP Settings

4.1 Initial IP Configuration via Network

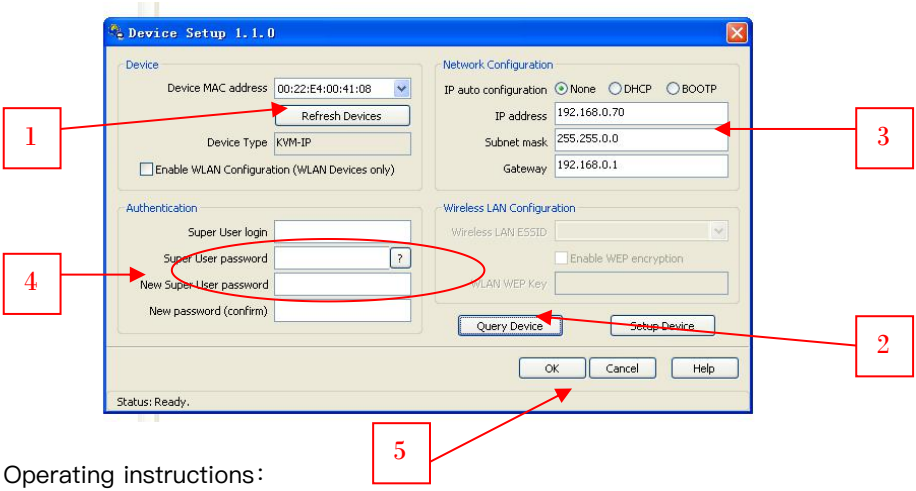
IP – KVM factory default settings:

DHCP	forbidden
Default IP address	192.168.0.70
Default Subnet mask	255.255.255.0

1) Read the CD and double click JAVA, ensure the Internet is available and install the JAVA step by step according to indications.

2) Copy the PSETUP to the computer in use and double click PSETUP.

3) Below menu appears on the screen:



Operating instructions:

1) It automatically gets the MAC address, if it is failed to do so, press the Refresh Devices according to above number 1.

2) Click Query Device (above number 2), it shows the IP KVM's IP address as well as gateway information (see above number 3).

3) Choose None in IP auto configuration, set up the IP address in above number 3 according to your network area (eg.192.168.X.XXX) .Input your account and password after setting the network path (above number 4).

User Login: super

Password: pass

Click OK to save your settings.

4) If you choose DHCP in IP auto configuration, there is no need to modify the IP address, it will automatically get the proper IP address.

★~Please remember the setting IP address for remote control~★

4.2 Configuration Setup via Serial Console

For using serial terminal, the KVM-over-IP has a serial line interface (host side). This connector is compliant with the RS-232 serial line standard. The serial line 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 with a serial terminal, e.g., Hyper Terminal, reset the KVM-over-IP and immediately press the "ESC" key. You will see some device information, and a "=>" prompt. Enter "config", press "Enter" key and wait for a few seconds for the configuration questions to appear.

As you proceed, the following questions will appear on the screen. To accept the default values shown in square brackets below, press "Enter" key.

IP auto configuration None/DHCP / BOOTP) :

IP address[192.168.0.70]:

Subnet mask[255.255.255.0]:

Gateway (0.0.0.0 for none) [0.0.0.0]:

IP auto configuration

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

IP address

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

Net mask

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

Gateway address

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

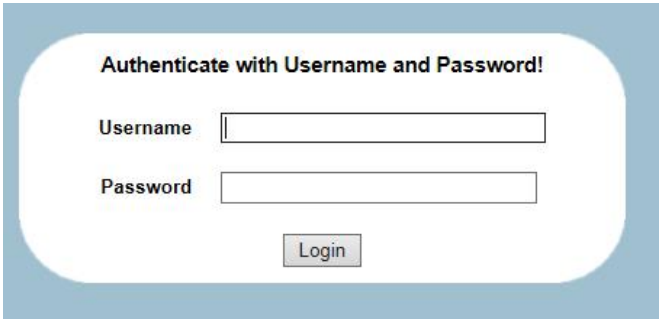
Warning:

User "super" is forbidden to log in via the serial port of the IP-KVM.

5.Log in

1) Open IE and type in the IP address you have set in PSETUP (as shown above number 1).

http:// 192.168.0.70(the IP address you have set according to your network area)



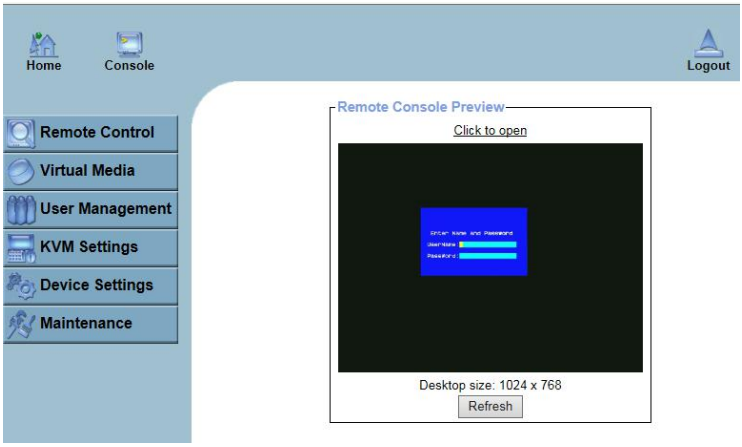
2) A screen appears as shown in above to indicate you to type your account and password after connected.

User name: super

Password: pass

3) Then below screen appears:

Click Console to open the IP-KVM remote console.



Warning:

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

5.1 Remote Console

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

- Main window of the remote console

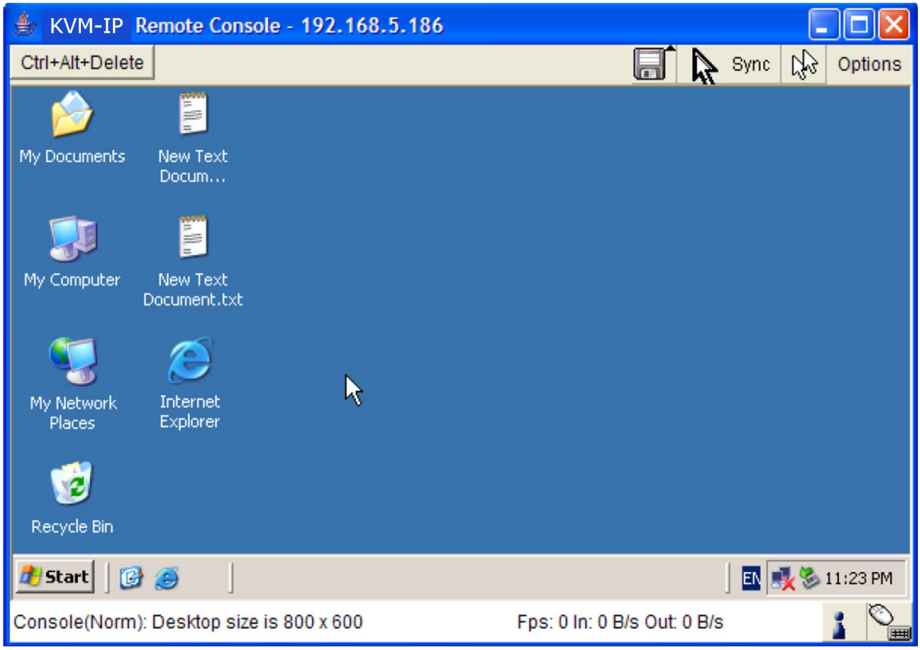


Diagram 6-1 Main window of the remote console

Warning:

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

- Control Bar of Remote Console

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

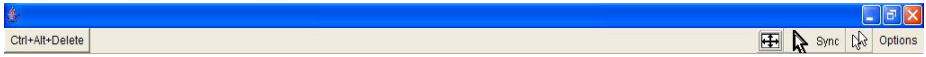


Diagram 6-2 Control bar of remote console

Ctrl+Alt+Delete 

Special button key to send the "Control Alt Delete" key combination to the remote system.

Auto Adjust button 

If the video display is of bad quality or distorted in some way, press this button and wait a few seconds while the KVM-over-IP tries to detect the video mode of VGA port to the controlled host and adjust itself for the best possible video quality.

Sync mouse 

Activates the mouse synchronization process. Choose this option in order to synchronize the local with the remote mouse cursor. This is especially necessary when using accelerated mouse settings on the host system. In general, there is no need to change mouse settings on the host.

Single/Double mouse mode 

Switches between the Single Mouse Mode (where only the remote mouse pointer is visible) and the Double Mouse Mode (where remote and local mouse pointers are visible and need to be synchronized). Single mouse mode is only available if using SUN JVM 1.4.2 or higher.

Options 

To open the Options menu, click on the button "Options".

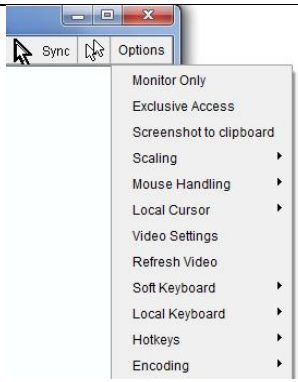


Diagram 6-3 Remote console options menu

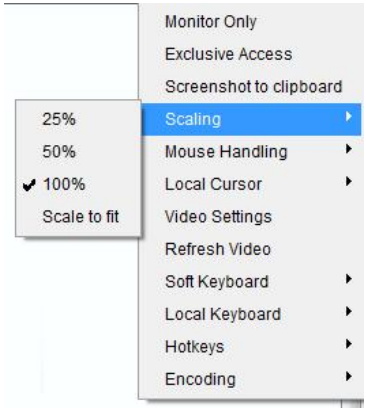


Diagram 6-4 Remote Console Options Menu: Scaling

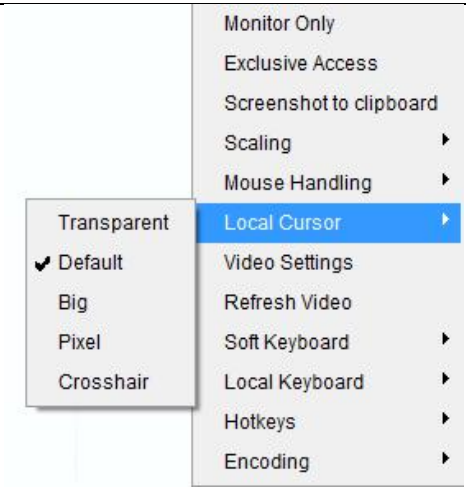


Diagram 6-5 Remote Console Options Menu:Cursor

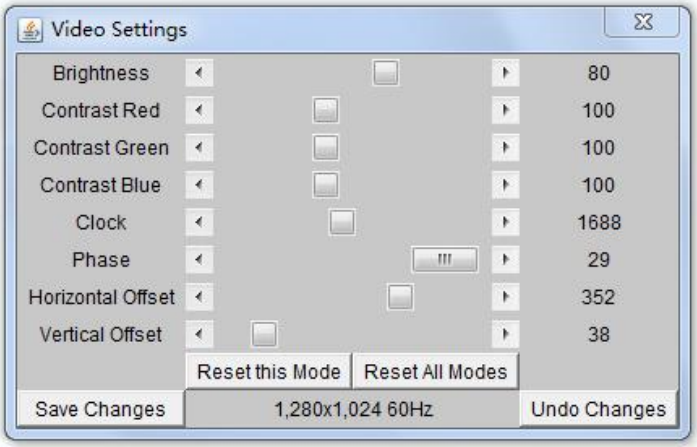


Diagram 6-6 Video Settings panel

Diagram 6-7 soft keyboard

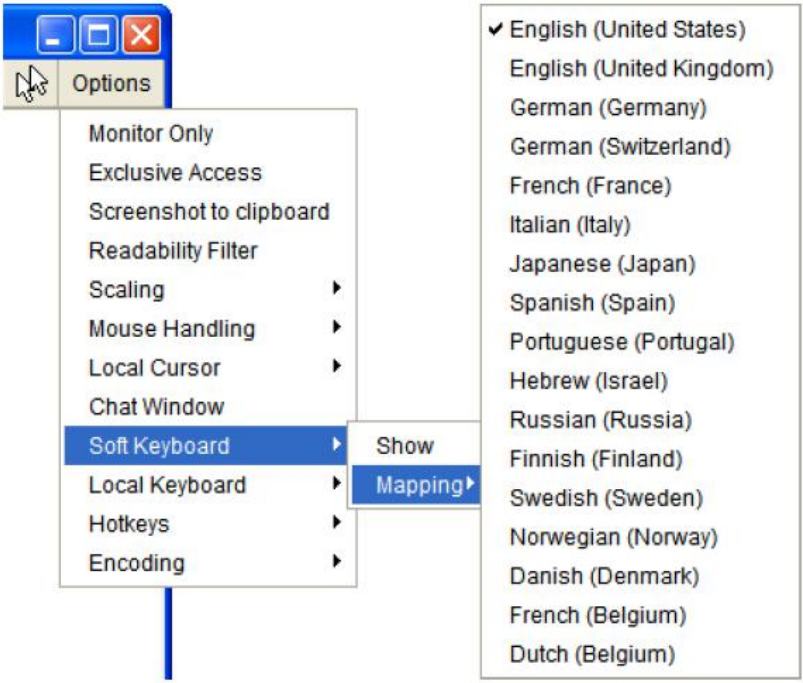


Diagram 6-8 Soft Keyboard Mapping

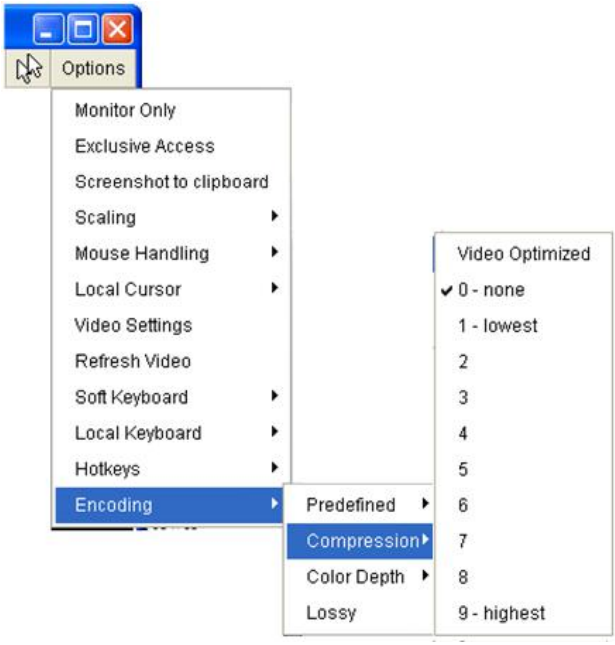


Diagram 6-9 Encoding Compression

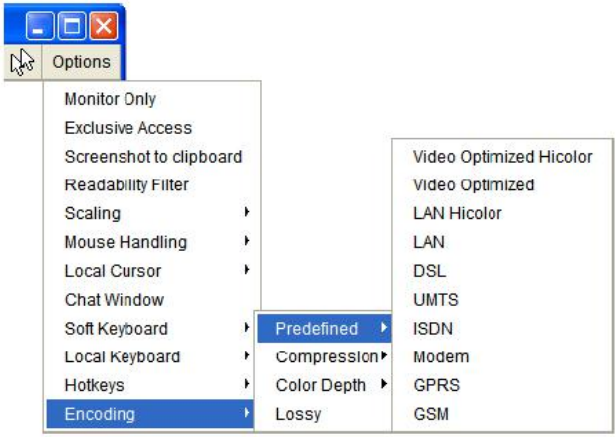


Diagram 6-10 Predefined Compression

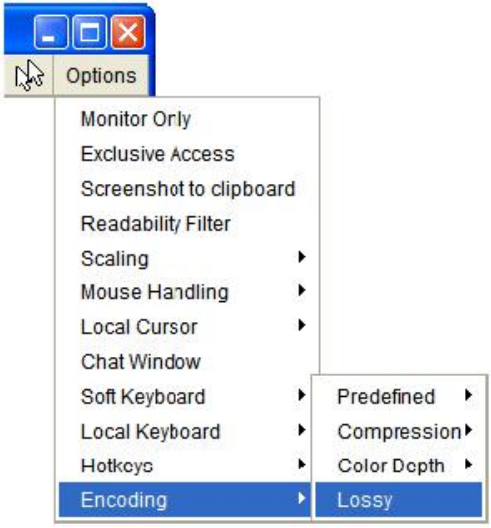


Diagram 6-11 Lossy Compression

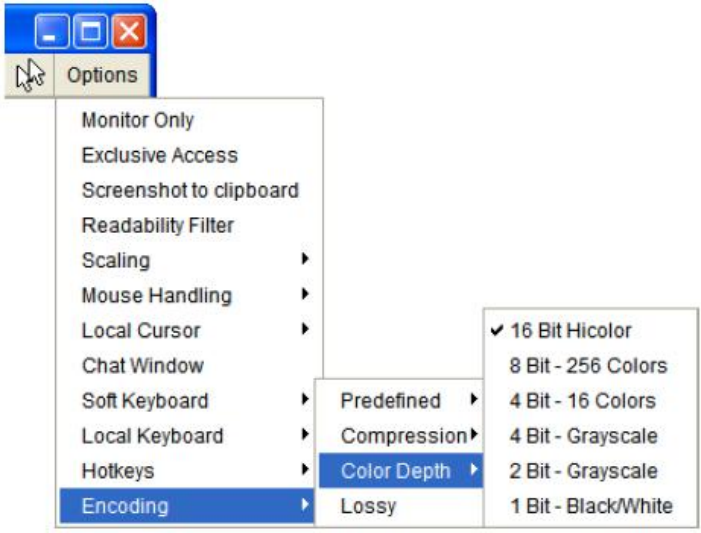


Diagram 6-12 Encoding Color depth

- **Remote status console**

Diagram 6-13 Status Line

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

Diagram 6-14 transmission rates

Press Alt+F12 exits the remote console.

6.IP Menu

6.1 Remote console

KVM console

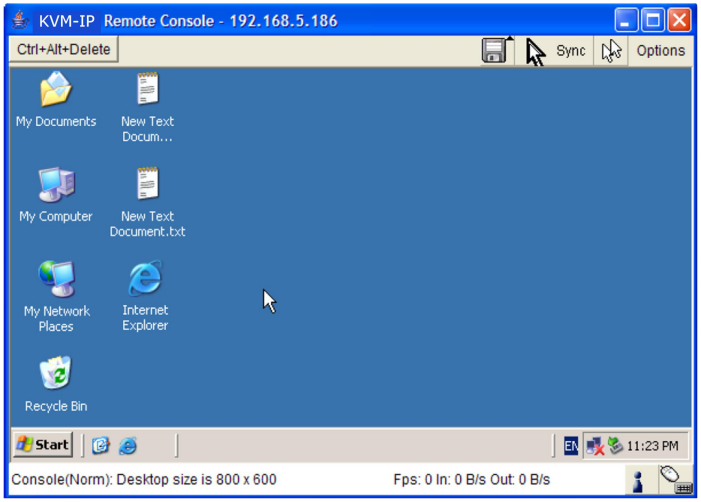


Diagram 7-1

Telnet Control

Diagram 7-2 Telnet console

The KVM-over-IP 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 KVM-over-IP host machine is using a text mode screen resolution.

Log in the Telnet console by the telnet command as required by the Telnet client, for instance in a UNIX shell:

telnet 192.168.0.70

Then the system will prompt for inputting a user name and password to log in the device. You need to input right credentials so that the Telnet management is fully conform to function controls in Web.

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

Telnet port supports two operating modes: command mode and terminal mode.Command mode is used for control or display some parameters.The terminal port mode is activated through access to serial port 1(if the serial port has set corresponding configuration), all the inputs will be redirected to serial port 1.

The following lists the command syntax and its application according to command mode:

Help: Display the list of possible commands

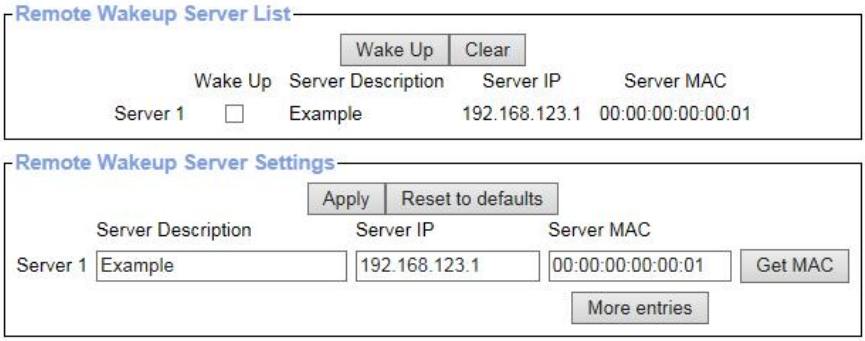
Cls: Clear the screen

Quit: Exits the current dialog box and disconnect from the user port.

Version: Shows the version information

Terminal: Activates the DMO of serial port 1.Press ESC exits the switch and return to command mode.

Remote Wake-up



The 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.

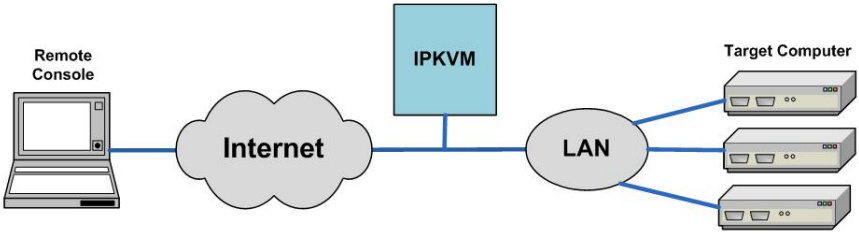


Diagram 7-3 Remote Wake up

Set up the computer you need to remotely wake up:

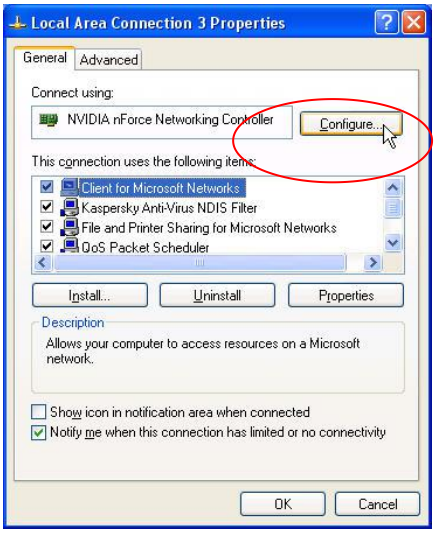
1. BIOS setting:

Enable the wake on settings in BIOS; make sure the Wake on Magic packet setting option is **Enable.**

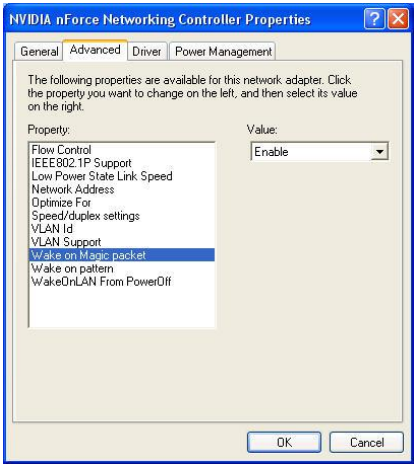
Note: Different BIOS version has different Wake on settings names,such as **Wake On LAN/PME、PME Event Wake Up or Power On By PCI Device.**

2. Windows setting:

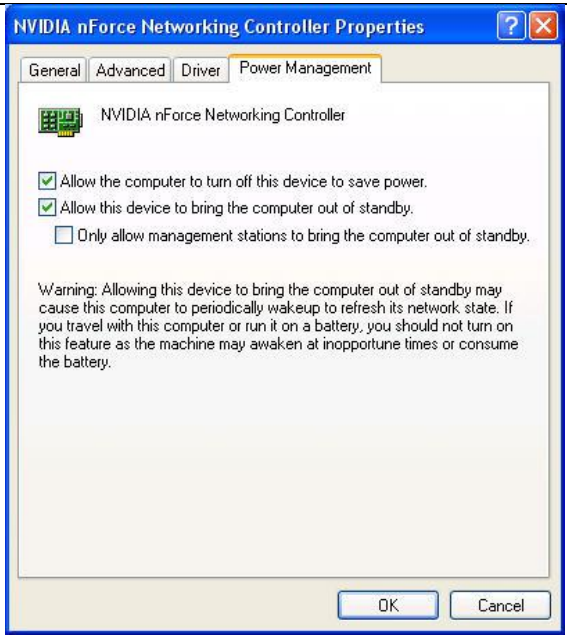
Enable 「Local connection attribute」 window



Make sure Wake on Magic packet is Enable.



Make sure the following two items are selected.

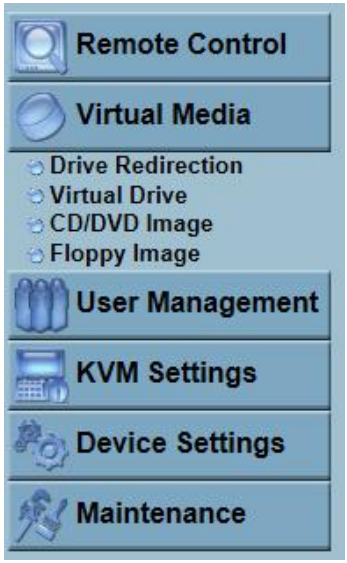


Settings on IP-KVM:

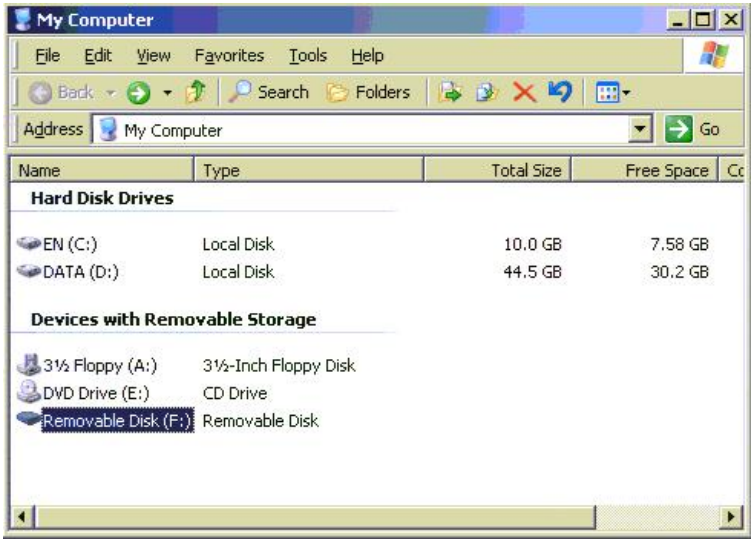
The control can be easily set up from the web page.

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

6.2 Virtual Media



Below is the host computer screen (the computer which connected with IP KVM)



Floppy Image

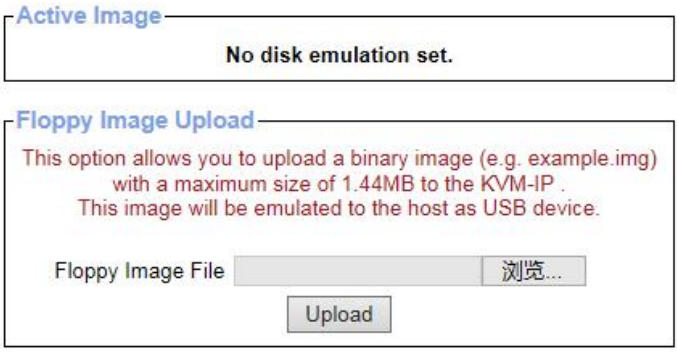


Diagram 7-4 virtual media-floppy disk

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:

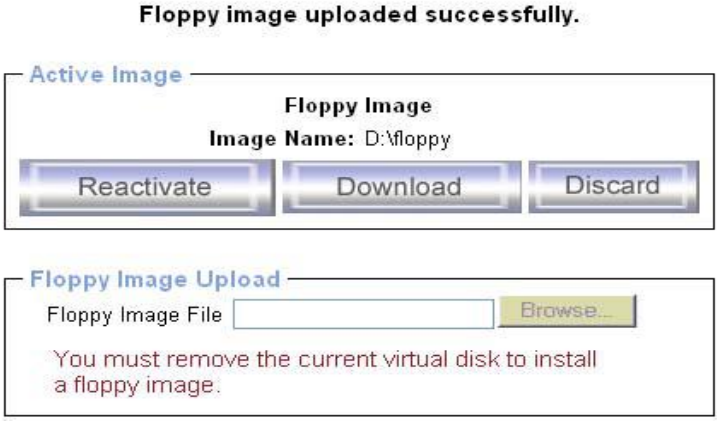
1. You need to create the floppy image file first (Please refer to the section "Creating a floppy image"). For this example, we use RawWrite software (or any other image-creator software) to create floppy image. Please use licensed software for this purpose.

2. You can find an image file saved at desire destination after you created it with RawWrite.

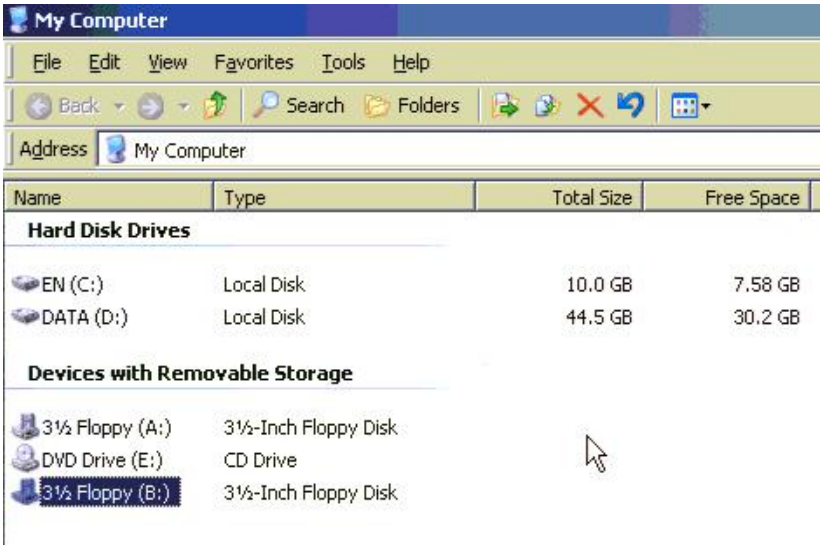
3. Open the browser to log into the IP-KVM. Click **Virtual Media**, and then **Floppy Disk.** Click the Browse button to choose the image file.

Click on the button **Upload** to initiate the transfer of the chosen image file into the IP-KVM module's on-board memory.

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



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



You may create a floppy image size up to 1.44Mb. This drive would be in read-only mode and would not allow you to write any information on this drive but copying only. This drive would be bootable under DOS mode if the motherboard/BIOS on the host computer supporting USB BOOTABLE function.

Notes:

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

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.

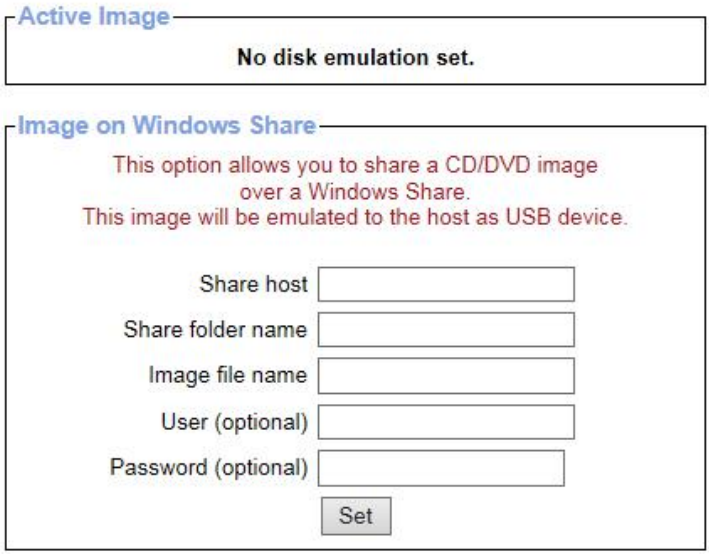


Diagram 7-5 Virtual Media – CD-ROM Image

Share host

The server name or its IP address (the PC that shares out the image file). On Windows 95, 98 and Windows ME do not specify the IP address but the server name ("NetBIOS Name").

Share folder name

The name of the share to be used.

Image file name

The image file name on the share folder.

User (optional)

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

Password (optional)

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

Notes:

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

Operation 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 **in 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

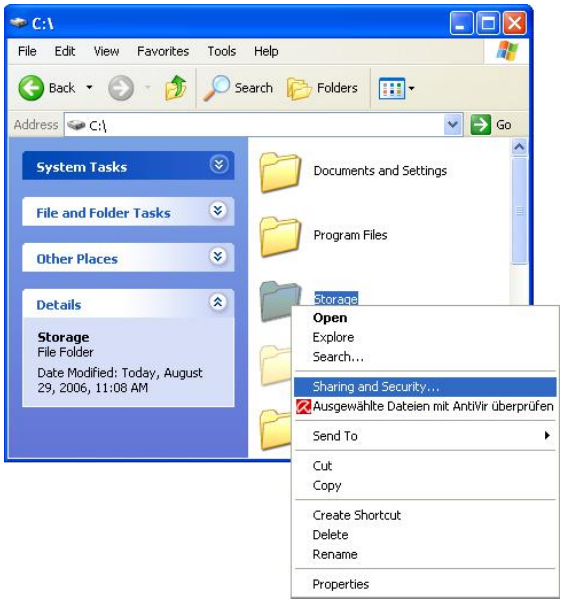


Diagram 7-6 Explorer Context Menu

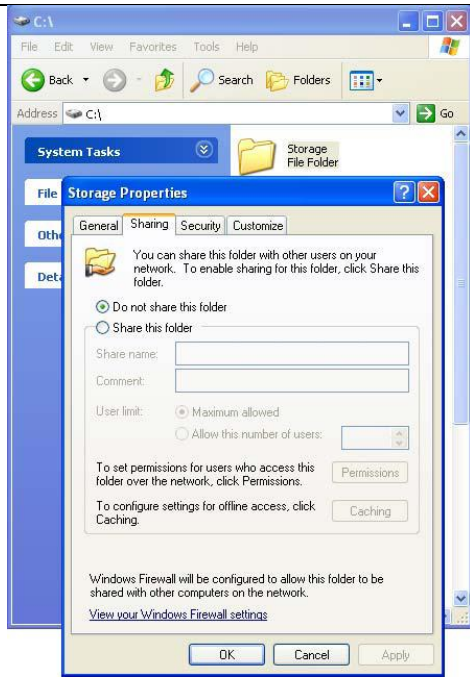


Diagram 7-7 sharing configuration dialog

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, and Linux)

If you like to access the share via SAMBA, SAMBA has to be set up properly. You may either edit the SAMBA configuration file /etc/samba/smb.conf or use

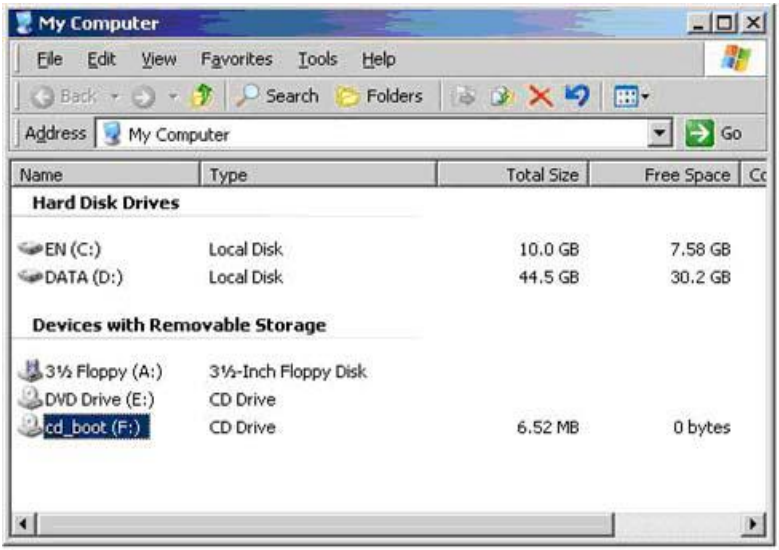
the Samba Web Administration Tool (SWAT) or WebMin to set the correct parameters.

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

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

2. If the Image file set successfully.

3. Open the remote console and you can see the virtual CD as below picture.



Creating an Image

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.

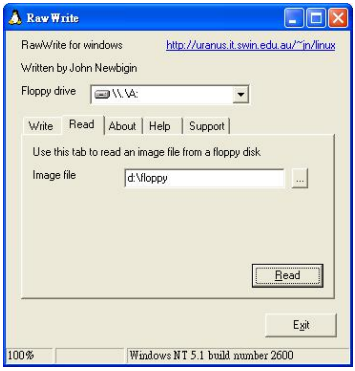


Diagram 7-8 RawWrite for Windows selection dialog

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

UNIX and UNIX-like OS

To create an image file, make use of “dd”. This is one of the original UNIX utilities and is included in every UNIX-like OS (UNIX, Sun Solaris, and Linux). To create a floppy image file, copy the contents of a floppy to a file. You can use the following command:

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

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

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

Diagram 7-9 Nero selection dialog

UNIX and UNIX-like OS

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

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

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

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

Drive Redirection

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

Diagram 7-10 Options of Drive Redirection

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

drive cache of the operating system of the remote host might contain older data. This
may confuse the remote host's operating system. We recommend using the Drive Redirection with care, especially the write support.

Disable Drive Redirection

To disable the function of Drive Redirection.

Force read-only connections

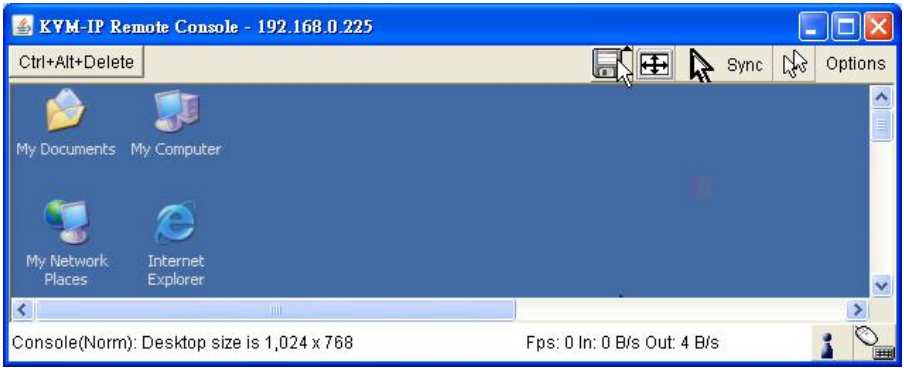
If enabled the Write Support for the Drive Redirection is switched off. It is not possible to write on a redirected device.

Click **Apply** to submit your changes.

Making a Drive Redirection

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

1. Run **Remote Control > KVM Console**.
2. Click on the "Floppy" icon 



You will see the Driver Redirection window as below.

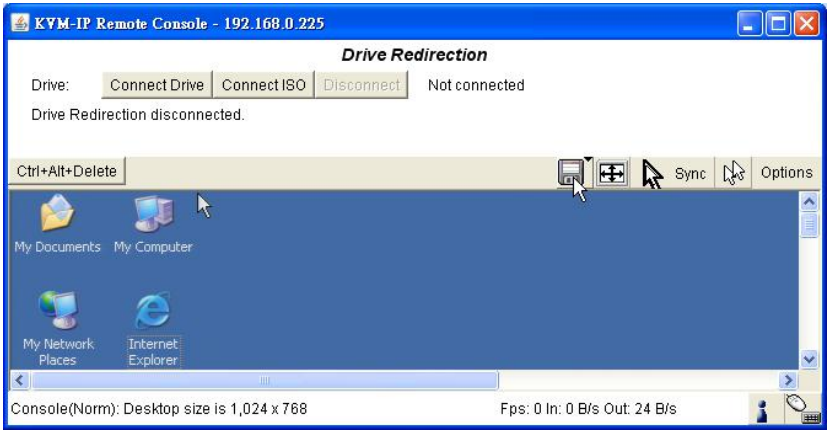
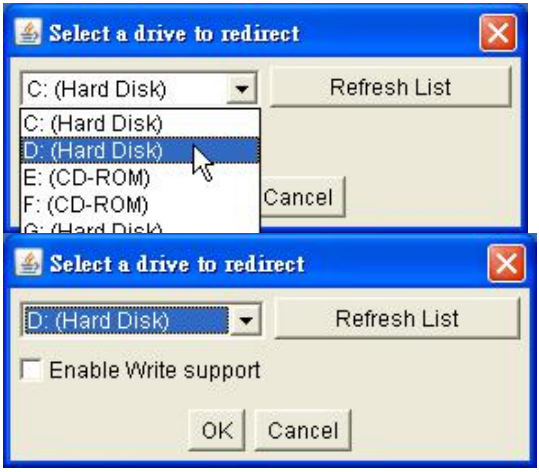


Diagram 7-11 Built-in Java Drive Redirection

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

3-1 If click on **Connect Drive**



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

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

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 only when you exactly know what you are doing.

Device Authentication

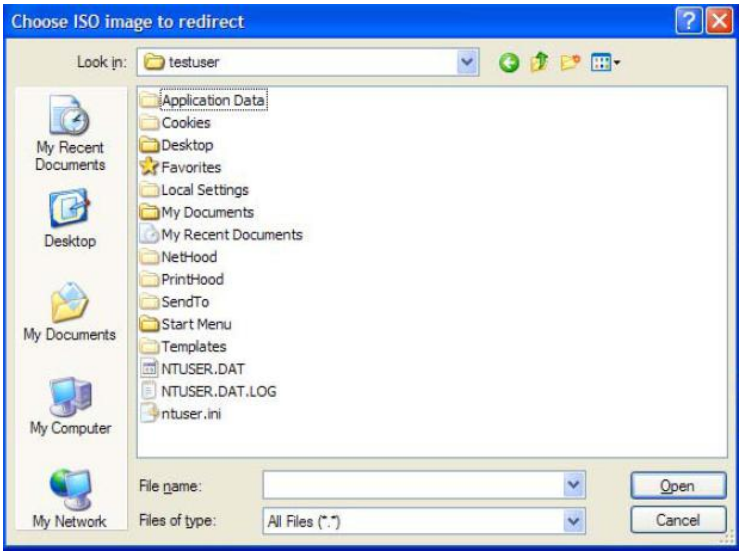
The factory default Username is "super" and the default Password is "pass".

Click **Connect** to redirect drive

Warning

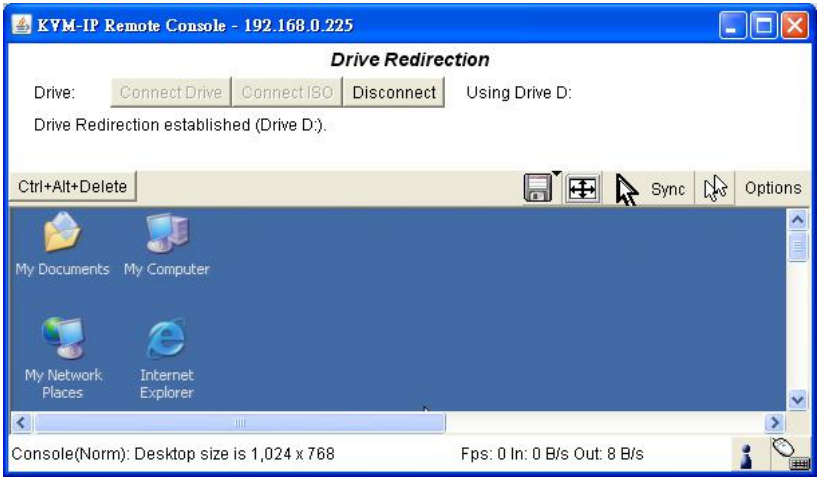
1. Drive Redirection is only possible with Windows 2000 or later versions.
2. The Drive Redirection works on a low SCSI level and the SCSI protocol cannot recognize partitions; therefore the whole drive selected will be shared instead of any particular partition.
3. While connecting to a legacy KVM switch, please select PS/2 mouse for **Keyboard/Mouse setting** from webpage. Otherwise you will not be able to use Hot-key.

3-2. If click on **Connect ISO**

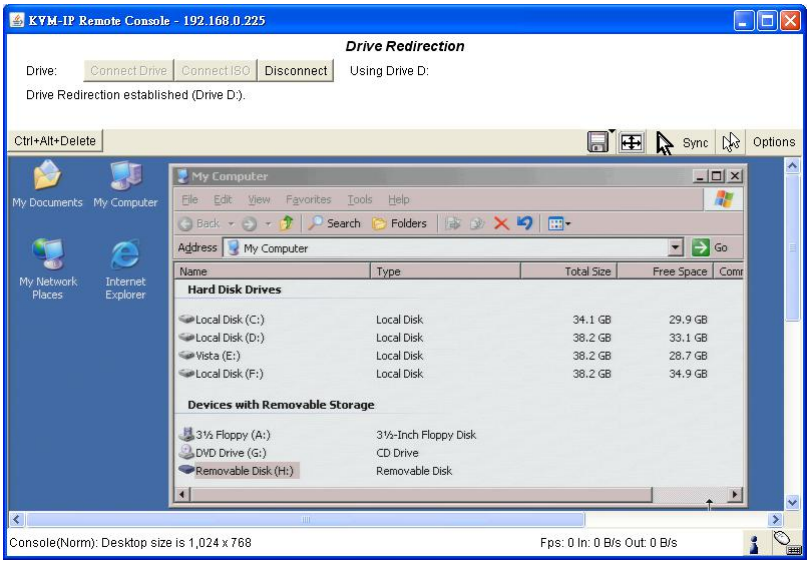


Select the ISO image file and click **Open**.

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

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

Please note that Virtual Drive creation is by Device manner not by Partition. Which means it looks for I/O in BIOS and sends the corresponding signal to host computer. This way, you are sending the entire hard drive (may consist of

'X' numbers of partitions) and emulate whatever number of partitions on host computer. You may also emulate a DVD-Drive with the same procedure. However, this DVD-Drive **Does NOT** support Bootable function like Floppy and CD-ROM emulation.

Virtual Drive

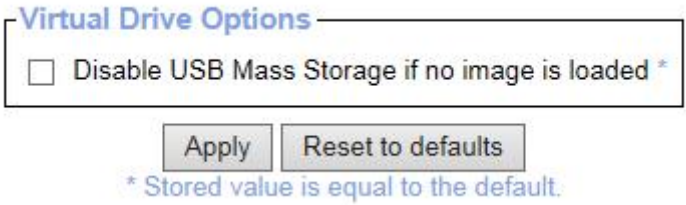


Diagram 7-12 USB mass storage option

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

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

6.3 User Management

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

Change Password

Diagram 7-13 Setting Passwords

Change password of currently logged in user:

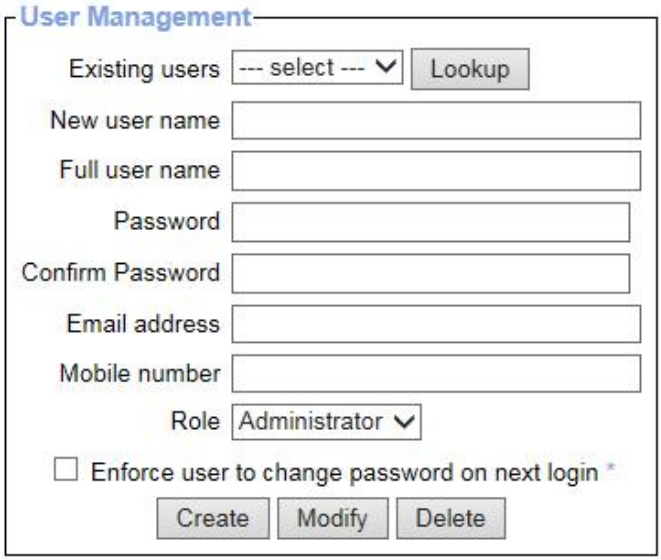
Old Password: type in current password

New Password: type in new password

Confirm New Password: re-type new password for verification

Click “Apply” to submit your changes.

sers and Groups



There are three kinds of levels of user accounts:

- **Super**-- Has all possible rights to configure the device
- **Administrator** -- Has partial rights to change configuration apart from critical settings
- **User** -- Has permission to access basic function of open Remote Console

You can choose the desired level from the selection box **role**.

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

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

Existing users

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

New User name

The new user name for the selected account.

Password

The password for the login name. It must be at least three characters long.

Confirm password

Confirmation of the password above.

Email address

This is optional.

Mobile number

This information may be optionally provided.

Role

Each user can be a member of a group (named a “role”) — there kinds can be shose from: super, administrator, or an regular user.

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

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

6.4 KVM Settings

User Console

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

Remote Console Settings for User

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

super | Update

Transmission Encoding

- ○ Automatic Detection *
- ◉ Pre-configured
  - Network speed: LAN (high color) *
- ○ Manually
  - Compression: 0 - none *
  - Color depth: 16 bit - high col *

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) Alt+F12 *

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	confirm Ctrl+Alt+Delete *	*

More entries

Apply | Reset to defaults

* Stored value is equal to the default.

Diagram 7-14 User Console Setting

Transmission Encoding

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

Automatic detection

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

Pre-configured

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

Manually

Allows to adjust both compression rate and the colour depth individually. Depending on the selected compression rate the data stream between the IP-KVM and the Remote Console will be compressed in order to save bandwidth. Since high compression rates consum more computing power of IP-KVM, they should not be used while several users are accessing the IP-KVM simultaneously. The standard color depth is 16 Bit (65536 colors). The other color depths are intended for slower network connections in order to allow a faster transmission of data. Therefore compression level 0 (no compression) uses only 16 Bit color depth. At lower bandwidths only 4 Bit (16 colors) and 2 Bit (4 gray scales) are recommended for typical desktop interfaces. Photo-like pictures have best results with 4 Bit (16 gray scales). 1 Bit color depth (black/white) should only be used for extremely slow network connections.

Remote Console Type

Specifies, which Remote Console Viewer to use.

Default Java-VM

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

Sun Microsystems Java Browser Plugin

Instructs the web browser of your administration system to use the JVM of Sun Microsystems. The JVM in the browser is used to run the code for the Remote Console window, which is actually a Java Applet. If you check this box for the first time on your administration system and the appropriate Java plug-in is not already installed on your system, it will be downloaded and installed automatically. However, in order to make the installation possible, you still need to answer the according dialogs with "yes". The download volume is around 11 Mbytes. The advantage of downloading Sun's JVM lays in providing a stable and identical Java Virtual Machine across different platforms. The Remote Console software is optimized for this JVM versions and offers wider range of functionality when run in SUN's JVM. Please make sure that you are installing Sun JVM v1.5 or above to your client system.

Miscellaneous Remote Console Settings

Start in Monitor Mode

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

Start in Exclusive Access Mode

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

Mouse hotkey

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

Remote Console Button Keys

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

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

"confirm" requests confirmation by a dialog box before the key strokes will be sent to the remote host.

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

Keyboard/Mouse

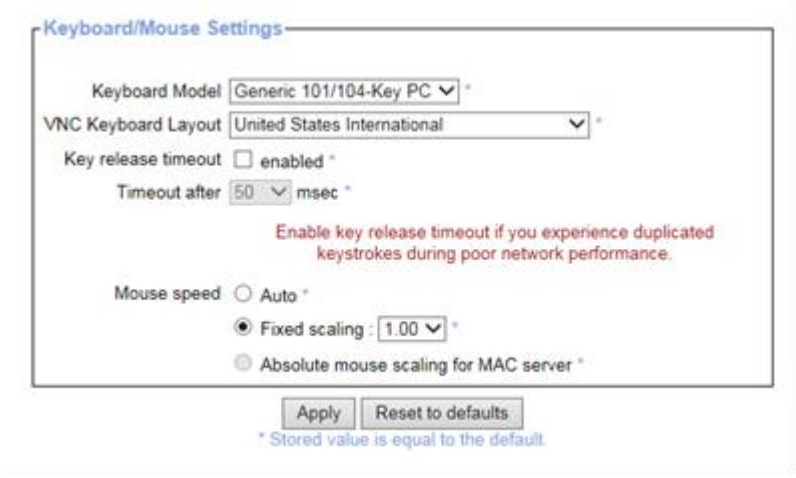


Diagram 7-15 Keyboard and Mouse Settings

PS/2 Keyboard Model

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

Keyboard timeout

Recommanded as "enable" for keyboard timeout when host is UNIX or UNIX-like OS.

Mouse Speed

•Auto mouse speed

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

•Fixed mouse speed

Use a direct translation of mouse movements between the local and the remote pointer.

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

•Absolute mouse scaling for MAC server

Use this option for MAC server.

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

Video

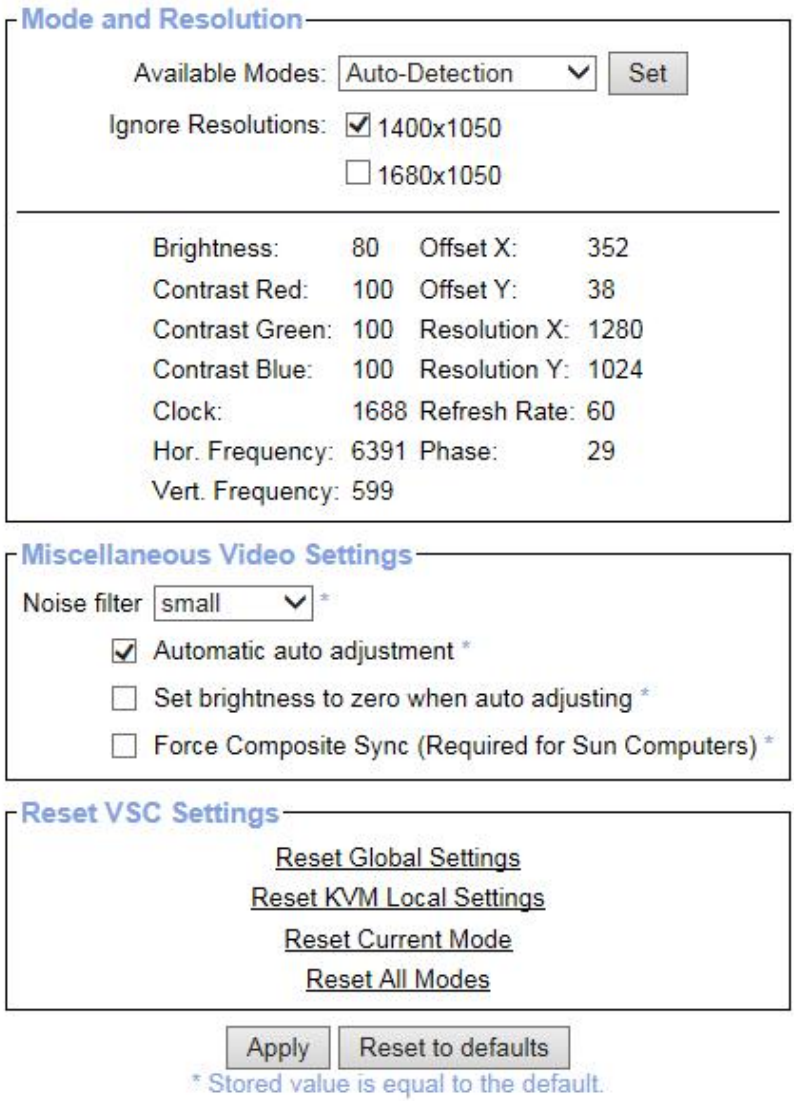


Diagram 7-16 Video Settings

Miscellaneous Video Settings

•Noise filter

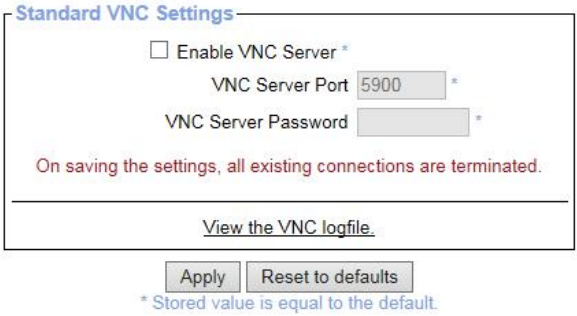
This option defines how the IP-KVM reacts to small changes in the video input signal. Turning on the noise filter can help reduce video flickering that is often caused by distortions, as well as lowering unnecessary bandwidth consumption. A large filter setting needs less network traffic and leads to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

•Force Composite Sync (Required for Sun Computers)

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

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

VNC



6.5 Device Settings

Network

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

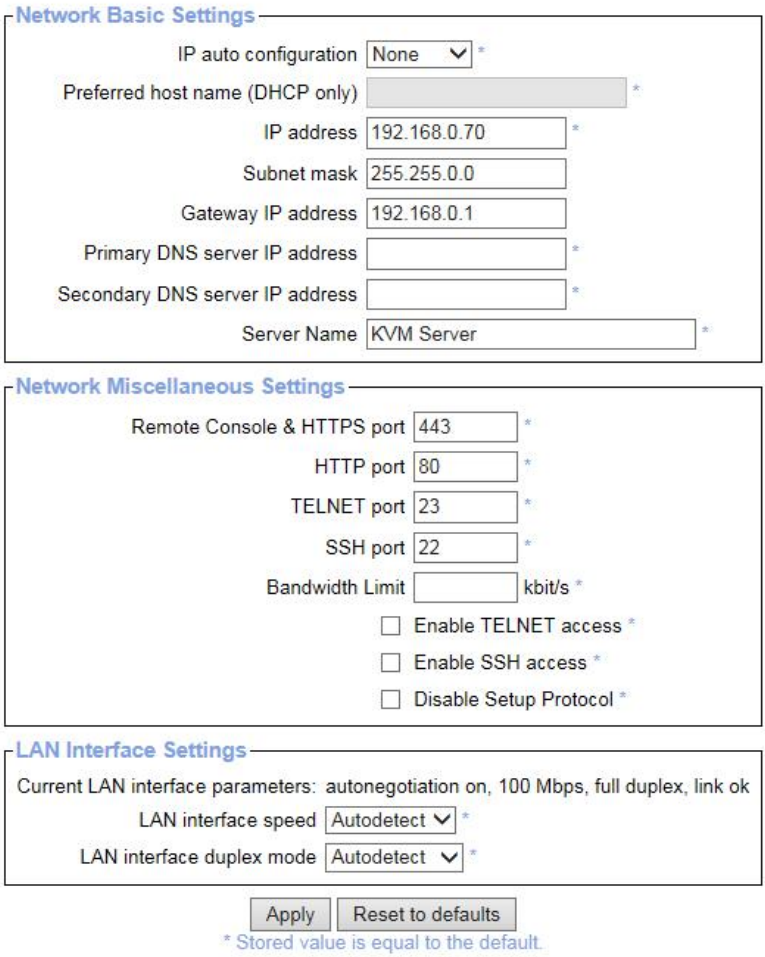


Diagram 7-17 Network Settings

Warning

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

Dynamic DNS

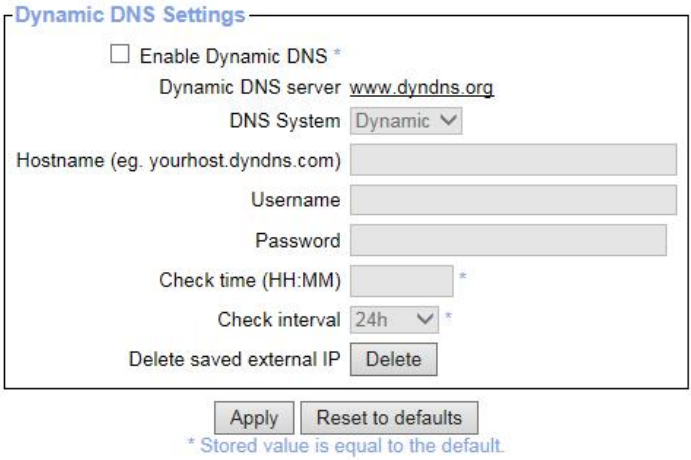


Diagram 7-18 Dynamic DNS

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

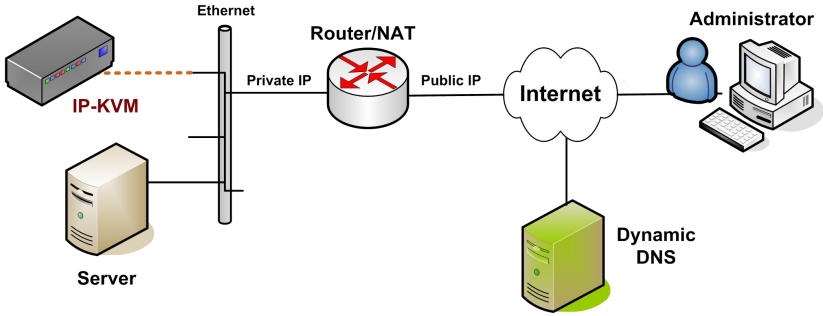


Diagram 7-19 Dynamic DNS Scenario

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

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

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

•Make sure that the LAN interface of the IP-KVM is properly configured.

•Enter the Dynamic DNS Settings configuration dialog as shown in Figure.

•Enable Dynamic DNS and change the settings according to your needs (see below).

Enable Dynamic DNS

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

Dynamic DNS server

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

DNS System

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

Hostname

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

Username

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

Password

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

Check time

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

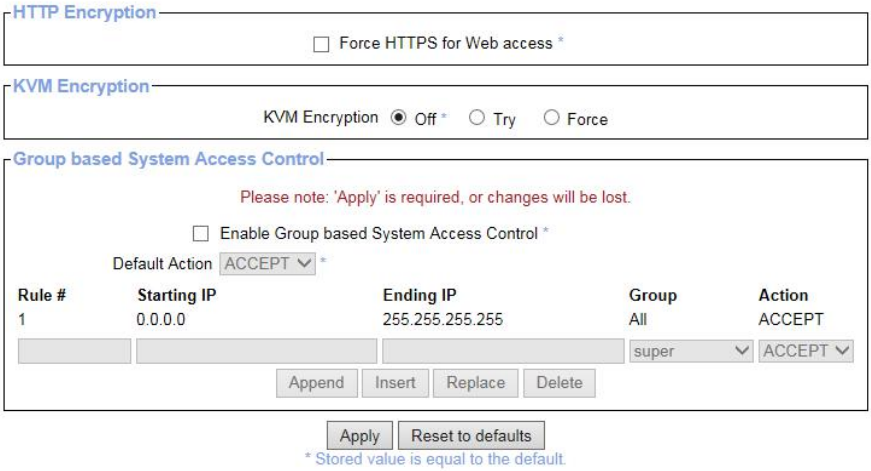
Check interval

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

Warning

The IP-KVM has its own independent real time clock. Make sure the time setting of the IP-KVM is correct. (See the Section *Date and Time*)

Security



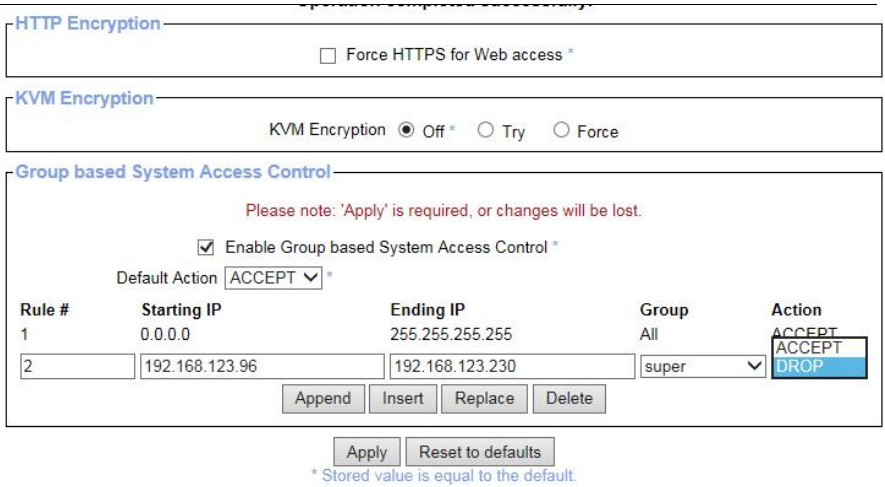


Diagram 7-22 IP Filter Settings

Certificate

Diagram 7-23 Certificate Settings

The IP-KVM uses the Secure Socket Layer (SSL) protocol for any encrypted network traffic between itself and a connected client. During the connection establishment the IP-KVM has to expose its identity to a client using a cryptographic certificate. The default certificate comes with IP-KVM device upon delivery is for testing purpose only. System administrator should not rely on this default certificate as the secured global access mechanism through Internet.

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

The following steps are necessary to create and install a SSL certificate for the IP-KVM:

- Create a SSL Certificate Signing Request using the panel shown in Figure. 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.

- Send the saved CSR string to a CA for certification. You will get the new certificate from the CA after a more or less complicated traditional authentication process (depending on the CA).
- Upload the certificate to the IP-KVM using the “Upload” button as shown in Figure below.

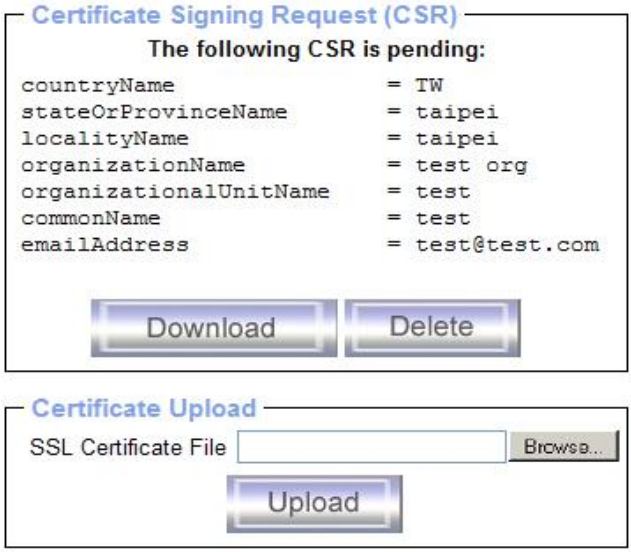


Diagram 7-24 SSL Certificate Upload

Diagram 7-25 CSR string

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

Warning

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

Common name

This is the network name of the IP-KVM once it is installed in the user's network (usually the fully qualified domain name). It is identical to the name that is used to access the IP-KVM with a web browser (without the "http://" prefix). In case the name given here and the actual network name differ, the browser will pop up a security warning when the IP-KVM is accessed using HTTPS.

Organizational unit

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

Organization

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

Locality/City

The city where the organization is located.

State/Province

The state or province where the organization is located.

Country (ISO code)

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

Challenge Password

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

Confirm Challenge Password

Confirmation of the Challenge Password

Email

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

Key length

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

Serial Port

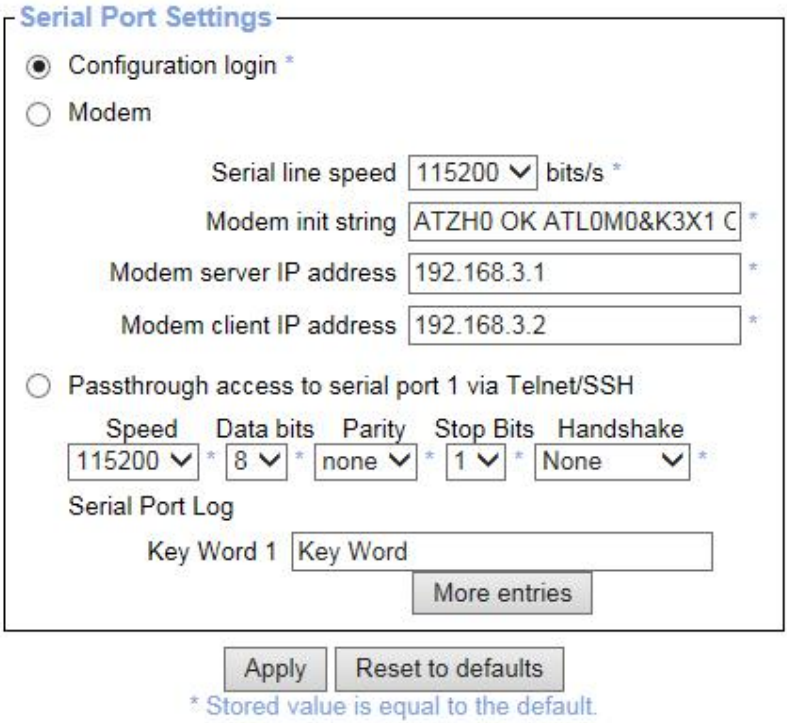


Diagram 7-27 Serial Port

Date / Time

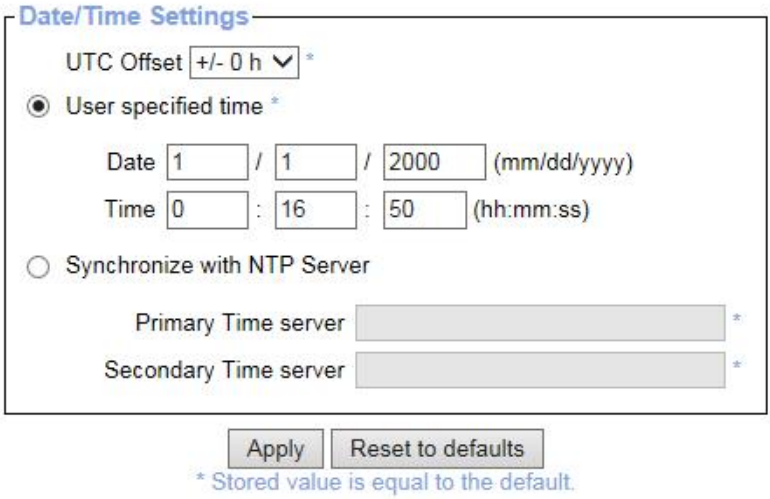


Diagram 7-28 Date / Time

This link refers to a page, where the internal real-time clock of the IP-KVM can be set up. You have the possibility to adjust the clock manually, or to use a NTP timeserver. Without a timeserver, your time setting will not be persistent, so you have to adjust it again, after IP-KVM loses power for more than a few minutes. To avoid this, you can use a NTP timeserver, which sets up the internal clock automatically to the current UTC time. Because NTP server time is always UTC, there is a setting that allows you to set up a static offset to get your local time.

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.

Event Log

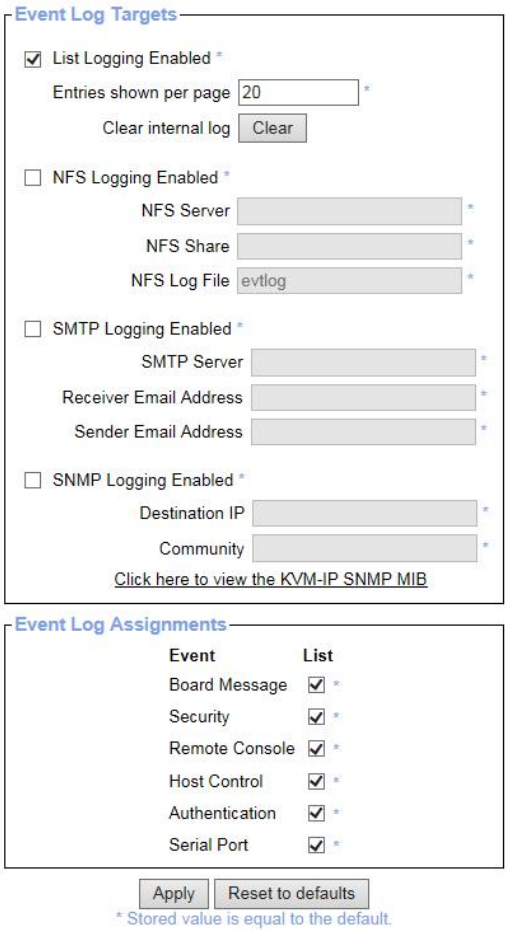


Diagram 7–29 Event Log

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

The common way to log events is to use the internal log list of the IP-KVM. To show the log list, click on “Event Log” on the “Maintenance” page. In the Event Log

Settings you can choose how many log entries are shown on each page. Furthermore, you can clear the log file here.

List logging enabled

The common way to log events is to use the internal log list of the IP-KVM. To show the log list, click on “Event Log” on the “Maintenance” page.

Since the IP-KVM’s system memory is used to save all the information, the maximum number of possible log list entries is restricted to 1.000 events. Every entry that exceeds this limit overrides the oldest one, automatically.

Warning

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

NFS Logging enabled

Define a NFS server, where a directory or a static link has to be exported, to write all logging data to a file that is located there. To write logging data from more than one IP-KVM devices to only one NFS share, you have to define a file name that is unique for each device. When you change the NFS settings and press the

button “Apply” , the NFS share will be mounted immediately. That means, the NFS share and the NFS server must be filled with valid sources or you will get an error message.

SMTP Logging enabled

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

SNMP Logging enabled

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

Here is a example of all gerenated event and its event group.

Device succesfully started	device
Board Reset performed by user...	device
Firmware upload failed.	device
No firmware file uploaded.	device

Uploaded firmware file discarded. device

Firmware validation failed. device

Firmware file uploaded by user... device

Firmware updated by user... device

Internal log file cleared by user... device

Security Violation security

Host Power host

Host Reset host

Connection to Remote Console failed: reason. console (several)

Connection to client ... Established. console

Connection to client ... Closed. console

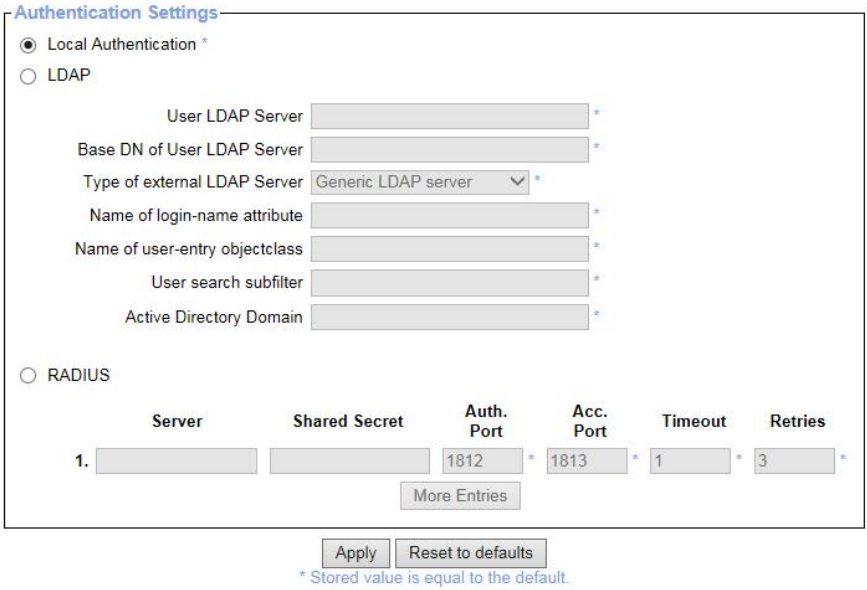
Login failed. auth

Login succeed. Auth

Warning

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

Authentication



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

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

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

LDAP Access

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

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

User LDAP Server

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

Base DN of User LDAP Server

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

Type of external LDAP Server

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

Name of login-name attribute

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

Name of user-entry object class

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

User search subfilter

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

Active Directory Domain

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

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 freeRADIUS 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 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 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 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.

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.

6.6 System Maintenance

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

Device Information

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

Diagram 7-30 Device Information

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

Connected Users

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

Diagram 7-31 Connected Users

Figure above displays the IP-KVM activity. From left to right the connected user(s), its IP address (from which host the user comes from) and its activity status is displayed. RC means that the Remote Console is open. If the Remote Console is opened in exclusive mode the term (exclusive mode) is added. For more information about this option see the Section called Remote Console Control Bar.

To display the user activity the last column contains either the term active for an active user or 30 min idle for a user who is inactive for a certain amount of time.

Even log

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

Event Log

[Prev][Next]

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

[Prev][Next]

Diagram 7-32 Event Log List

Update Firmware

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

Firmware Upload

Firmware File

Upload

Diagram 7-33 Update Firmwares

The IP-KVM is a complete standalone computer. The software it runs is called firmware. The firmware of the 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 IP-KVM the new uncompressed firmware file has to be accessible on the system that you use for connecting to the 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.

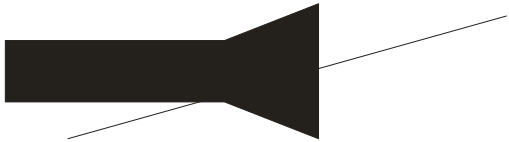
The IP-KVM will automatically initiate a self-reboot upon completion of upgrade process to make newly upgraded firmware effective. At the end of countdown counter expires, the browser will redirect user to the login homepage. Users shall refer to **Maintenance > Device Information** page to check the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

Warning!!!

IP-KVM will verify firmware checksum before proceed upgrade procedure. The mechanism help to prevent false firmware file to damage 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 IP-KVM.

Updating the firmware is a three-stage process:

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

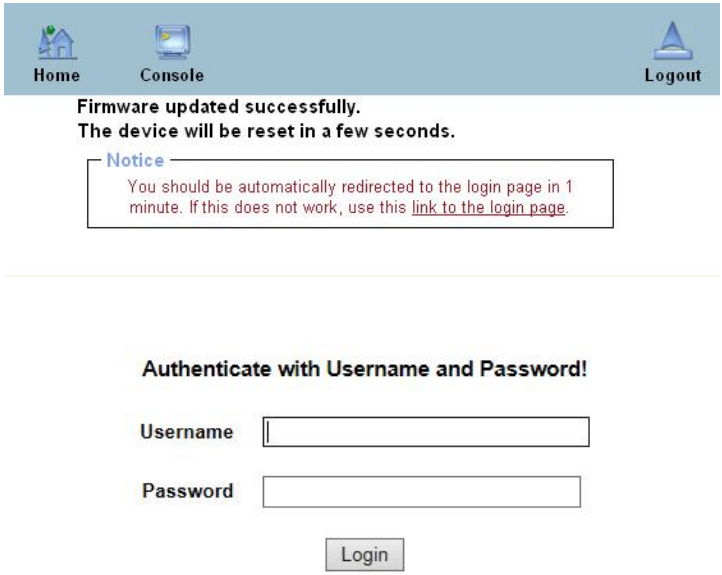


2. In order to do that you need to select the file on your local system using the button "**Browse**" of the Upload Firmware panel. Click **Upload**. Once the firmware file has been uploaded, it is checked whether it is a valid firmware file and whether there were any transmission errors. In case of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

3. 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.

4. 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.

Unit Reset

This section allows you to reset specific parts of the device. This involves resetting keyboard/mouse, USB, video engine, or the IP-KVM device itself.

In general, the IP-KVM requires a reset when implementing a firmware update. In the event of an abnormal operation, a number of subsystems may be reset without resetting the entire IP-KVM.

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

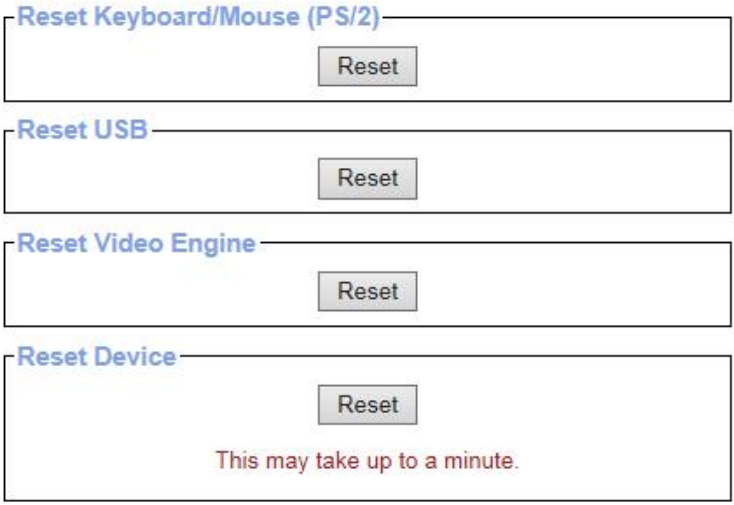


Diagram 7-34 Unit Reset

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

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

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

7.Appendix

7.1 USB Emulation Keyboard

Mac Keyboard

The PC compatible (101/104 keys) keyboard can emulate the functions of the Mac keyboard. The emulation mappings are listed in the below table:

PC Keyboard	MAC Keyboard
[Shift]	Shift
[Ctrl]	Ctrl
	⌘
L_Win & “1”	
L_Win & “2”	
L_Win & “3”	
L_Win & F12	
[Alt]	Alt
[Print Screen]	F13
[Scroll Lock]	F14
	=
[Enter]	Return
[Backspace]	Delete
[Insert]	Help

Sun Keyboard

The PC compatible (101/104 keys) keyboard can emulate the functions of the Sun keyboard when the control key [L_Win] is used in conjunction with other keys.The corresponding functions are shown in the below table:

PC Keyboard	Sun Keyboard
L_Win&L_Alt	Stop
L_Win&F4	Again
L_Win&L_Ctrl	Props
L_Win&F5	Undo
L_Win&F1	Front
L_Win&F6	Copy
L_Win&F2	Open
L_Win&F7	Paste
L_Win&F3	Find
L_Win&F8	Cut
L_Win&”1”	V_DN
L_Win&”2”	Mute
L_Win&”3”	V_UP
L_Win&F12	Power
L_Win&F11	Help
L_Win&L_Shift	Compose
	◆

Model			8 Port	16 Port	32 Port
Direct computer connections			8	16	32
Max computer connections			256	512	1024
Port selection			Front panel LEDs, OSD menu		
Connector	Console	Keyboard Mouse	2 * USB TYPE A		
		Monitor	1-HDB-15 Female(blue)		
	KVM port (RJ-45)		8	16	32
	Upgrading switch		1* RJ11 Female		
	Power		3-Prong AC socket		
Switch	Port selection		8* LEDs	16 * LEDs	32 * LEDs
	Reset		1* tuch-button		
	Upgrading switch		1* toggle switch		
	Power		1* rocker switch		
LED Indicator	Online		8 (green)	16 (green)	32(green)
	Selected		8 (orange)	16 (orange)	32(orange)
	Power		1(blue)		
	Cascade Display		2*7- Segment (orange)		
IP module	Remote access connection		1 x RJ-45		
	Firmware upgrading port		1 x Serial DB9 Pin		
	IP settings		DHCP, Bootp, Fixed IP(DDNS supported)		
	Event Log		NFS, SMTP, SNMP trap		
	Management Interface		Web, Utility, Telnet, Serial port		
I/R value			100V- 240Vac , 50-60Hz , <1.5A		

Power consumption		8W	9W	10W
Video Signal		1600x1200@60Hz(50m); 1280x1024@60Hz(100m); DDC2B		
Environment Requirements	Operating Temperature	0–40℃		
	Store Temperature	–20–60℃		
	Humidity	0–80%RH,Non–condensing		
Physical Features	Material	Metal		
	Weight	2.6kg	2.8kg	3.0kg
	Dimension	433*171*44.5mm		

7.2 Specifications

7.3 FAQ

1.There is no image after open up.

Solutions:

1）Check the power LED, if it is not keeps on, check the 220V power input.

2）Make sure the monitor is connected and power on.

2.No password window pops up after boot, there is no response from the keyboard

Solutions:

1)Make sure the keyboard is OK.

2)Plug out the PS/2 keyboard, then plug in and the keyboard indicating LED flash once.

3.Enter the password window and select one port; there is no host computer screen.

Solutions:

1)Check the current port, make sure it has connected to the host computer, make sure the host computer output video signal.

2)Check the LED of corresponding port (green and orange light keep on at the same time).

3)Check the network cable connection.

4)Check the module connection.

5)Change a normal module to that port, if OK then the module is damaged.

4. Poor display quality of PC screen.

Solutions:

1) Adjust the definition and brightness.

2) Use good quality network cable such as CAT5 cables or upper.

3) Shorten the network cable length.

4) Lower the display resolution.

5. OSD menu doesn't pop up.

Solutions:

1) Check the keyboard LED, make sure it is flashing, if not, invoke the OSD menu again.

2) If the keyboard LED is flashing, it means we have entered the OSD menu, click 【Esc】,【Scroll_ Lock】or【Num_ Lock】exits OSD menu and invoke again.

6. When I switch to one port, the keyboard and mouse do not work.

Solutions:

1)Make sure you have exited the OSD menu, we have entered the OSD menu if the keyboard LED is flashing, and we can't operate the host computer via keyboard and mouse at this moment.

2)Make sure we can operate the OSD menu via keyboard and mouse, if so the KVM is OK.

3)Moving the mouse or clicking keyboard to see whether the KVM switching

module orange LED is flashing, if not, please change a module.

4)Reboot the host computer; make sure the KVM module has been connected to the host computer before boot.

7.I can't invoke OSD main menu.

Solutions:

1)Check the keyboard, make sure it works.

2)Double click 【Scroll_Lock】

3)Double click 【F12】

4)Double click 【Caps Lock】

8.OSD displays with error code or error display when cascading.

Solutions:

1) Invoke OSD menu after finishing cascading, select【Load default】in【F1】,press Enter to refresh OSD ROM.

9. I can't connect to the IP module.

Solutions:

1) Check the network (the IP address of the KVM).

2) Make sure the KVM is on.

3) Check the IP address as well as other IP settings of the KVM.

10. Forget the password to the IP module.

Solutions:

1) Use the default user "super" and password "pass".

2) Please reach to your supplier if you forget your changed password.

11. Special combination key such as ALT+F2, ALT+F3 are intercepted by the console which can't be sent to the controlled port.

Solution:

You need to define “remote button key”. Set the remote button key from the IP module web: Configuration→Remote Button Key

12. The browser is not conforming to the IP module.

Solutions:

1) Make sure the browser cache setting is correct.

2) Make sure the browser cache setting is not setting as “never check new page”.

If the browser cache setting is setting as “never check new page”, the new page will be loaded via the browser rather than the IP module.

13. Remote mouse not work or unable to sync.

Solution:

Make sure the mouse setting is correct in the IP module.

Phone: +1 (877) 205 5306

Live service http://www.fs.com/product_catalogs.html