LevelOne

ACC-2000

KVM IP Console Module

User Manual

Ver. 1.0.0-0709

Safety

FCC

This equipment has been tested and found to comply with Part 15 of the FCC Rules. Operation is subject to the following two conditions:
(1) This device may not cause harmful interference
(2) This device must accept any interference received, including interference that may cause undesired operation.

CE

This equipment is in compliance with the requirements of the following regulations: EN 55 022: CLASS B

RoHS

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

Table of Contents

1. Introduction

The KVM over IP technology (KVM Switch + IP Console Module) combines digital remote KVM access via IP networks with comprehensive and integrated system management. The KVM over IP defines a new class of remote KVM access which provides flexibility that can prevent extra costs, save times and reduce spaces, and equipment.
The KVM over IP provides convenient, remote KVM access and control via LAN or Internet. It captures, digitizes, and compresses video signal and transmits it with keyboard and mouse signals to and from a remote computer. KVM over IP provides a non-intrusive solution for remote access and control. Remote access and control software runs on its embedded processors only but not on mission-critical servers, so that there is no interference with server operation or impact on network performance.

The KVM IP Console Module will automatically detect the current video mode of the console, however manual fine-tuning is recommended to receive the best video quality.

1.1 Feature overview

- Remotely access computers via LAN, WAN or the Internet.
- KVM access over IP and analogous telephone line (modem needed).
- Full control under any OS, in BIOS mode, during boot, at Blue Screens
- No additional software necessary on servers
- 256 bit SSL encryption of all transmitted data and Certificate management
- Automatically senses video resolution for best possible screen capture
- High-performance mouse tracking and synchronization
- Automatic adjustment of data rate to transmission line
- Remote mass storage control
- Control over all java-enabled Browsers
- Firmware update via web interface

1.2 System requirement

Hardware

Item	Description
Local Host	KVM switch unit (KVM-0831, KVM-1631, KCM-0831, KCM-1631)
Remote Console	Server which linked into the network

Software

Item	Description
Local Host	No additional software necessary
Remote Console	(1) Java Runtime Environment : version 1.4.2 or above (2) Browser: Microsoft Internet Explorer version 6.0 or above or Netscape or Mozilla or Safari

1.3 When the server is up and running

The KVM over IP provides a full control over the remote servers. The Management Console allows user to access the remote server's graphics, keyboard and mouse and to send commands to the server. User can also perform periodic maintenance of the server. Using the Console Redirection Service, users are able to do the following:

I. Reboot the system
II. Watch the boot process.
III. Boot the system from a separate partition to load the diagnostic environment.
IV. Run special diagnostic programs.

1.4 When the server is dead

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

I. Hard disk failure 50%
II. Power cable detached, power supply failure 28%
III. CPU, Controller, main board failure 10%
IV. CPU fan failure 8%
V. RAM failure 4%

Using the 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

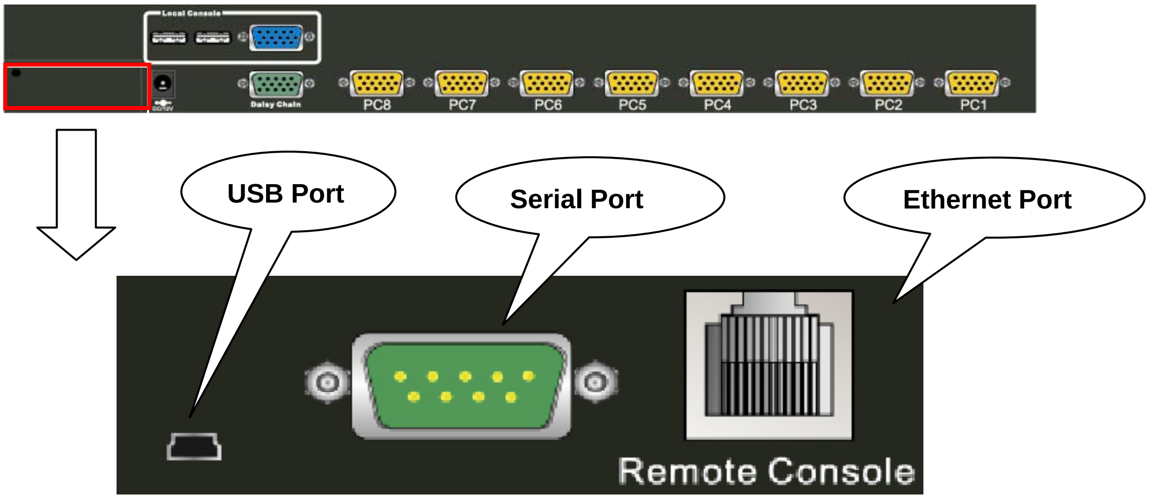
2. The quick installation guide

The KVM IP Console Module redirects local keyboard, mouse and video data to a remote administration console. It allows user to control one or many computers locally at the server site or remotely via the Internet using a standard web browser. User can securely gain BIOS level access to systems for maintenance, support, or failure recovery over the Internet. Communication is secure via SSL encryption. Use in conjunction with a KVM switch for multiple-server access.

2.1 Installation

The KVM IP Console Module works with the KVM Switch that has an expansion slot.
Ex) KVM-0831/1631, KCM-0831/1631

Below is a diagram illustrated KVM-0831 and ACC-2000.



Please perform the following steps:

1. Connect Ethernet to LAN port and/or modem to serial port, depending on how user would like to access the KVM IP Console Module.
2. (Optional) Connect the type A connector of USB A-B cable to the host computer, while using remote mass storage control.

Please perform the following steps:

3. Power down computer and the KVM Switch
4. Remove the cover on the expansion slot from KVM Switch and carefully slide in the KVM IP Console Module into the expansion slot.
5. Connect the power supply to the KVM Switch once IP Console Module firmly installed.
6. Connect the monitor, keyboard and mouse to the KVM Switch.

7. Use VGA cable (15-pin HDDB Male / Male) connects computer and KVM Switch.

Please refer to KVM-0831/1631 user manual for more detail.

2.2 Initial IP configuration

For the default value, DHCP mode is disabled, and the IP settings are as listed below:

IP address	192.168.1.22
Subnet mask	255.255.255.0
Default Gateway	None

(IP auto configuration = None)

If DHCP mode is enabled (IP auto configuration = DHCP), the KVM IP Console Module will try to contact a DHCP server in the subnet to which it is physically connected. If a DHCP server is found, it may provide a valid IP address, gateway address and net mask. Before user connects the device to the local subnet, be sure to complete the corresponding configuration of the DHCP server. It is recommended to configure a fixed IP assignment to the MAC address of the KVM IP Console Module. User is able to find the MAC address label on the bottom of KVM IP Console Module.

KVM IP Console Module Setup Tool

If this initial configuration does not meet the local requirements, please use the setup tool to discover KVM IP Console Module and change the configurations as user requested. The setup tool **IPSetup** can be found in the CD delivered with KVM Switch (KVM-0831/1631 & KCM-0831/1631). User can also download the setup tool from website at www.level1.com Follow the procedures described below for using setup tool **IPSetup**.

DHCP

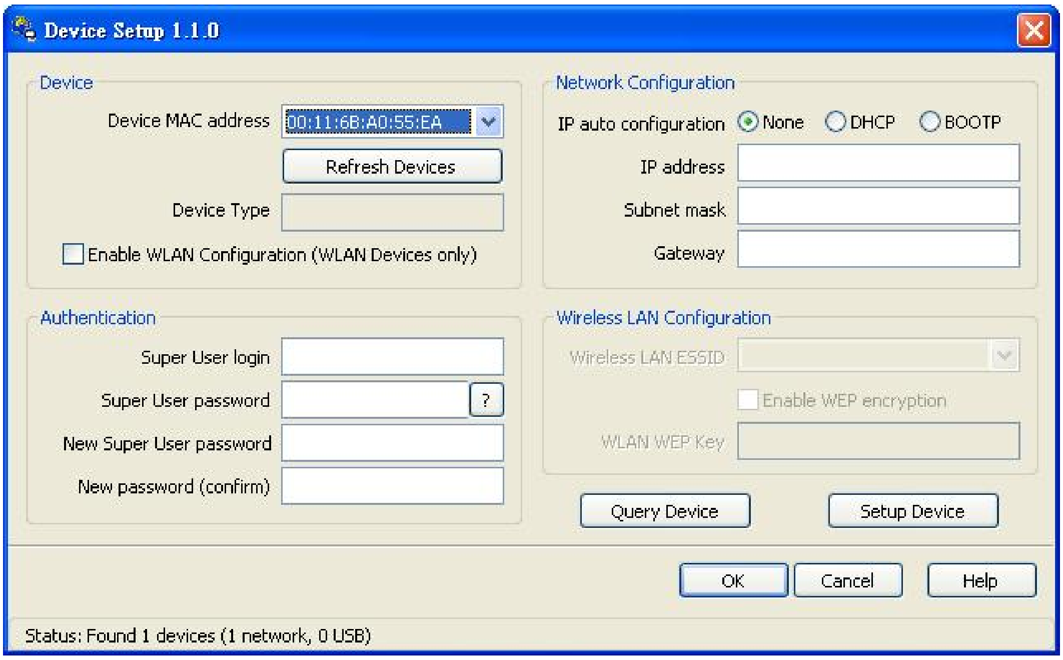
If user has installed the KVM IP Console Module in a network with DHCP, user is able to use the **IPSetup** to find out the IP for KVM IP Console Module.

(1) Plug Ethernet cable to KVM IP Console Module. KVM IP Console Module will get an IP via DHCP.

(2) Using **IPSetup** (run PSetup.exe) to look for KVM IP Console Module.

a. Select MAC address which label on bottom of KVM IP Console Module

b. Click **Query Device**



Device Setup 1.1.0

Device

Device MAC address 00:11:6B:A0:55:EA

Device Type

□ Enable WLAN Configuration (WLAN Devices only)

Network Configuration

IP auto configuration ● None ○ DHCP ○ BOOTP

IP address

Subnet mask

Gateway

Authentication

Super User login

Super User password

New Super User password

New password (confirm)

Wireless LAN Configuration

Wireless LAN ESSID

□ Enable WEP encryption

WLAN WEP Key

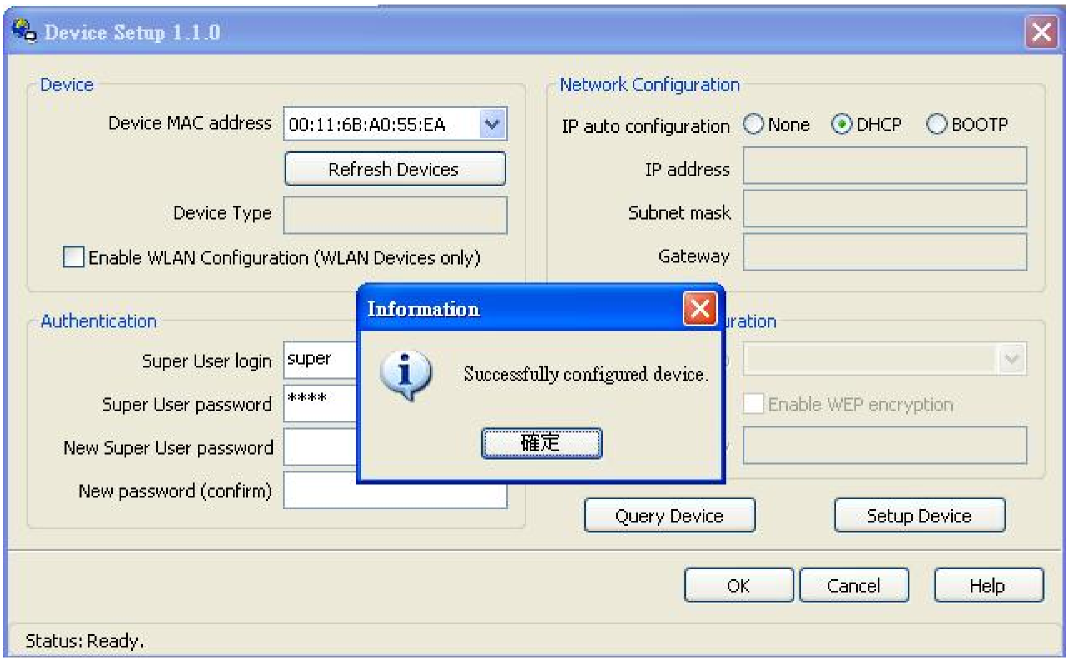
Status: Found 1 devices (1 network, 0 USB)

Setting for Fixed IP

a. Set “IP auto configuration” as “**None**”; enter the specific IP address and Subnet mask

b. Type in the login name and password for Authentication (default: **super**/**pass**)

c. Click **Setup Device**. If the login name and password are corrected, it will then authenticated, and display the following message “Successfully configured device”. It will show “Permission Denied” if the user name or password is incorrect.



Device Setup 1.1.0

Device

Device MAC address 00:11:6B:A0:55:EA

Device Type

□ Enable WLAN Configuration (WLAN Devices only)

Network Configuration

IP auto configuration ○ None ● DHCP ○ BOOTP

IP address

Subnet mask

Gateway

Authentication

Super User login super

Super User password ****

New Super User password

New password (confirm)

□ Enable WEP encryption

Information

Successfully configured device.

Status: Ready.

Install JVM on Client system

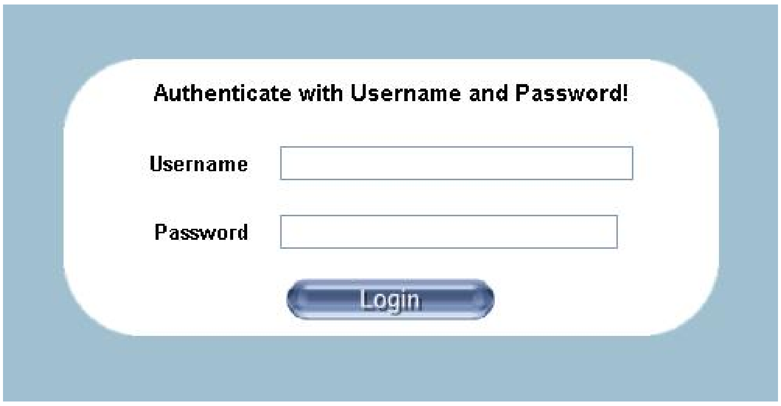
KVM IP Console Module was accessed using a standard JAVA enabled web browser. User must install Sun JVM 1.4.2 or above to the device.

Note: Minimum requirement for web browser; Internet Explorer 6.0 or Netscape 7.0 or Molliza 1.6 (and above)

Connect the KVM IP Console Module via Web

Using the HTTP protocol or a secure encrypted connection via HTTPS and entering the configured IP address of the KVM IP Console Module into web browser to connect to the KVM Switch for remote management.

This will lead to the KVM IP Console login page as display below.



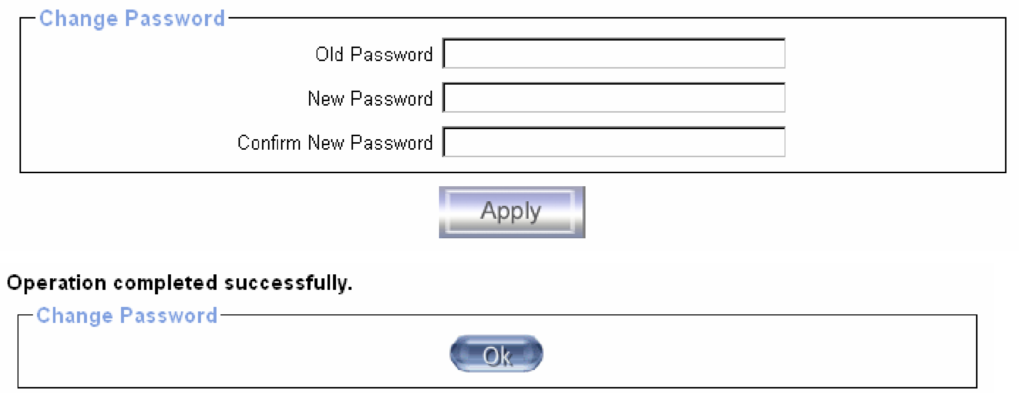
Authenticate with Username and Password!

Default settings:

Username	super
Password	pass

The super user has all permissions to administrate KVM IP Console.

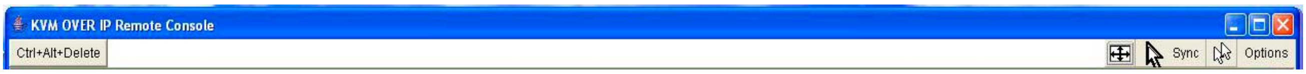
For security reason, after initial login, the system will prompt for requesting new password.



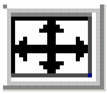
Operation completed successfully.

Control servers via Remote Console

The Remote Console is the redirected screen, keyboard and mouse of the host server to the KVM Switch which KVM IP Console Module is installed. The Remote Console will behave exactly the same way as if user were sitting directly facing the server and achieve the definition of **remote management**. Open the console by selecting the preview picture on the main site of the HTML front end. Figure 1-2 shows the heading of the Remote Console.



There are some options to choose from, and the important ones are the following:

Auto Adjust button 

If the video displayed is of bad quality or distorted in some way, press this button and wait a few seconds while KVM Switch tries to adjust itself for the best possible video quality.

Sync Mouse

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 server. In general there is no need to change mouse settings on the host.

Video Settings in Options Menu

This opens a new window with elements to control the KVM Switch Video Settings. User can change some values setting, for instance the brightness and contrast of the picture displayed, which may improve the video quality. It is also possible to revert to the default settings for all video modes or only the current one.

Note: If the local mouse pointer is not synchronized with the remote mouse pointer, press the Auto Adjust Button once.

3. Configuration

3.1 Initial Configuration

If DHCP mode is enabled (IP auto configuration = DHCP), the KVM IP Console Module will try to contact a DHCP server in the subnet to which it is physically connected. If a DHCP server is found, it may provide a valid IP address, gateway address and net mask. Before user connects the device to the local subnet, be sure to complete the corresponding configuration of the DHCP server. It is recommended to configure a fixed IP assignment to the MAC address of the KVM IP Console Module. User can find the MAC address labeled on the bottom side of the metal housing.

If DHCP mode is disabled (IP auto configuration = None), the factory default IP settings are as below:

IP address	192.168.1.22
Subnet mask	255.255.255.0
Default Gateway	None

Initial Network Configurations

KVM IP Console Module Setup Tool

If this initial configuration does not meet your local requirements, use the setup tool to change the configurations as you need. The setup tool **IPSetup** can be found in the CD delivered with KVM Switch (KVM-0831/1631 & KCM-0831/1631). User can also download the setup tool from website at www.level1.com Follow the procedures described below for using setup tool **IPSetup**.

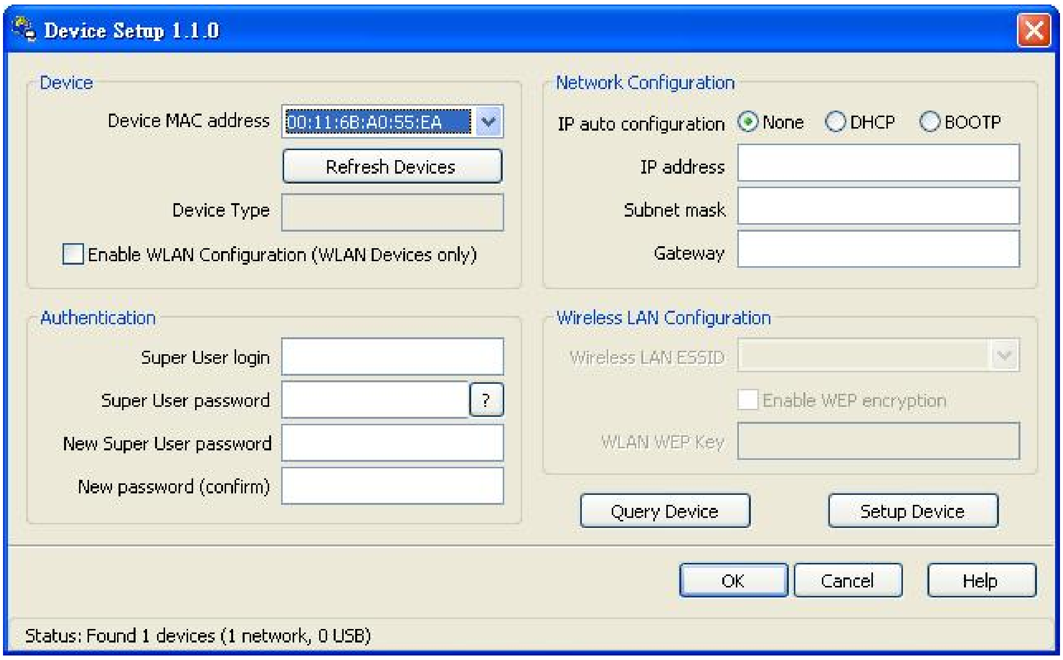
DHCP

If user has installed the KVM IP Console Module on a network that has DHCP server enabled, **IPSetup** can be used to find out the IP address for KVV IP Console Module.

(1) Plug Ethernet cable to KVM IP Console Module, it will then get an IP via DHCP.
(2) Using **IPSetup** (run IPSetup.exe) to look for KVM IP Console Module.
 a. Select MAC address which label on bottom of KVM IP Console Module
 b. Click **Query Device**

Notes:

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



Device MAC address: 00:11:6B:A0:55:EA

Device Type:

□ Enable WLAN Configuration (WLAN Devices only)

Super User login:

Super User password:

New Super User password:

New password (confirm):

IP auto configuration: ● None ○ DHCP ○ BOOTP

IP address:

Subnet mask:

Gateway:

Wireless LAN ESSID:

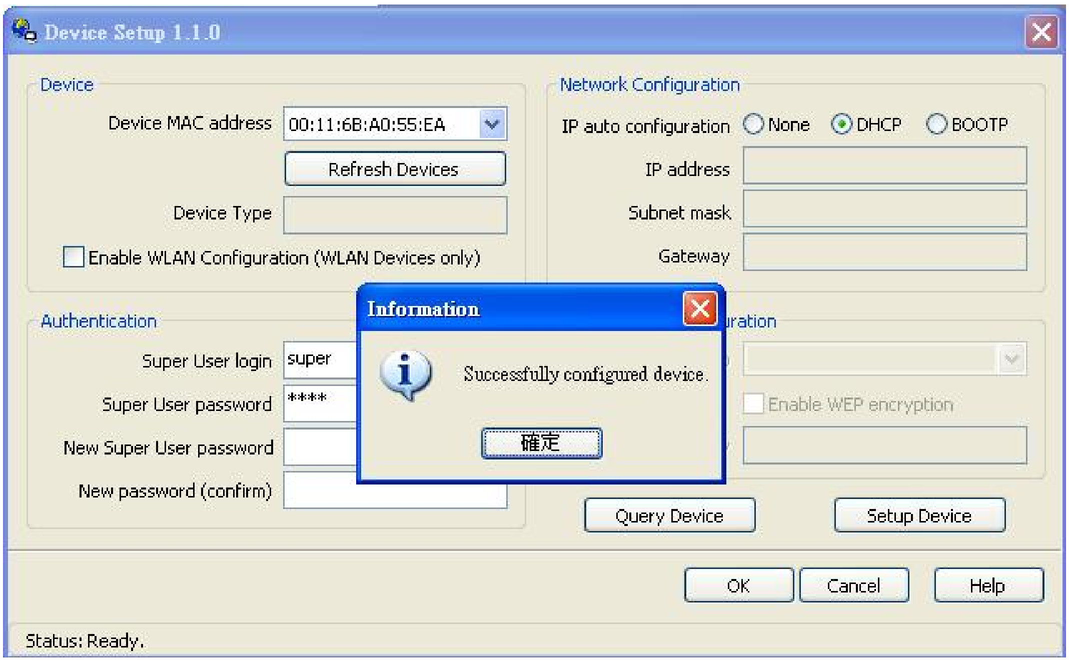
□ Enable WEP encryption

WLAN WEP Key:

Status: Found 1 devices (1 network, 0 USB)

Setup fixed IP

a. Setup “IP auto configuration” as “**None**” ; setup IP address and Subnet mask
b. Enter user login and password for Authentication (default : super/pass)
c. Click **Setup Device**. If super login was authenticated, it’ll show “Successfully configured device”. Otherwise it’ll show “Permission Denied”.



Device MAC address: 00:11:6B:A0:55:EA

Device Type:

□ Enable WLAN Configuration (WLAN Devices only)

Super User login: super

Super User password: ****

New Super User password:

New password (confirm):

IP auto configuration: ○ None ● DHCP ○ BOOTP

IP address:

Subnet mask:

Gateway:

□ Enable WEP encryption

Successfully configured device.

Status: Ready.

Authentication

To modify the authentication settings, enter user login name and password, then assign new password.

Super user login

Enter the login name of the super user. The initial value is “***super***”. All characters are in lower case.

Super user password

Enter the current password for the super user. This initial password is “***pass***”. All characters are in lower case.

New super user password

Assign the new password for administrator.

New password (confirm)

Re-enter the new password for confirmation.

Press “OK” to apply newly assign password; otherwise click “Cancel”.

3.1.1 Initial configuration via serial console

For using serial terminal, the KVM IP Console Module has a serial line interface. This connector is compliant with the RS-232 serial line standard. The serial line has to be configured with the parameters given below.

When configuring with a serial terminal, e.g., Hyper Terminal, reset the KVM IP Console Module and immediately press the “ESC” key. Some device information will be displayed, and a “=>” sigh will prompt. Enter “config”, then press Enter key to wait for the configuration questions to appear.

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

As proceeding, the following questions will appear on the screen. To accept the default values shown in square brackets below, press the Enter key from user keyboard.

```
IP auto configuration (none/dhcp/bootp):

IP [192.168.1.22]:
Net mask [255.255.255.0]:
Gateway (0.0.0.0 for none) [0.0.0.0]:
```

IP auto-configuration
With this option, user can specify whether the KVM IP Console Module should get its network settings from a DHCP or BOOTP server. For DHCP, enter “dhcp”, and for BOOTP enter “bootp”. If user does 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 of the KVM IP Console Module; this option is only available if IP auto-configuration is disabled.

Net mask
The net mask of the connecting IP subnet; this option is only available if IP auto-configuration is disabled.

Gateway address
The IP address of the default router for the connecting IP subnet; if user does not have a default router, enter 0.0.0.0. This option is only available if IP auto-configuration is disabled.

3.2 Keyboard, Mouse, and Video configuration

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

3.2.1 KVM over IP keyboard settings

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

3.2.2 Remote Mouse Settings

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

Auto mouse speed

The automatic mouse speed mode tries to detect the speed and acceleration settings of the host system automatically. See the section below for more detailed explanation.

Fixed mouse speed

This mode just translates the mouse movements from the Remote Console in a way that one pixel move will result in n-pixel moves on the remote system. This parameter n is adjustable with the scaling. Please note that this works only when mouse acceleration is turned off on the remote system.

3.2.3 Automatic mouse speed and mouse synchronization

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

Fast Sync

The fast synchronization is used to correct a temporary, but fixed skew. Choose the option using the Remote Console options menu or press the mouse synchronization hotkey sequence in case you defined one.

Intelligent Sync

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

Note

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

3.2.4 Host system mouse settings

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

Note

The following limitations do not apply when USB and Mouse Type "Windows >= 2000, Mac OSX"

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

Special Mouse Driver

There are mouse drivers that influence the synchronization process and lead to desynchronized mouse pointers. If this happens, make sure do not use a special vendor-specific mouse driver on your host system.

Windows XP Mouse Settings

Windows XP knows a setting named "improve mouse acceleration", which has to be deactivated.

Active Desktop

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

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

3.2.5 Single and Double Mouse Mode

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

3.2.6 Recommended Mouse Settings

For the different operating systems we can give the following advice:

MS Windows 2000/2003 (Professional and Server) and XP (all versions)
In general, we recommend the usage of a mouse via USB. Choose USB without Mouse Sync. For a PS/2 mouse choose Auto Mouse Speed. For XP disable the option “enhance pointer precision” in the Control Panel.

SUN Solaris
Adjust the mouse settings either via xset m 1 or use the CDE Control Panel to set the mouse to “1:1, no acceleration”. As an alternative you may also use the Single Mouse Mode.

MAC OS X
Recommend using the Single Mouse Mode.

3.2.7 Video Modes

The KVM IP Console Module recognizes a limited number of common video modes; please do not use any custom mode to link with special video modes when running X11 on the host system. Otherwise, the KVM IP Console Module may not be able to detect them. Recommend of using any of the standard VESA video modes.

4. Usage

4.1 Prerequisites

The KVM IP Console Module features an embedded operating system and applications offering a variety of standardized interfaces. This chapter will describe both these interfaces, and the way to use them in a more detailed manner. The interfaces are accessed using the TCP/IP protocol family, thus it can be accessed using the LAN port of the device.

The following interfaces are supported:

HTTP/HTTPS
Full access is provided by the embedded web server. The KVM IP Console Module environment can be entirely managed using a standard web browser. User can access the KVM over IP by using the insecure HTTP protocol, or using the encrypted HTTPS protocol. Whenever possible, use HTTPS.

Telnet
A standard Telnet client can be used to access an arbitrary device connected to the KVM IP Console Module's serial port via a terminal mode.

The primary interface of the KVM IP Console Module is the HTTP interface. This is covered extensively in this chapter. Other interfaces are addressed in subtopics.

In order to use the Remote Console window of the managed host system, the browser has to come with a Java Runtime Environment version 1.4.2 or above. If the browser has no Java support (such as on a small handheld device), users are still able to maintain the KVM IP Console Module by using the administration forms displayed by the browser itself.

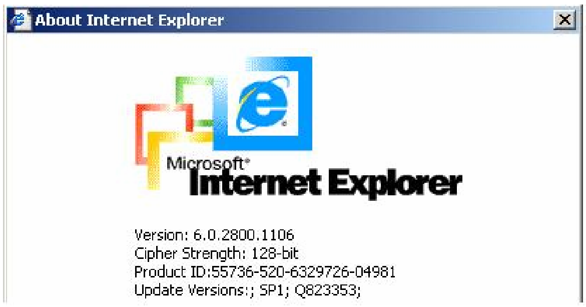
For an insecure connection to the KVM IP Console Module, it is recommended using the following browsers:

Microsoft Internet Explorer version 6.0 or higher on Windows 2000 and Windows XP

Netscape Navigator 7.0 or Mozilla 1.6 on Windows 2000, Windows XP, Unix, Linux and UNIX-like Operating Systems

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

Using the Internet Explorer, open the menu entry “?” and “Info” to read about the key length that is currently activated. The dialog box contains a link that leads you to information on how to upgrade your browser to a state of the art encryption scheme. Below figure shows the dialog box presented by the Internet Explorer 6.0.



Version: 6.0.2800.1106
Cipher Strength: 128-bit
Product ID:55736-520-6329726-04981
Update Versions:; SP1; Q823353;

Newer web browsers generally support higher encryption on default.

4.2 Login into the KVM IP Console Module and logout

4.2.1 Login into the KVM IP Console Module

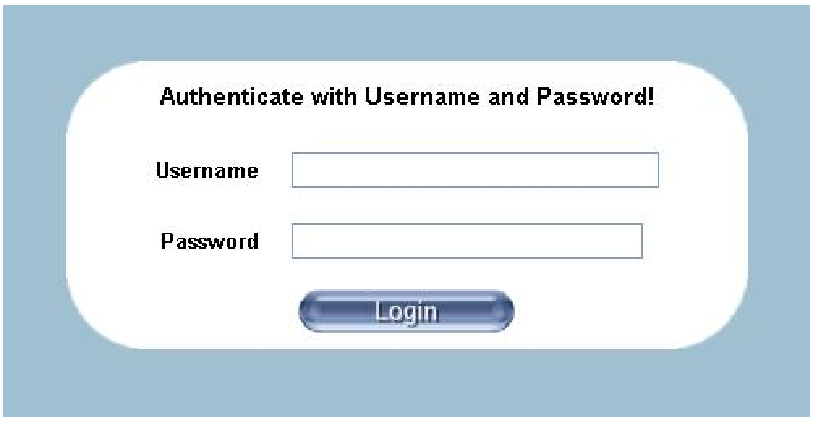
Launch web browser; direct it to the address of KVM IP Console Module, which user configured during the installation process. The address used might be an IP address or a domain name, in the case where user has given KVM IP Console Module a symbolic name in the DNS. For instance, type the following in the URL field of your browser when establishing an unsecured connection:

http://<IP address of KVM IP Console Module>

When using a secure connection, type in:

https://<IP address of KVM IP Console Module>

This will lead to the KVM IP Console Module login page as shown in below figure.



Authenticate with Username and Password!

The KVM IP Console Module has a built-in super user (administrator) that has all permissions to administrate the KVM IP Console Module

:

Username	super (factory default)
Password	pass (factory default)

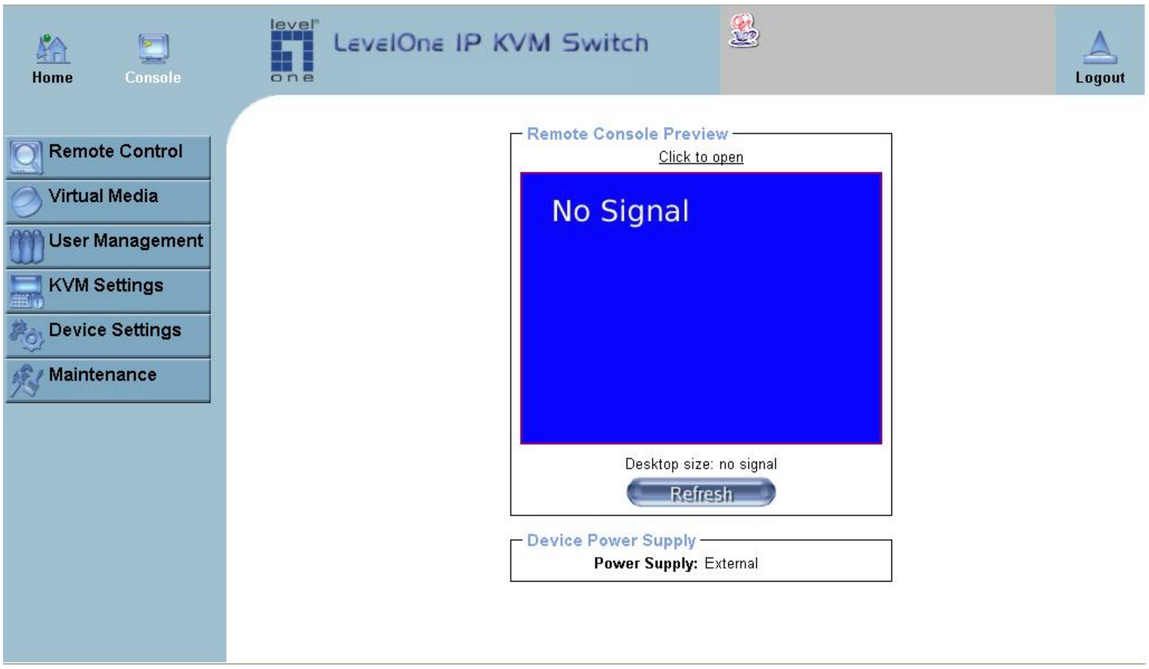
Note

The user “super” is not allowed to login via the serial interface of the KVM IP Console Module. Please make sure to change the password immediately after initial setup. Without assigning new password might result unauthorized access to the KVM switch.

The Web Browser must accept cookies, or else login will fail.

Navigation

Having logged into the KVM IP Console Module successfully, the main page will appear. This page consists of three parts; each of them contains specific information. Within the right frame, task-specific information is displayed that depends on the section user has selected.



Desktop size: no signal

Power Supply: External

Return to the main page of the KVM IP Console Module .

Open the remote console.

Logout

Exit from the KVM IP Console Module

Note

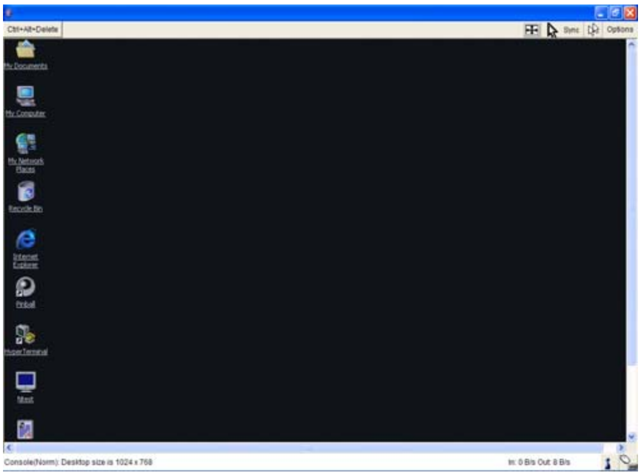
The KVM IP Console Module will automatically logout if there is no activity for 30 minutes.

4.2.2 Logout from the KVM IP Console Module

This link logs out the current user and presents a new login screen. Please note that an automatic logout will be performed in case there is no activity for 30 minutes.

4.3 The Remote Console

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



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

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

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

4.4 Main Window

Starting the Remote Console opens an additional window. It displays the screen content of your host system. The Remote Console will behave exactly in the same way as if you were sitting locally in front of the screen of your remote system. That means keyboard and mouse can be used in the usual way. However, be aware of the fact that the remote system will react to keyboard and mouse actions with a slight delay. The delay depends on the bandwidth of the link to which you use to connect to the KVM IP Console Module.

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

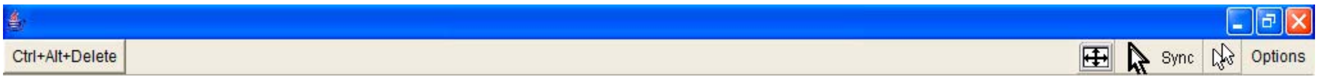
The Remote Console window will always tries to show the remote screen with its optimal size. That means it will adapt its size to the size of the remote screen initially and after the screen resolution of the remote screen has been changed. However, user can always resize the Remote Console window in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

Note

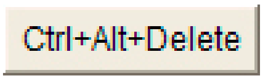
In difference to the remote host system, the Remote Console window on the local window system is just one window among others. In order to make keyboard and mouse work, the Remote Console window must have the local input focus.

4.4.1 Remote Console Control Bar

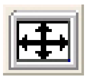
The upper part of the Remote Console window contains a control bar. Using its elements user can see the state of the Remote Console and adjust the local Remote Console settings. A description for each control follows.



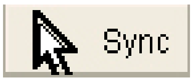
Remote Console Control Bar

Ctrl+Alt+Delete 

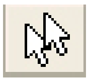
Special button key to send the “Control Alt Delete” key combination to the remote system (see also section 6.4.1 for defining new button keys).

Auto Adjust button 

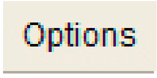
If the video display is blurry with unclear display quality, press this button and wait for few seconds while the KVM IP Console Module tries to detect the video mode of VGA port to the controlled host and adjust itself for the best possible video quality.

Sync mouse 

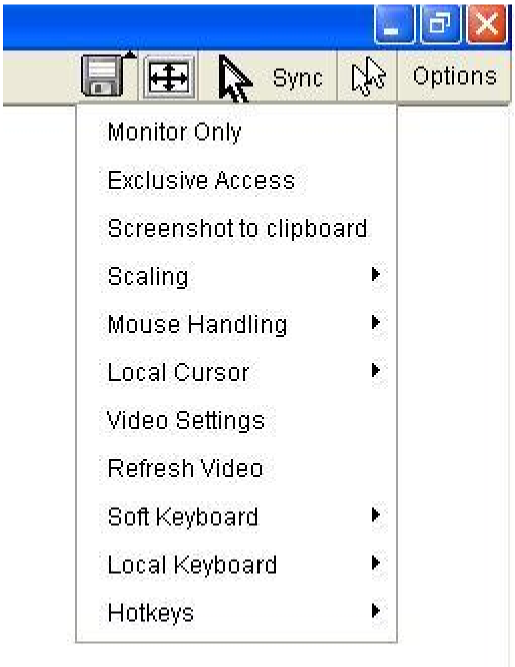
Activates the mouse synchronization process. Choose this option in order to synchronize the local with the remote mouse cursor. This is especially necessary when using accelerated mouse settings on the host system. In general, there is no need to change mouse settings on the host.

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”.



Remote Console Options Menu

A short description of the options follows.

Monitor Only

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

Exclusive Access

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

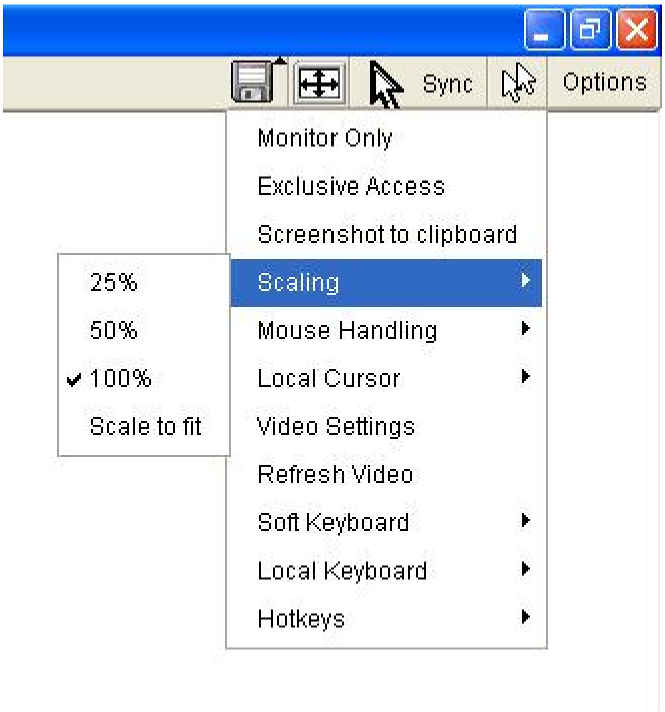
A change in the access mode is also visible in the status line.

Remote Console Exclusive Mode

Scaling

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

When user designate 25%, 50%, or100% scaling, the size of Remote Console window is calculated according to the remote host video setting with scaling algorithm execution. When select designate “Scale to fit”, the remote video displaying is scaled to fit the size of Remote Console window.



Remote Console Options Menu:Scaling

Mouse Handling

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

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

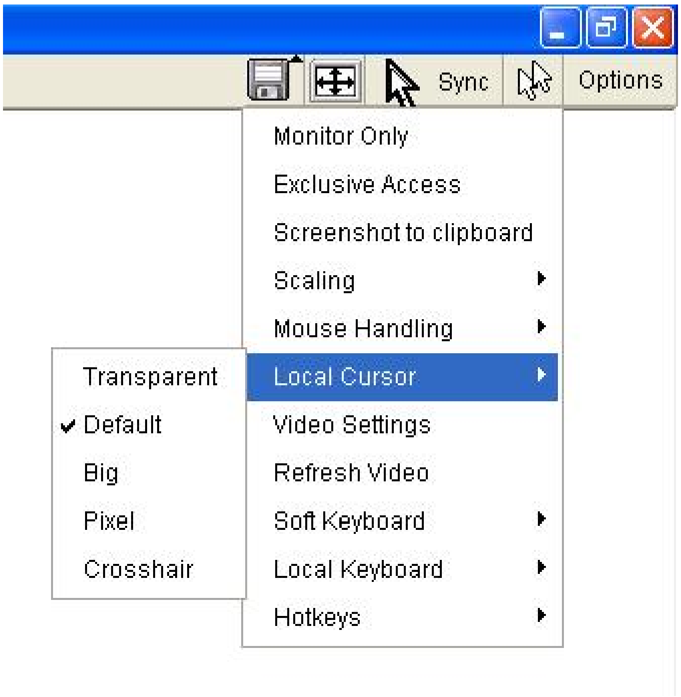
Intelligent Sync --
Use this option if the fast sync does not work or the mouse settings have been changed on the host system.

Note

Intelligent Sync. method takes more time than the fast Sync. And also requires a correctly adjusted picture. Use the auto adjustment function to setup the picture.

Local Cursor

The local mouse pointer offers a list of different cursor shapes to choose from. The selected shape will be saved for the current user and activated the next time this user opens the Remote Console. The number of available shapes depends on the Java Virtual Machine; a version of 1.4.2 or above offers the full list.



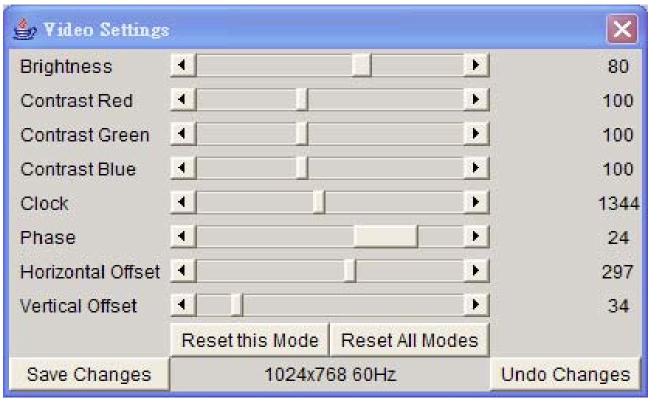
Remote Console Options Menu:Cursor

Video Settings

Open a panel for changing the KVM IP Console Module video settings. The KVM IP Console Module features two different dialogs, which for adjusting the video settings.

Video Settings through the HTML-Frontend
To enable local video port, select this option. This option decides if the local video output of the KVM IP Console Module is active and passing through the incoming signal from the host system.
The option Noise Filter defines how the KVM IP Console Module reacts to small changes in the video input signal. Turning on the noise filter can help reduce video flickering that is often caused by distortions, as well as lowering unnecessary bandwidth consumption. A large filter setting needs less network traffic and leads to a faster video display, but small changes in some display regions may not be recognized immediately. A small filter displays all changes instantly but may lead to a constant amount of network traffic even if display content is not really changing (depending on the quality of the video input signal). All in all the default setting should be suitable for most situations.

Video Settings through the remote console



Brightness	80
Contrast Red	100
Contrast Green	100
Contrast Blue	100
Clock	1344
Phase	24
Horizontal Offset	297
Vertical Offset	34

1024x768 60Hz

Video Settings Panel

Brightness Controls the brightness of the picture

Contrast Controls the contrast of the picture

Clock Defines the horizontal frequency for a video line and depends on the video mode. Different video card types may require different values here. The default settings in conjuction with the auto adjustment procedure should be adequate for all common configurations. If the picture quality is still unclear after auto adjustment, user may try to change this setting together with the sampling phase to achieve a better quality.

Phase Defines the phase for video sampling, used to control the display quality together with the setting for sampling clock.

Horizontal Position Use the left and right buttons to move the picture in horizontal direction while this option is selected.

Vertical Position Use the left and right buttons to move the picture in vertical direction while this option is selected.

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

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

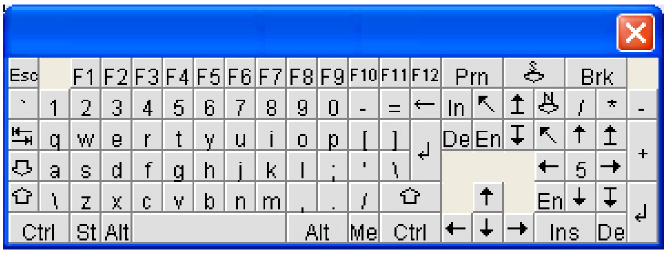
Save changes Save changes permanently

Undo Changes Restore last settings

Refresh Video

Click to run this menu item for retrieving the whole video again from the controlled host and displayed on Remote Console. In normal situation, only changed parts of video will be packed and sent from the KVM IP Console Module, for saving network bandwidth. This function is mainly used for troubleshooting purpose where some old video fragments are displayed as not updated in time for some reason; for example, noise filter for VGA is setting too large.

Soft Keyboard


Esc F1 F2 F3 F4 F5 F6 F7 F8 F9 F10 F11 F12 Prn Brk
` 1 2 3 4 5 6 7 8 9 0 - = In / * -
q w e r t y u i o p [ ] De En +
a s d f g h j k l ; ' \ 5
\ z x c v b n m , . / En
Ctrl St Alt Alt Me Ctrl Ins De

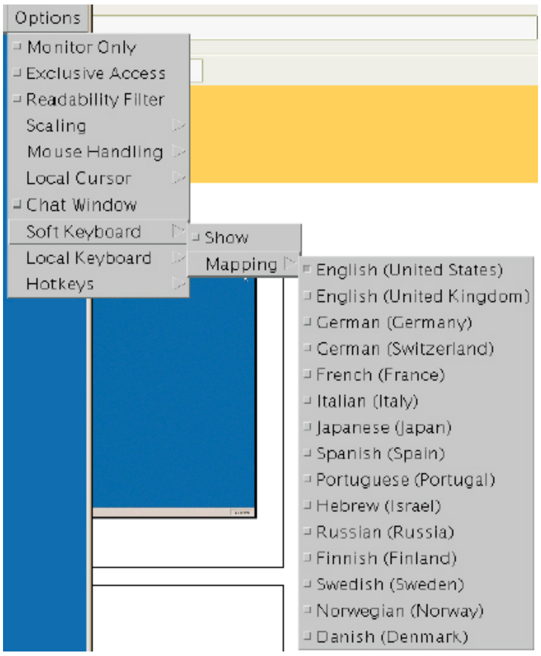
Soft Keyboard

Open up the Menu for the Soft-Keyboard.

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

Mapping

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



Soft Keyboard Mapping

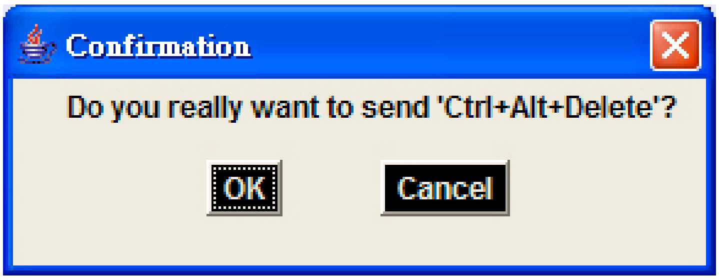
Local Keyboard

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

Hotkeys

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

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



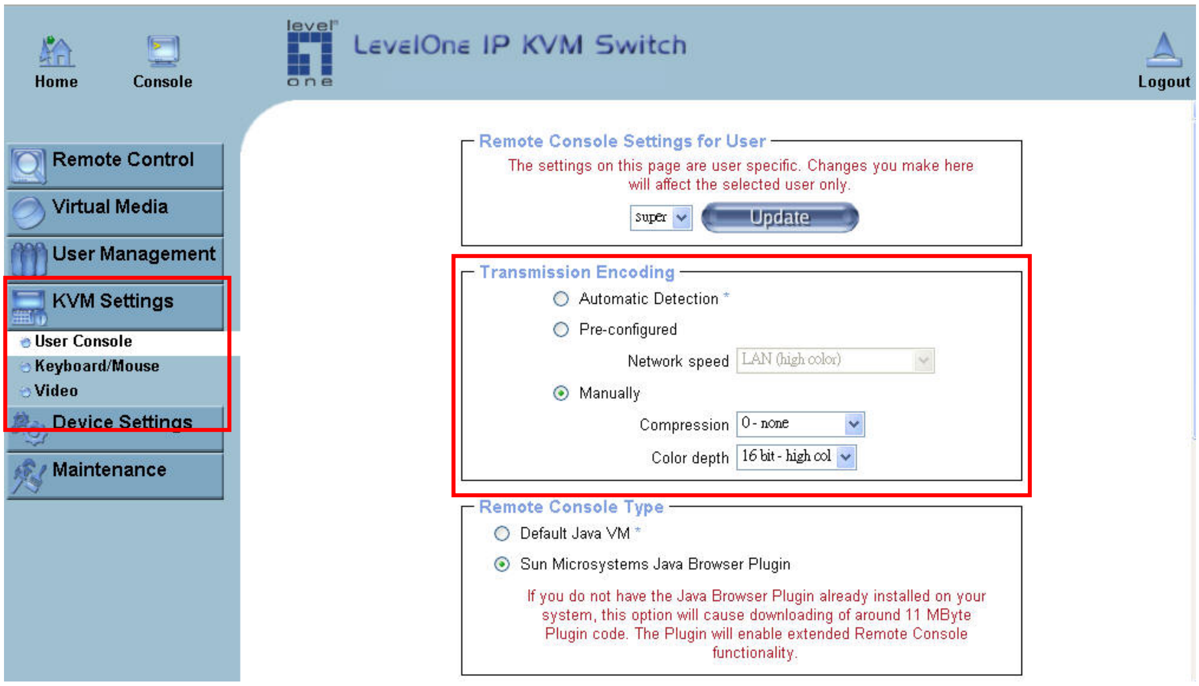
Confirmation

Do you really want to send 'Ctrl+Alt+Delete'?

Remote Console Confirmation Dialog

Encoding

These options are used to adjust the encoding level in terms of compression and color depth. These options are only available when user selects “Manually” under Transmission Encoding section. Please notify that the default value is “Automatic Detection”, which Compression and Color depth will detect automatically.



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 *

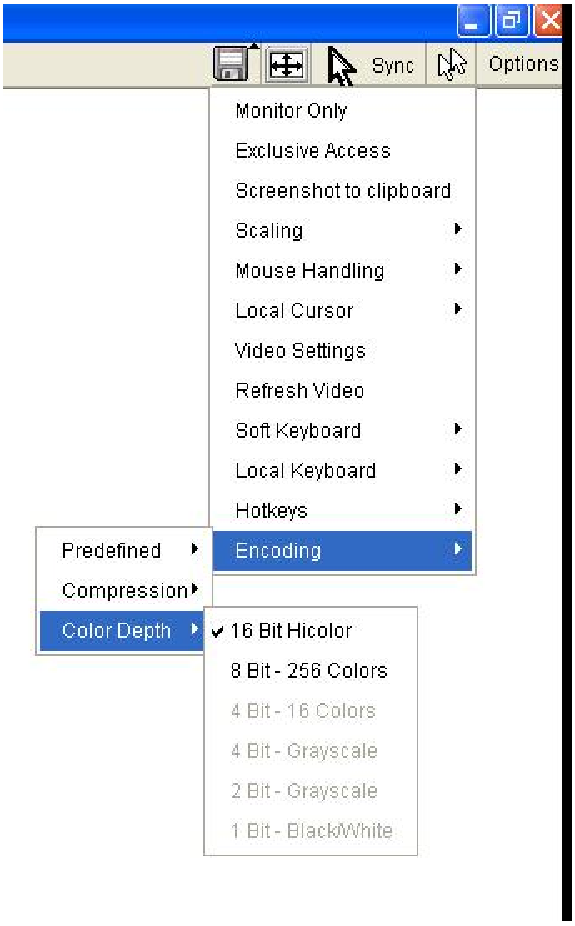
● Sun Microsystems Java Browser Plugin

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.

Compression Level: User may select a value between 1 and 9 for the desired compression level with level 1 enabling the fastest compression and level 9 the best compression. The most suitable compression level should always be seen as a compromise between the network bandwidth that is available, on the video picture to be transferred, and on the number of changes between two single video pictures. It is recommended using a higher compression level if the network bandwidth is low. The higher the compression level the more time is needed to pack and unpack the video data on either side of the connection. The compression quality depends on the video picture itself, e.g. the number of the colors or the diversity of pixels. The lower the compression quality, the more data have to be sent and the longer it may take to transfer the whole video picture.

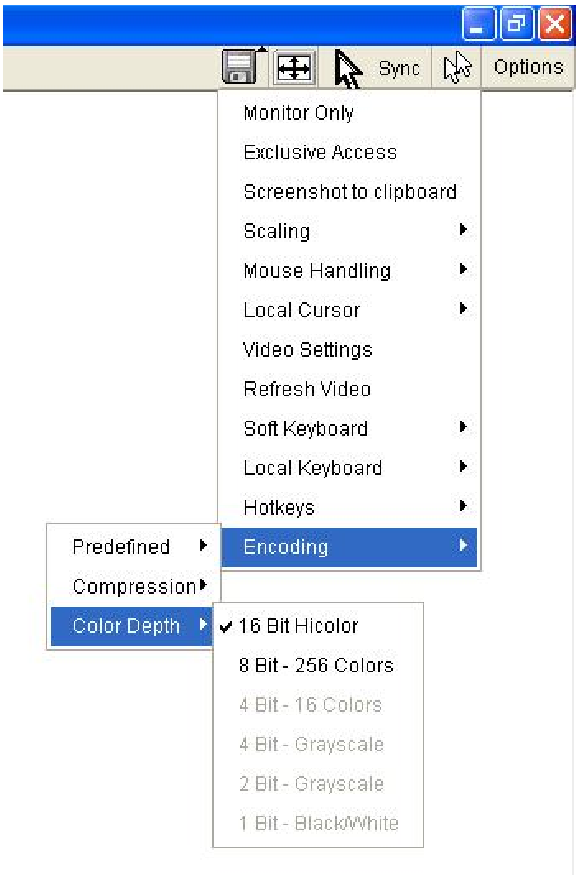
If level 0 is chosen the video compression is disabled, completely.

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



Encoding Compression

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



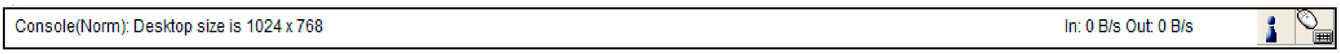
Encoding Color depth

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

4.4.2 Remote Console Status Line

Status line

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

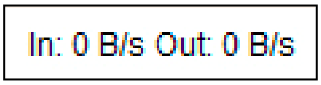


Console(Norm): Desktop size is 1024 x 768

In: 0 B/s Out: 0 B/s

Status line

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


In: 0 B/s Out: 0 B/s

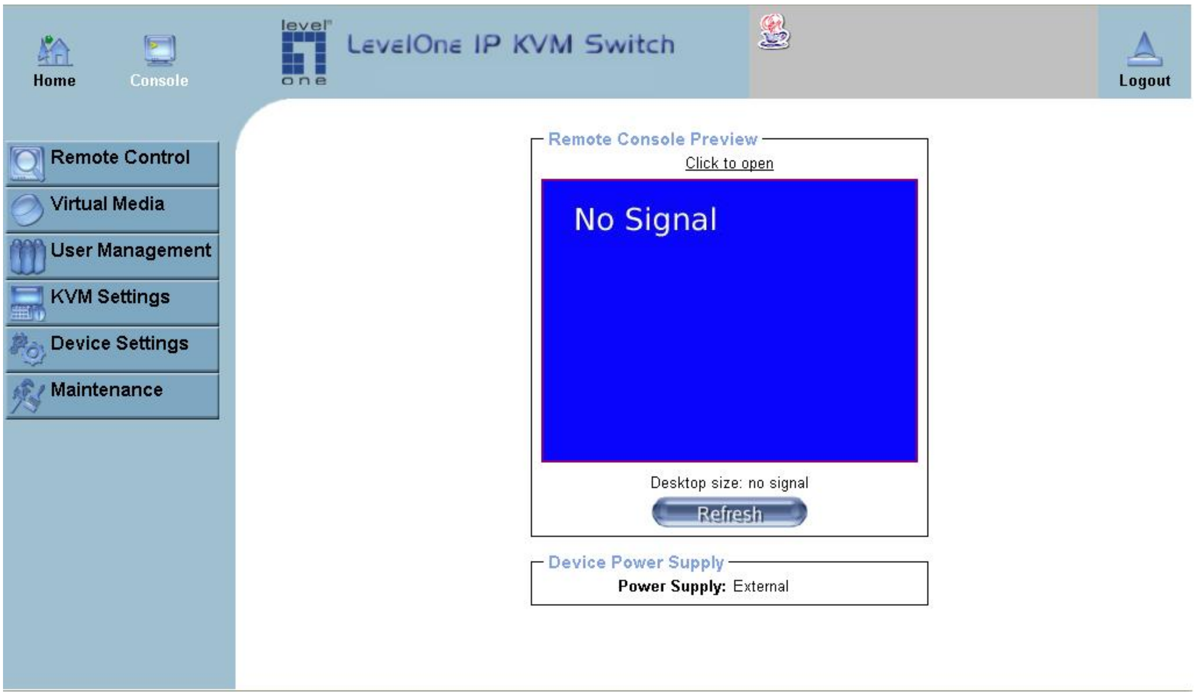
Status line transfer rate

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

5. Menu Options

5.1 Remote Control

5.1.1 KVM Console



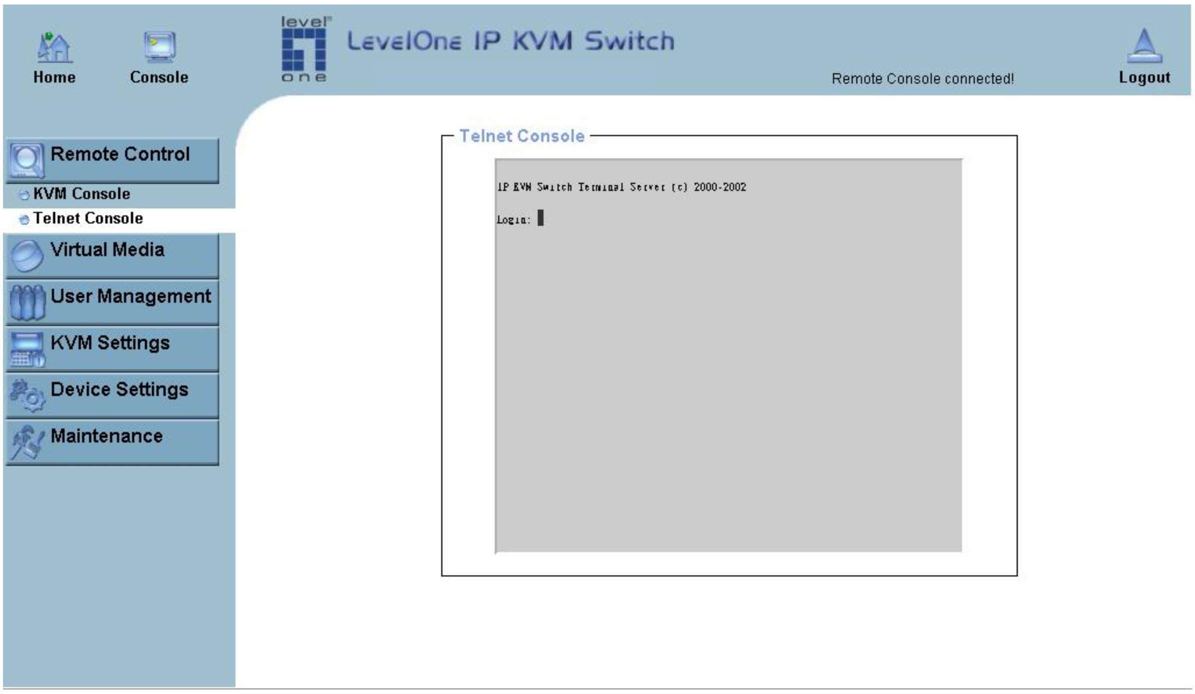
Desktop size: no signal

Power Supply: External

KVM Console

To open the KVM console, either clicks on the menu entry on the left, or on the console picture on the right. To refresh the picture, click on the button “Refresh”.

5.1.2 Telnet Console



```
IP KVM Switch Terminal Server (c) 2000-2002

Login: █
```

Telnet Console

The KVM IP Console Module 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 IP Console Module host machine is using a text mode screen resolution.

Connecting to the KVM IP Console Module is done as usual and as required by the Telnet client, for instance in a UNIX shell: telnet 192.168.1.22

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

After the successfully logged into the KVM IP Console Module a command line will be presented and then user can enter according management commands.

In general, the Telnet interface supports two operation modes: the command line mode and the terminal mode. The command line mode is used to control or display some parameters. In terminal mode the pass-through access to serial port 1 is activated (if the serial settings were configured accordingly). All inputs are redirected to the device on serial port 1 and its answers are displayed on the Telnet interface.

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

help

Displays the list of possible commands

cls

Clears the screen

quit

Exits the current session and disconnects from the client

version

Displays the release information

terminal

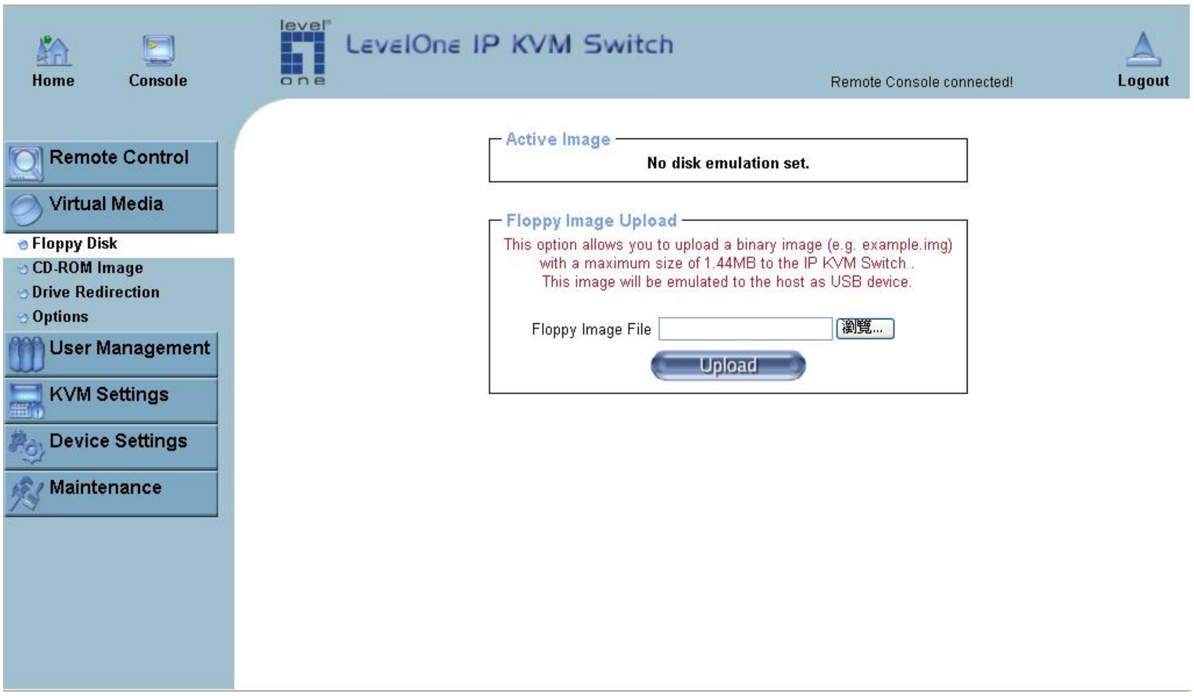
Starts the terminal passthrough mode for serial port 1. The key sequence *esc exit* switches back to the command mode.

5.2 Remote Power

Please refer to “Serial Power Controller - User Manual” for details.

5.3 Virtual Media

5.3.1 Floppy Disk



Remote Console connected!

Active Image

No disk emulation set.

Floppy Image Upload

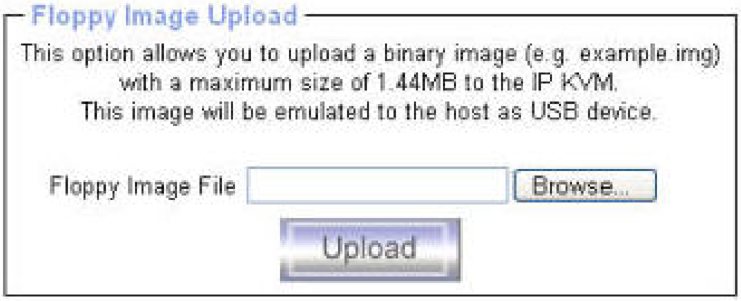
This option allows you to upload a binary image (e.g. example.img) with a maximum size of 1.44MB to the IP KVM Switch . This image will be emulated to the host as USB device.

Floppy Image File

Virtual Floppy Area

Upload a Floppy Image

A certain (floppy) image can be built up in two steps. Click “Browse” button and select the image file.



Floppy Image Upload

This option allows you to upload a binary image (e.g. example.img) with a maximum size of 1.44MB to the IP KVM.
This image will be emulated to the host as USB device.

Floppy Image File

Figure 6-7. Select Image File

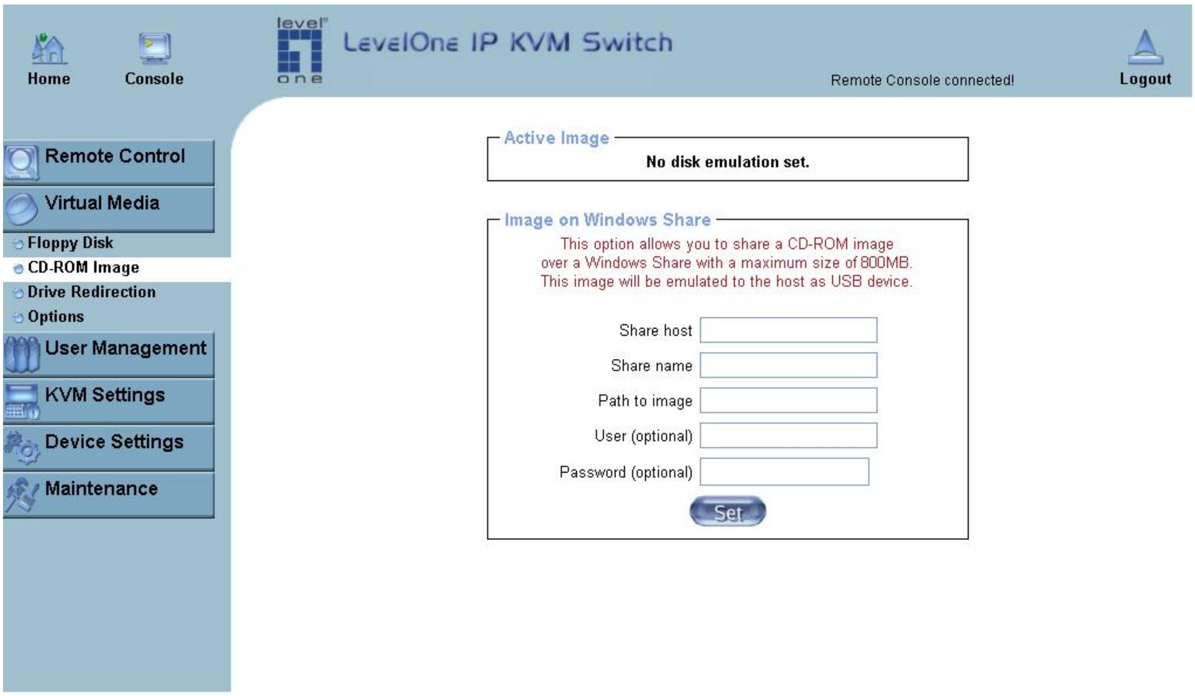
The maximum image size is limited to 1.44MB. For larger image please refer to next section.

Click “Upload” button to upload the chosen image file into the KVM IP Console Module’s onboard memory. This image file is kept in the onboard memory of the KVM IP Console Module until the end of the current session, as user logged out, or initiated a reboot of the KVM IP Console Module.

5.3.2 CD-ROM Image

Use Image on Windows Share (SAMBA)

To include an image from a Windows share, select “CD-ROM” from the submenu.



Remote Console connected!

Active Image

No disk emulation set.

Image on Windows Share

This option allows you to share a CD-ROM image over a Windows Share with a maximum size of 800MB.
This image will be emulated to the host as USB device.

Share host

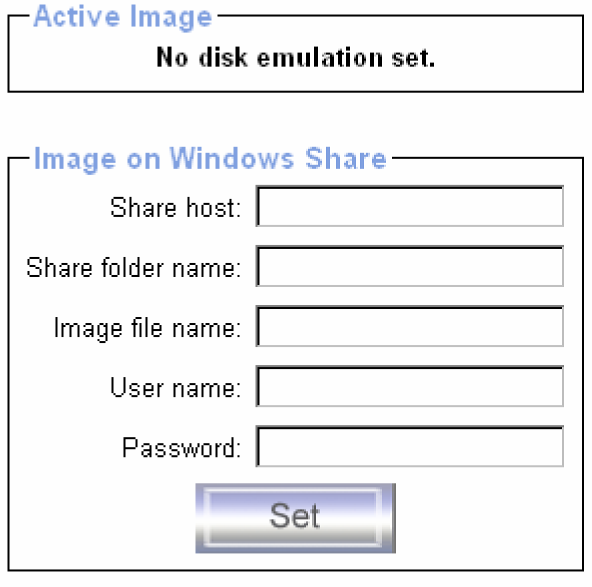
Share name

Path to image

User (optional)

Password (optional)

Selecting CD ROM



Active Image

No disk emulation set.

Image on Windows Share

Share host:

Share folder name:

Image file name:

User name:

Password:

Select Windows Share

The following information has to be given to mount the image properly:

Share host -- The server name or its IP address.

Share folder name -- The name of the share folder to be used.

Image file name -- The name of the image file on the share folder.

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

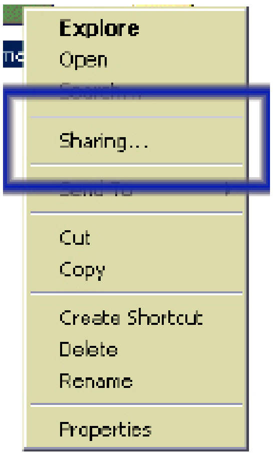
Password -- If necessary, specify the password for the given user name.

To register the specified file image and its location click on the button “Set”.
The specified image file is supposed to be accessible from the KVM IP Console Module. The information above has to be given from the point of view of the KVM IP Console Module. It is important to specify correct IP addresses, and device names. Otherwise, KVM IP Console Module may not be able to access the referenced image file.

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 system administrator for help to complete this task.

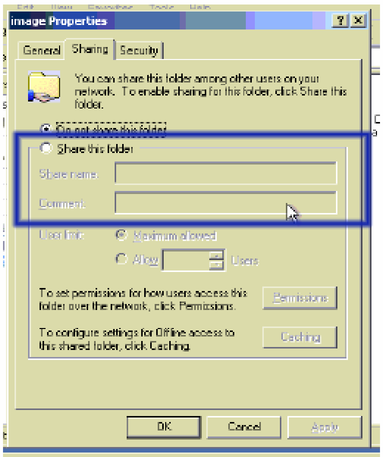
Windows 2000/XP

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



Explorer context menu

Select “Sharing” to open the configuration dialog.



You can share this folder among other users on your network. To enable sharing for this folder, click Share this folder.

● Do not share this folder

○ Share this folder

Share name:

Comment:

User limit: ● Maximum allowed

○ Allow Users

To set permissions for how users access this folder over the network, click Permissions.

To configure settings for Offline access to this shared folder, click Caching.

Share configuration dialog

Adjust the settings for the selected directory. Activate the selected directory as a share. Select “Sharing this folder”.

Choose an appropriate name for the share. User may also add a short description for this folder (input field “Comment”). If necessary, adjust the permissions (button “permissions”). Click “OK” to set the options for this share.

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

If user likes to access the share via SAMBA, SAMBA has to be set up properly. User 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.

Creating an Image

Floppy Images

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).

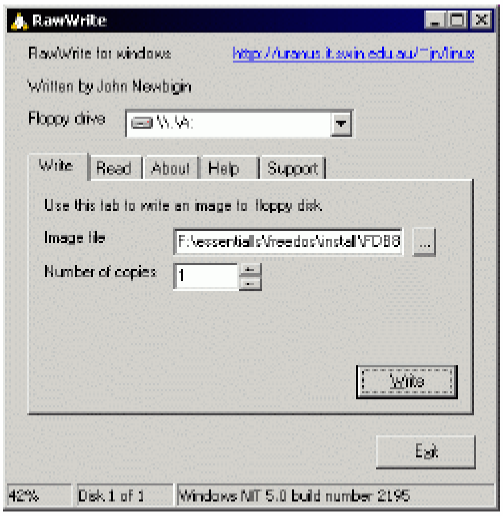
To create a floppy image file, copy the contents of a floppy to a file. You can use the following command:

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.)

MS Windows

User can use the tool "Raw Write for Windows". It is included on the CD ROM shipped with KVM Switch (KVM-0831/1631 & KCM-0831/1631)



RawWrite for windows http://uranus.it.swin.edu.au/~jn/linux

Written by John Newbigin

Floppy drive: \\.\A:

Use this tab to write an image to floppy disk.

Image file: F:\essentials\freedos\install\FDB8

Number of copies: 1

42% | Disk 1 of 1 | Windows NT 5.0 build number 2195

Raw Write for Windows selection dialog

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

For related tools you may have a look at www.fdos.org

CD ROM/ISO Images

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

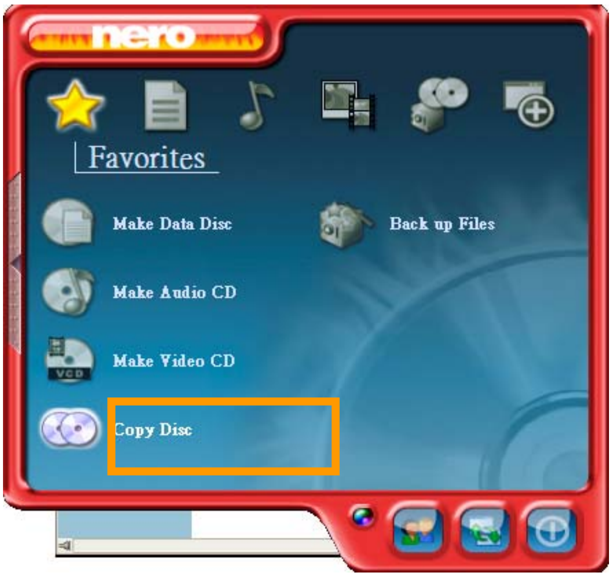
dd [*if=/dev/cdrom*] [*of=/tmp/cdrom.image*]

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.).

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.

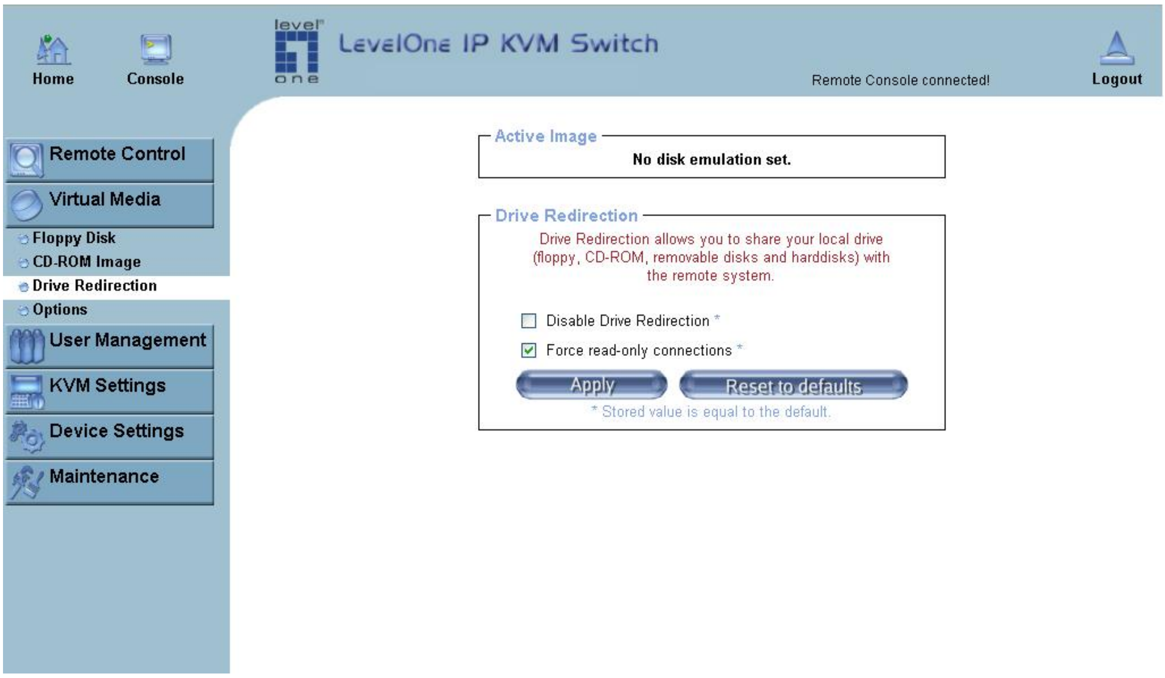
For example, with “Nero” you choose “Copy and Backup”. Then, navigate to the “Copy Disc” section. Select the CD ROM or DVD drive you would like to create an image from. Specify the filename of the image, and save the CD ROM content in that file.



Nero selection dialog

5.3.3 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 the local disc.



Active Image

No disk emulation set.

Drive Redirection

Drive Redirection allows you to share your local drive (floppy, CD-ROM, removable disks and harddisks) with the remote system.

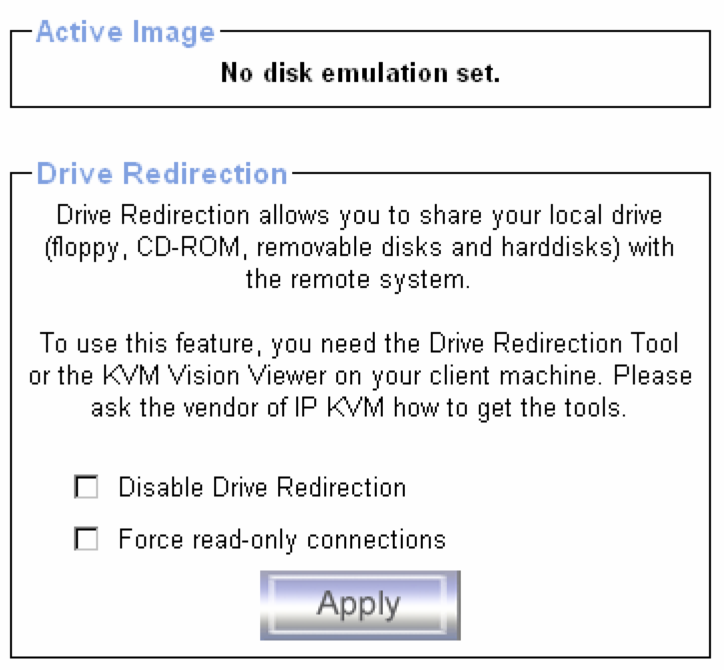
☐ Disable Drive Redirection *

☑ Force read-only connections *

* Stored value is equal to the default.

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.



Active Image

No disk emulation set.

Drive Redirection

Drive Redirection allows you to share your local drive (floppy, CD-ROM, removable disks and harddisks) with the remote system.

To use this feature, you need the Drive Redirection Tool or the KVM Vision Viewer on your client machine. Please ask the vendor of IP KVM how to get the tools.

☐ Disable Drive Redirection

☐ Force read-only connections

Disable Drive Redirection

If enabled the Drive Redirection is switched off.

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.

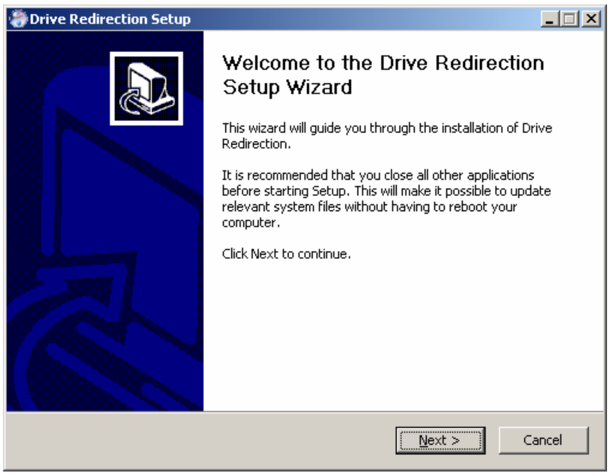
Click **Apply** to submit your changes.

There are two methods of Drive Redirections:

1. **External Drive Redirection Utility**
2. **Built-in Java Drive Redirection function in Remote Console**

5.3.3.1 Drive Redirection Utility Installation

Please follow the Drive Redirection Setup Wizard step by step to install the driver from the attached CD ROM.



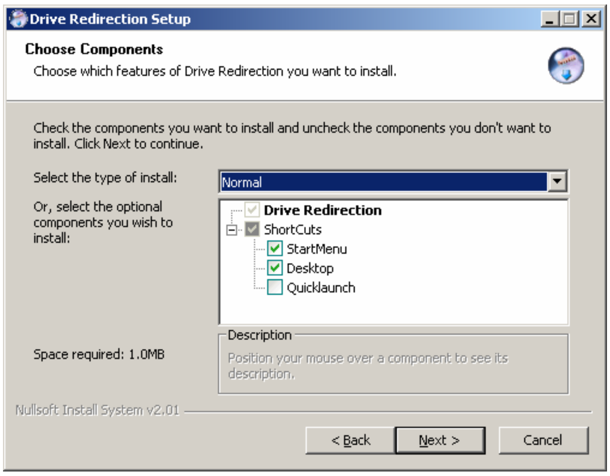
Drive Redirection Setup

Welcome to the Drive Redirection Setup Wizard

This wizard will guide you through the installation of Drive Redirection.

It is recommended that you close all other applications before starting Setup. This will make it possible to update relevant system files without having to reboot your computer.

Click Next to continue.



Drive Redirection Setup

Choose Components

Choose which features of Drive Redirection you want to install.

Check the components you want to install and uncheck the components you don't want to install. Click Next to continue.

Select the type of install: Normal

Or, select the optional components you wish to install:

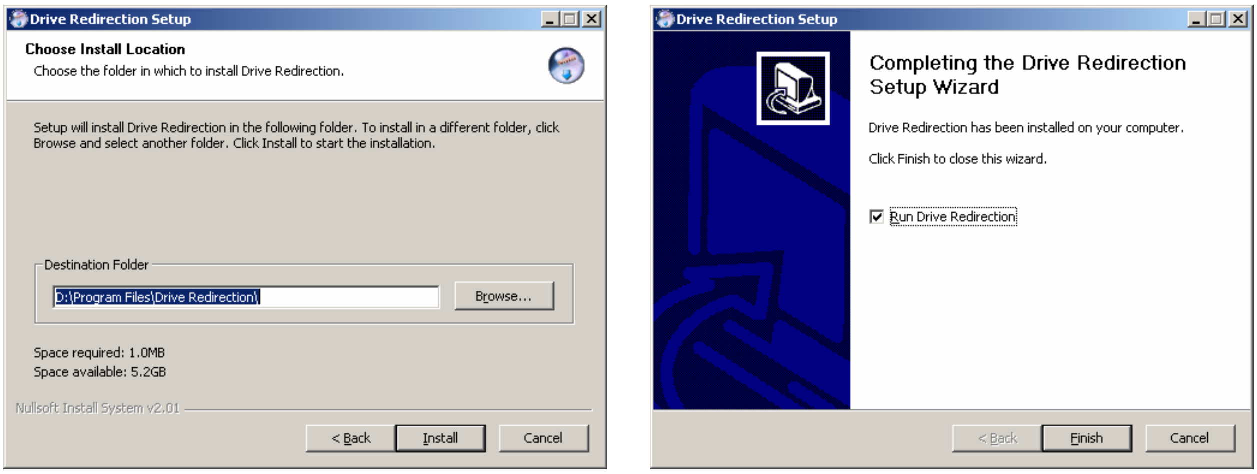
- ☑ Drive Redirection
- ☑ ShortCuts
  - ☑ StartMenu
  - ☑ Desktop
  - ☐ Quicklaunch

Space required: 1.0MB

Description

Position your mouse over a component to see its description.

Nullsoft Install System v2.01



Drive Redirection Setup

Choose Install Location

Choose the folder in which to install Drive Redirection.

Setup will install Drive Redirection in the following folder. To install in a different folder, click Browse and select another folder. Click Install to start the installation.

Destination Folder: D:\Program Files\Drive Redirection\

Space required: 1.0MB
Space available: 5.2GB

Nullsoft Install System v2.01

Drive Redirection Setup

Completing the Drive Redirection Setup Wizard

Drive Redirection has been installed on your computer.

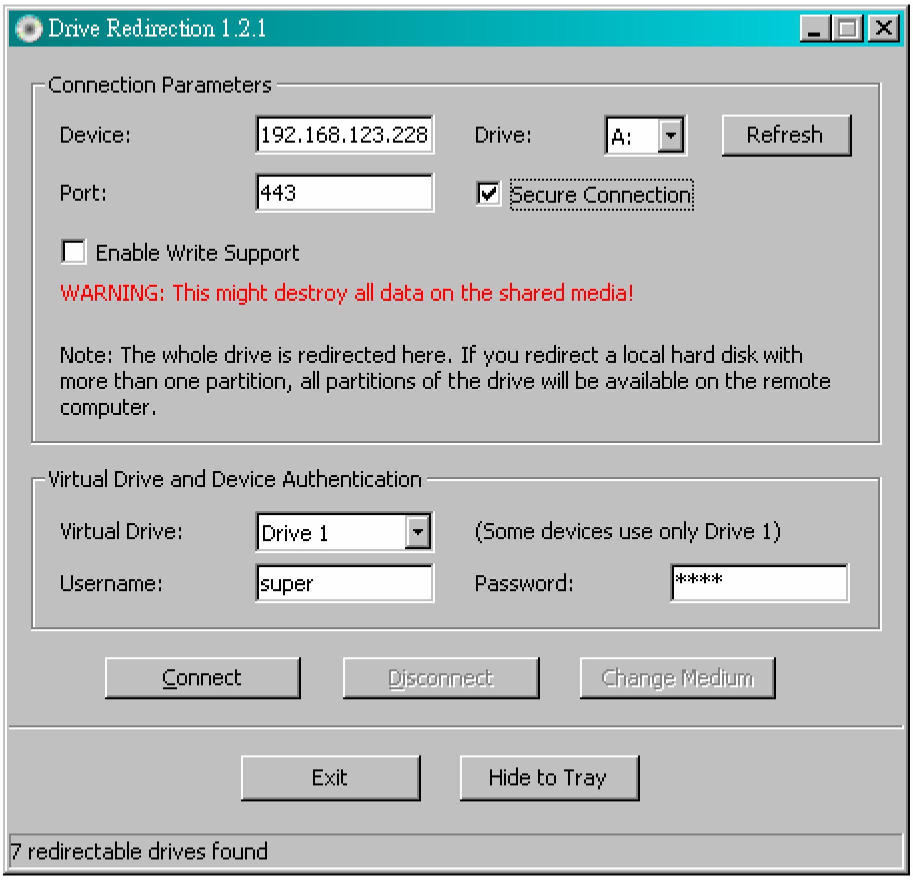
Click Finish to close this wizard.

☑ Run Drive Redirection

Drive Redirection Setup

Drive Redirection Settings

Start Drive Redirection



Drive Redirection 1.2.1

Connection Parameters

Device: 192.168.123.228

Drive: A:

Port: 443

☑ Secure Connection

☐ Enable Write Support

WARNING: This might destroy all data on the shared media!

Note: The whole drive is redirected here. If you redirect a local hard disk with more than one partition, all partitions of the drive will be available on the remote computer.

Virtual Drive and Device Authentication

Virtual Drive: Drive 1

(Some devices use only Drive 1)

Username: super

Password: ****

7 redirectable drives found

Drive Redirection dialog

Drive to redirect

Device
This is the address (either the DNS name or the IP address) of the KVM IP Console Module user would like to connect to.

Drive
The local drive you want to share with the remote computer, which could be Floppy disc, CD-ROMs, USB-Sticks and hard drives.

Port
This is the network port. By default, KVM IP Console Module uses the remote console port (#443) here. User may change this value, if user changed the remote console port in the KVM IP Console Module's network settings.

Secure Connection
Enable this box to establish a secure connection via SSL. This will maximize the security but may reduce the connection speed.

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

Note

Drive Redirection is only possible with Windows 2000 and above.

The Drive Redirection works on a low SCSI level and the SCSI protocol cannot recognize partitions; therefore the whole drive selected will be shared instead of any particular partition.

While connecting to a legacy KVM switch, please select PS/2 mouse fore Keyboard/Mouse setting from webpage. Otherwise user may not be able to use HotKeys.

Navigation Buttons

Connect/Disconnect

To establish the drive redirection, please press the **Connect** button once. If all the settings are correct, the status bar displays that the connection has been established, the Connect button is disabled and the Disconnect button is enabled.

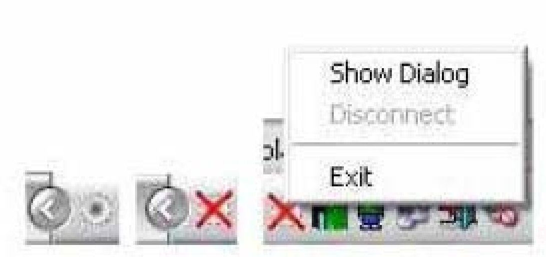
On an error, the status line shows the error message. The drive redirection software tries to lock the local drive before it is redirected. That means that it tries to prevent the local operating system from accessing the drive as long as it is redirected. This may also fail, especially if a file on 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.

With the **Disconnect** button, a connection via Drive Redirection connection is stopped.

Exit/Hide

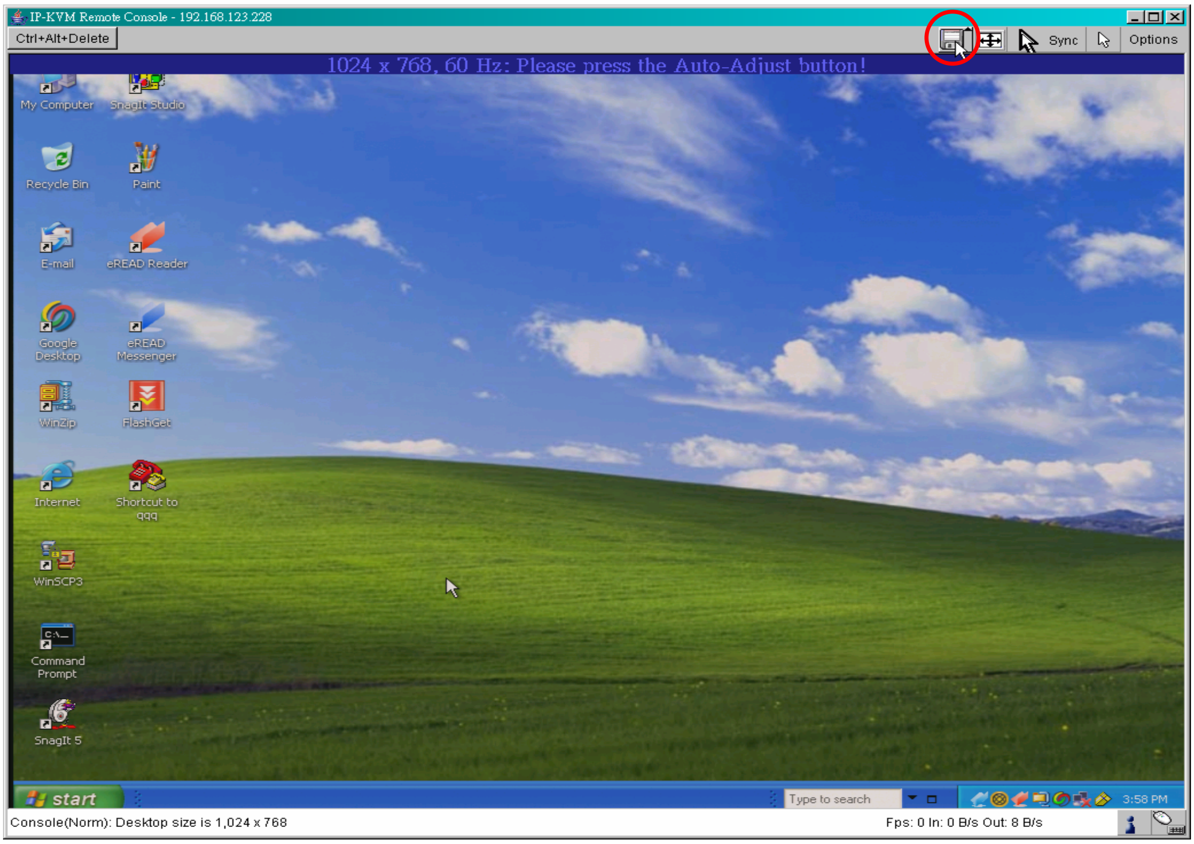
If the **Exit** button is pressed, the Drive Redirection software is closed. If a Drive Redirection Connection is active, the connection will be closed before the application terminates.

Using the Hide to Tray button the application is hidden, but not terminated completely. That means that an active connection will be kept active until it is closed explicitly. You can access the software by its tray icon. The tray icon also shows whether a connection is established or not. A double click on the icon shows the application window, or with a right click you may access a small menu



5.3.3.2 Built-in Java Drive Redirection

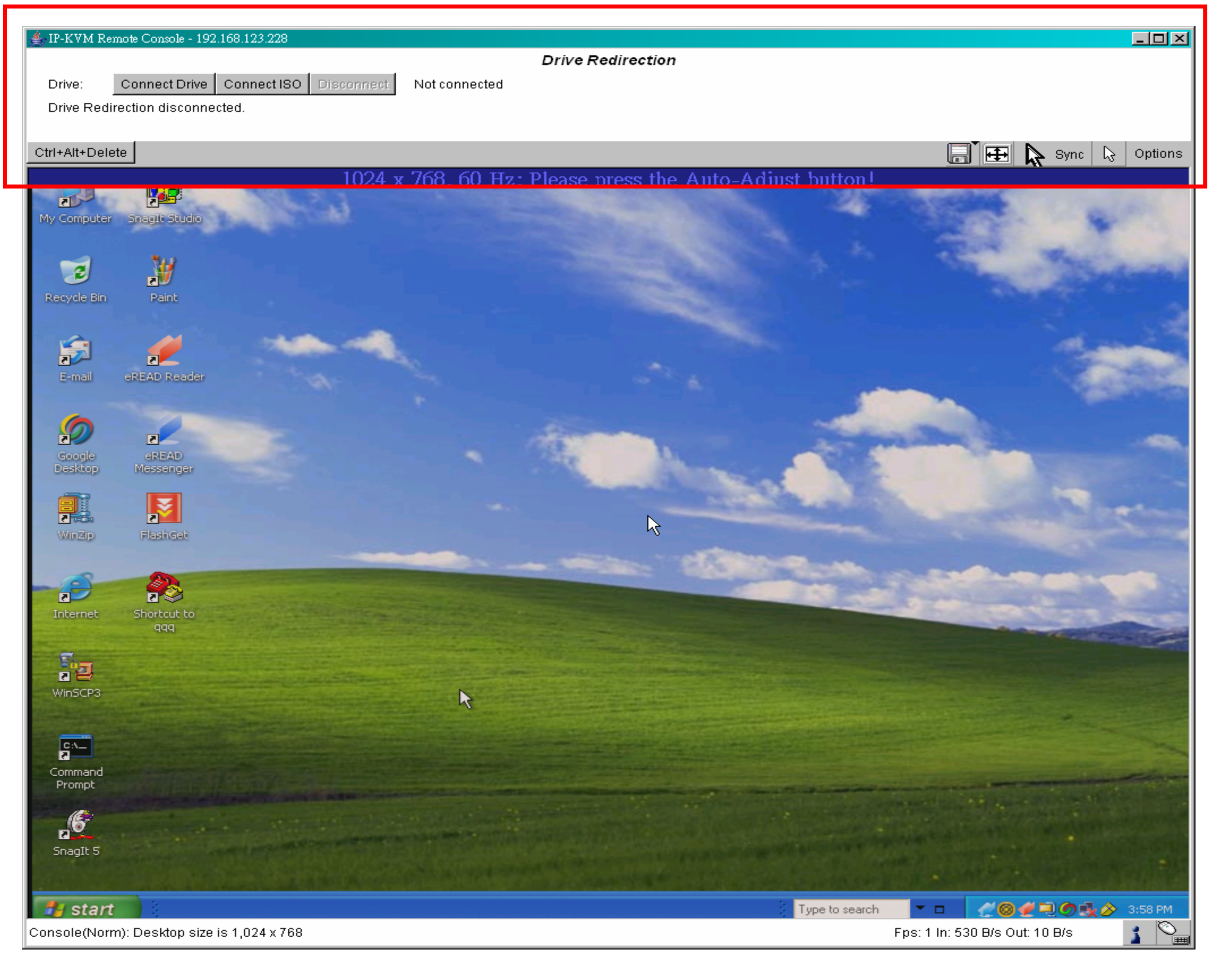
1. Run Remote Control > KVM Console.
2. Click “Floppy” icon



1024 x 768, 60 Hz: Please press the Auto-Adjust button!

Console(Norm): Desktop size is 1,024 x 768

Fps: 0 In: 0 B/s Out: 8 B/s



IP-KVM Remote Console - 192.168.123.228

Drive Redirection

Drive: Connect Drive | Connect ISO | Disconnect   Not connected

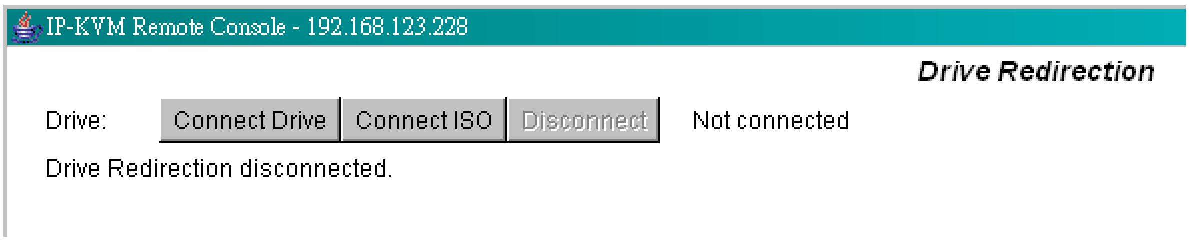
Drive Redirection disconnected.

1024 x 768, 60 Hz: Please press the Auto-Adjust button!

Console(Norm): Desktop size is 1,024 x 768

Fps: 1 In: 530 B/s Out: 10 B/s

3. Click **Connect Drive** or **Connect ISO**



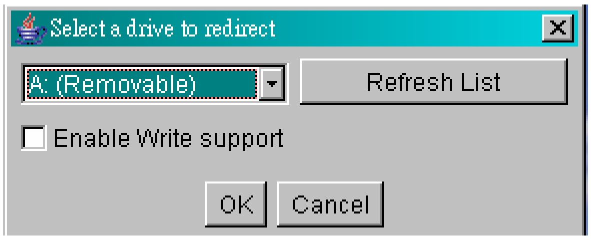
IP-KVM Remote Console - 192.168.123.228

Drive Redirection

Drive: Connect Drive | Connect ISO | Disconnect   Not connected

Drive Redirection disconnected.

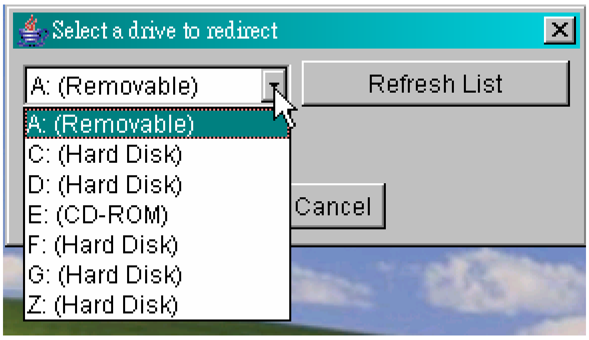
4. Select a drive to redirect (if Connect Drive)



Select a drive to redirect

A: (Removable)

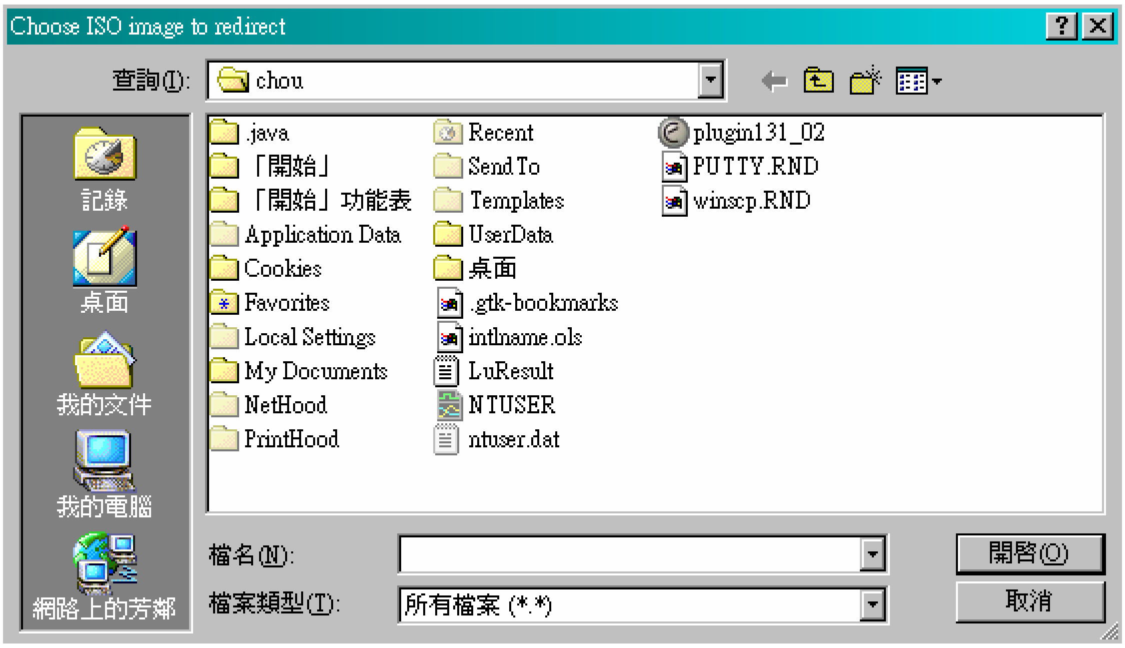
□ Enable Write support



Select a drive to redirect

A: (Removable)
C: (Hard Disk)
D: (Hard Disk)
E: (CD-ROM)
F: (Hard Disk)
G: (Hard Disk)
Z: (Hard Disk)

5. Select a ISO image to redirect (if Connect ISO)



Choose ISO image to redirect

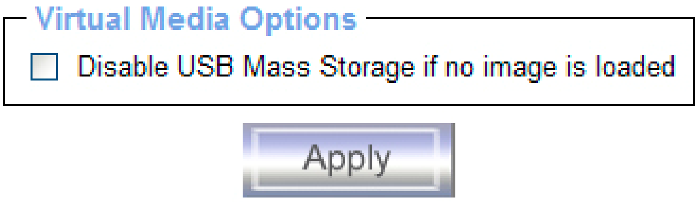
查詢(I): chou

.java
「開始」
「開始」功能表
Application Data
Cookies
Favorites
Local Settings
My Documents
NetHood
PrintHood
Recent
Send To
Templates
UserData
桌面
.gtk-bookmarks
intlname.ols
LuResult
NTUSER
ntuser.dat
plugin131_02
PUTTY.RND
winscp.RND

檔名(N):

檔案類型(T): 所有檔案 (*.*)

5.3.4 Options



Virtual Media Options

□ Disable USB Mass Storage if no image is loaded

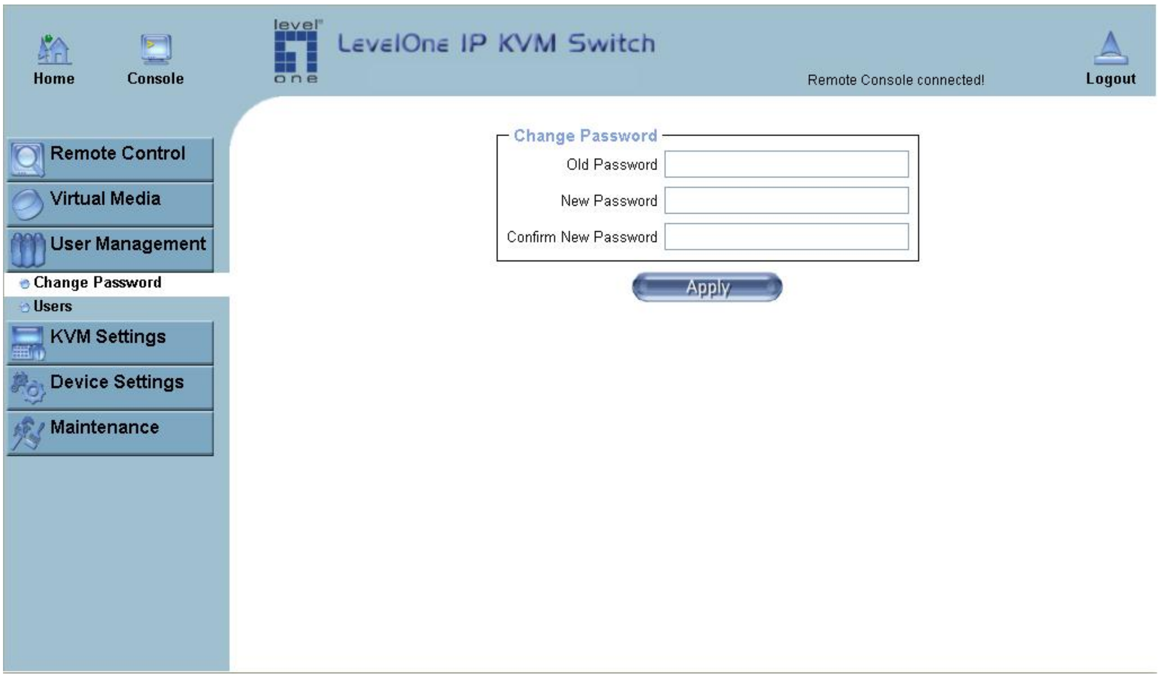
USB mass storage option

Set this option to disable the mass storage emulation (and hide the virtual drive) if no image file is currently loaded. 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.

To set this option, press the button “Apply”.

5.4 User Management

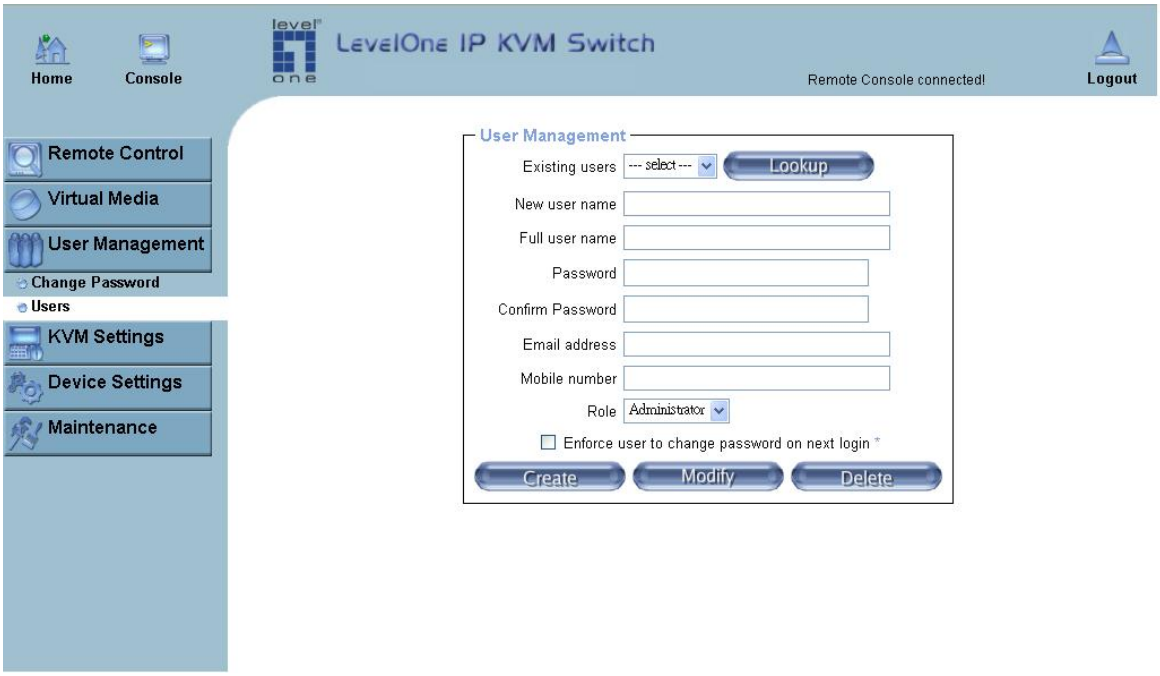
5.4.1 Change Password



Set password

To change the password, enter the new password in the upper entry field. Retype the password in the field below. Click “Apply” to submit your changes.

5.4.2 Users and Groups



Set User

The KVM IP Console Module 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 KVM IP Console Module 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 KVM IP Console Module.

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”) - either an administrator, or an regular user. Choose the desired role from the selection box.

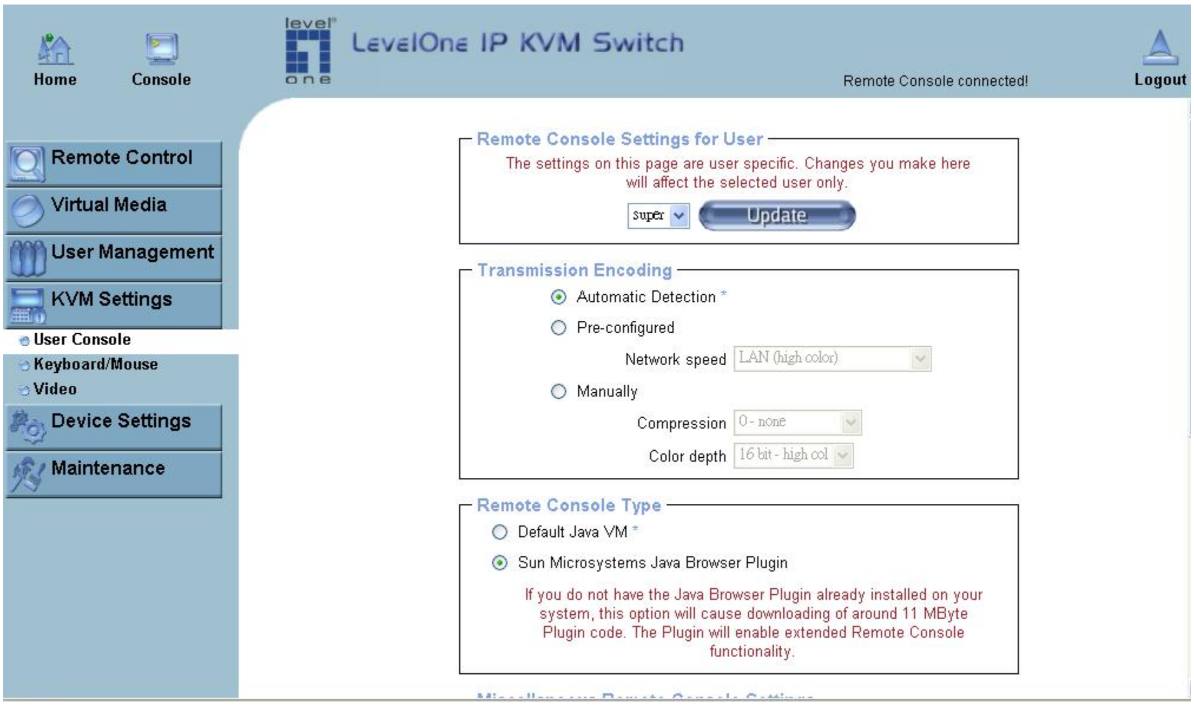
To create an user press the button “Create”. The button “Modify” changes the dis- played user settings. To delete an user press the button “Delete”.

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

5.5 KVM Settings

5.5.1 User Console

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



Remote Console Settings for User

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

super ▾ 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.

User Console Settings (Part 1)

User select box

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

Transmission Encoding

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

Automatic detection

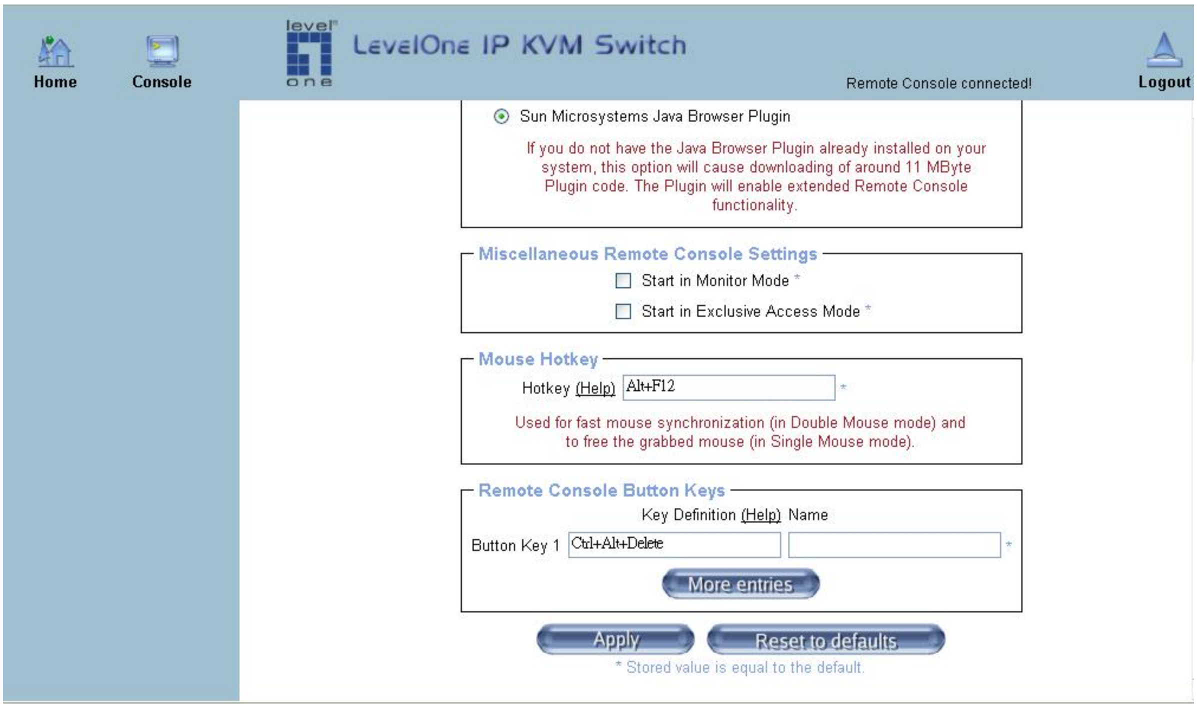
The encoding and the compression level is determined automatically from the available bandwidth and the current content of the video image.

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 KVM IP Console Module and the Remote Console will be compressed in order to save bandwidth. Since high compression rates consum more computing power of KVM IP Console Module, they should not be used while several users are accessing the KVM IP Console Module 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 connected!

● 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	Ctrl+Alt+Delete	*

More entries

Apply Reset to defaults

* Stored value is equal to the default.

User Console Settings (Part 2)

Remote Console Type

Specifies, which Remote Console Viewer to use.

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

Sun Microsystems Java Browser Plugin
Instructs the web browser of your administration system to use the JVM of Sun Microsystems. The JVM in the browser is used to run the code for the Remote Console

window, which is actually a Java Applet. If you check this box for the first time on your administration system and the appropriate Java plug-in is not already installed on your system, it will be downloaded and installed automatically. However, in order to make the installation possible, you still need to answer the according dialogs with “yes” . The download volume is around 11 Mbytes. The advantage of downloading Sun's JVM lays in providing a stable and identical Java Virtual Machine across different platforms. The Remote Console software is optimized for this JVM versions and offers wider range of functionality when run in SUN's JVM. Please make sure that you are installing Sun JVM 1.4.2 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 user 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.

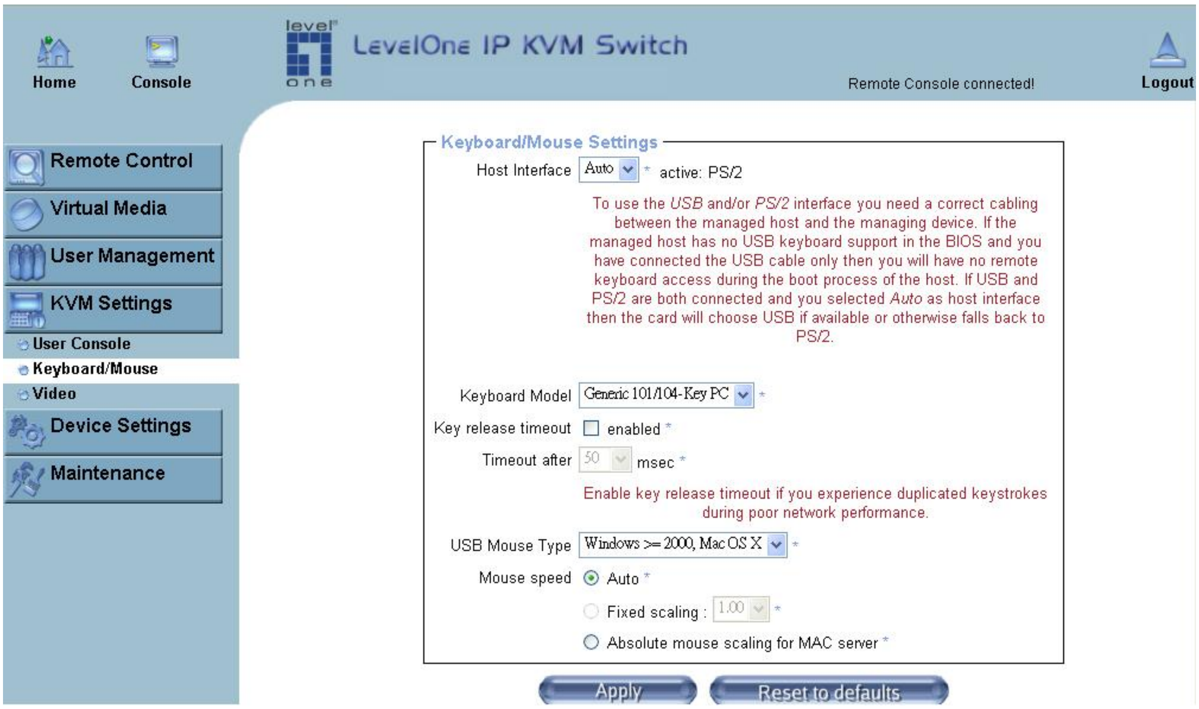
Remote Console Button Keys
Button Keys allow simulating keystrokes on the remote system that cannot be generated locally. The reason for this might be a missing key or the fact, that the local operating system of the Remote Console is unconditionally catching this keystroke already. Typical examples 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.

5.5.2 Keyboard/Mouse



Keyboard/Mouse Settings

Host Interface: Auto * active: PS/2

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

Keyboard Model: Generic 101/104-Key PC *

Key release timeout: □ enabled *

Timeout after: 50 msec *

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

USB Mouse Type: Windows >= 2000, Mac OS X *

Mouse speed: ● Auto *
○ Fixed scaling : 1.00 *
○ Absolute mouse scaling for MAC server *

Keyboard and Mouse Settings

Host Interface

Enables a certain interface the mouse is connected to. You can choose between “Auto” for automatic detection, “USB” for an USB mouse, and “PS/2” for a PS/2 mouse.

Note

To use the USB and/or PS/2 interface, user need to have a correct cabling between the managed host and the managing device. If the managed host has no USB keyboard support in the BIOS, then there will be no remote keyboard access during the boot process of the host. If the USB and PS/2 are both connected and user also selected “Auto” as the host interface, it will then auto detect USB if it is available, or otherwise it will falls back to PS/2.

To get USB remote keyboard access during the boot process of the host, the following conditions must be fulfilled:

Host BIOS must have USB keyboard support

USB cable must be connected or must be selected in the Host interface option

PS/2 Keyboard Model

Enables a certain keyboard layout. User may 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.

USB Mouse Type

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

Mouse Speed

Auto mouse speed

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

Fixed mouse speed

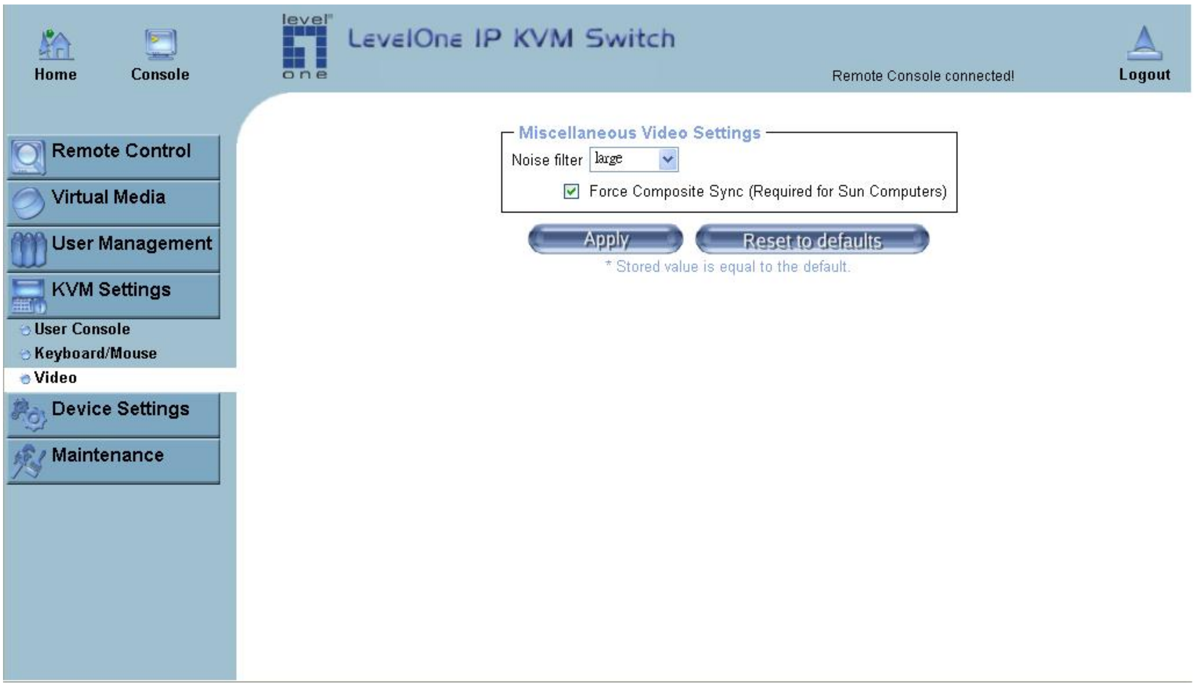
Use a direct translation of mouse movements between the local and the remote pointer.

User 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 KVM IP Console Module is not functioning under this setting.

Absolute mouse scaling for MAC server

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

5.5.3 Video



Miscellaneous Video Settings

Noise filter large

☑ Force Composite Sync (Required for Sun Computers)

* Stored value is equal to the default.

Video Settings

Miscellaneous Video Settings

Noise filter

This option defines how the KVM IP Console Module 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)

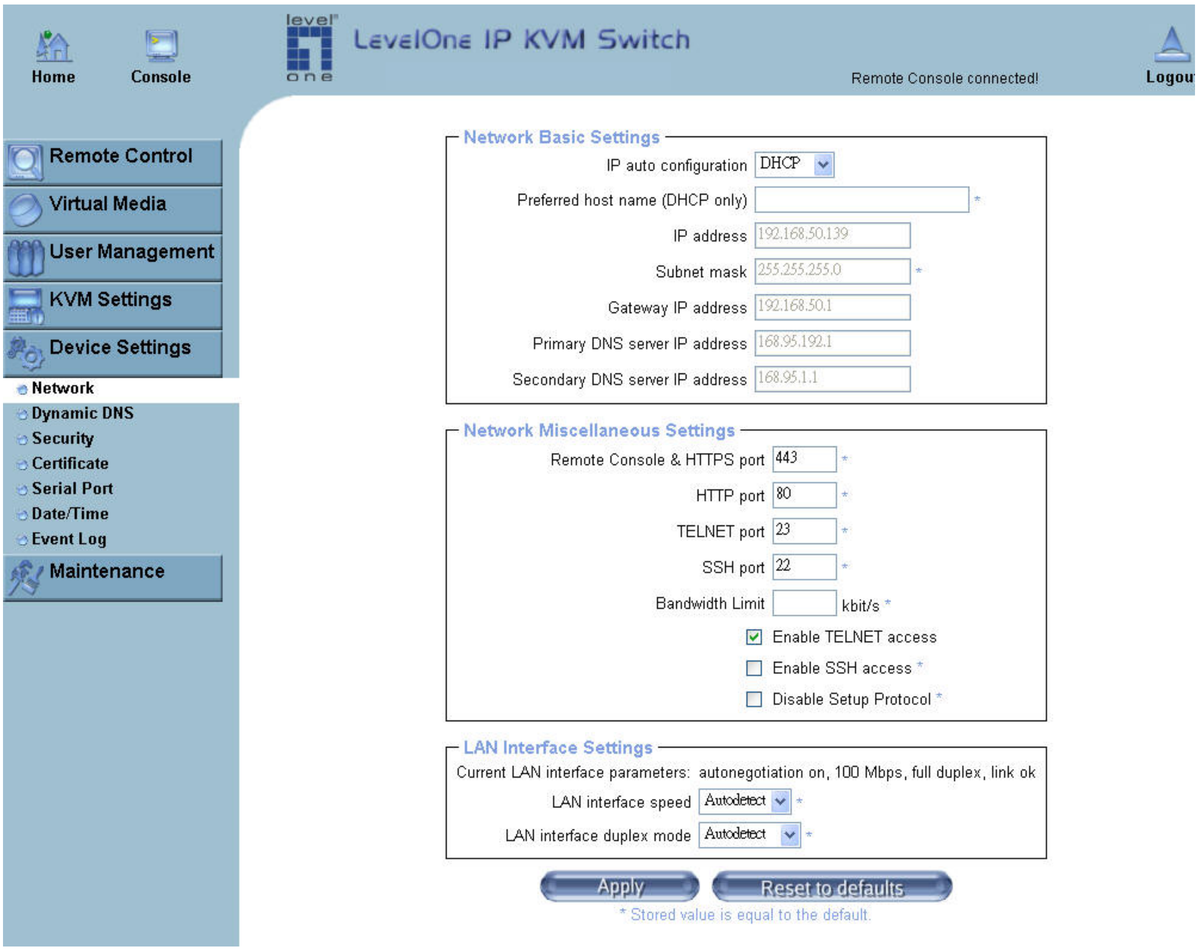
When connecting the device directly to legacy Sun computer (with composite sync as the video output, it may be possible that KVM IP Console Module don’t recognize the composite sync automatically. To support signal transmission from a Sun machine, enable this option. If not enabled the picture of the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

To set the options, click on the button “Apply”.

5.6 Device Settings

5.6.1 Network

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



Network Basic Settings

IP auto configuration	DHCP
Preferred host name (DHCP only)	*
IP address	192.168.50.139
Subnet mask	255.255.255.0 *
Gateway IP address	192.168.50.1
Primary DNS server IP address	168.95.192.1
Secondary DNS server IP address	168.95.1.1

Network Miscellaneous Settings

Remote Console & HTTPS port	443 *
HTTP port	80 *
TELNET port	23 *
SSH port	22 *
Bandwidth Limit	kbit/s *

☑ Enable TELNET access

□ Enable SSH access *

□ Disable Setup Protocol *

LAN Interface Settings

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

LAN interface speed	Autodetect *
LAN interface duplex mode	Autodetect *

* Stored value is equal to the default.

Network Settings

Warning

The initial IP configuration is usually done directly at the host system using the special procedure described in Table 4-1.

Note

Changing the network settings of the KVM IP Console Module might result in losing connection. In case user change the settings remotely, please make sure that all the values are correct and may still have an option to access the KVM IP Console Module.

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

Preferred host name

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

IP address
IP address in the usual dot notation.

Subnet Mask
The net mask of the local network.

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

Primary DNS Server IP Address
IP address of the primary Domain Name Server in dot notation. This option may be left empty, however the KVM IP Console Module will not be able to perform name resolution.

Secondary DNS Server IP Address
IP address of the secondary Domain Name Server in dot notation. It will be used in case the Primary DNS Server cannot be contacted.

Remote Console And HTTPS port
Port number at which the KVM IP Console Module's Remote Console server and HTTPS server are listening. If left empty the default value will be used.

HTTP port
Port number at which the KVM IP Console Module's HTTP server is listening. If left empty the default value will be used.

Telnet port
Port number at which the KVM IP Console Module's Telnet server is listening. If left empty the default value will be used.

SSH port
Listing the Port number at which the KVM IP Console Module SSH (Secure SHell) server is using. If left empty the default value (port 22) will be used.

Bandwidth limitation
The maximum network traffic generated through the KVM IP Console Module ethernet device. Value in Kbit/s.

Enable Telnet access

Enables the Telnet function.

Enable SSH access

Enables the SSH (Secure SHell) function.

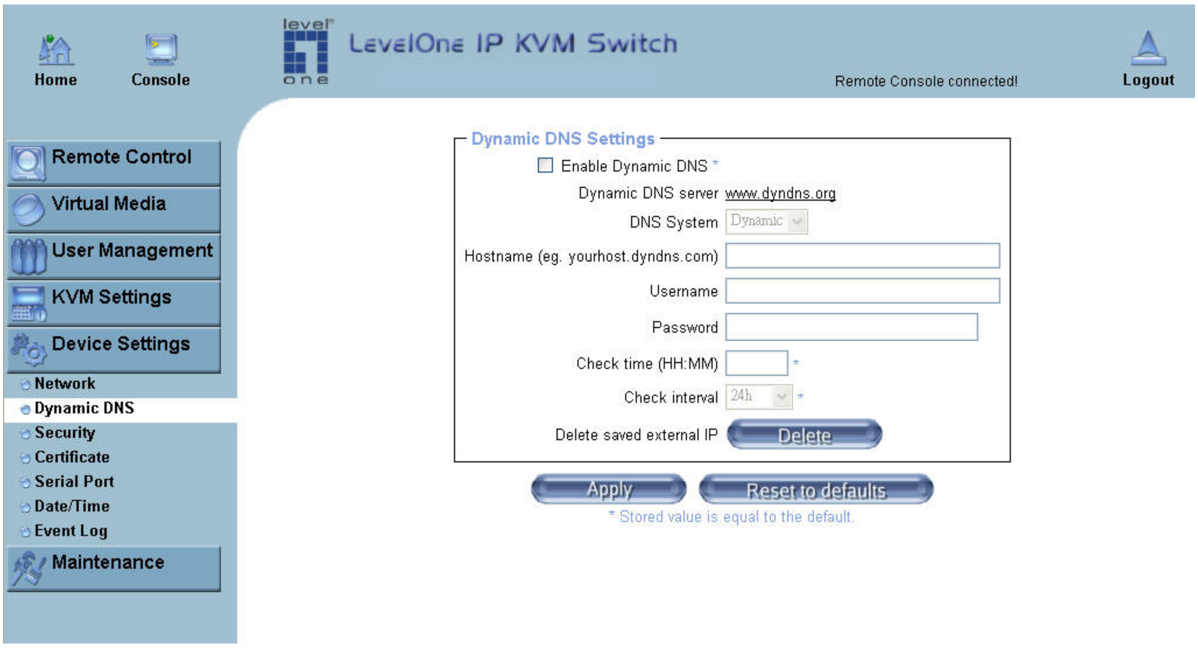
Disable Setup Protocol

Enable this option to exclude the KVM IP Console Module from the setup protocol. Setup protocol is a proprietary layer-2 MAC-based protocol to allow some configuration software to detect KVM IP Console Module devices in the network, even without IP address, and then config network related settings to KVM IP Console Module.

LAN Interface Settings

The “Autodetect” will set the ethernet speed to the fastest possible value supported by both endpoints of the link. For example, if you use a 10M/half duplex HUB, this speed will be auto-selected. If this option does not work with some network device (HUB, switches, and routers), you can set the Ethernet interface speed of KVM IP Console Module manually to the values as supported by the network device.

5.6.2 Dynamic DNS



Dynamic DNS Settings

☐ Enable Dynamic DNS *

Dynamic DNS server www.dyndns.org

DNS System Dynamic

Hostname (eg. yourhost.dyndns.com)

Username

Password

Check time (HH:MM) *

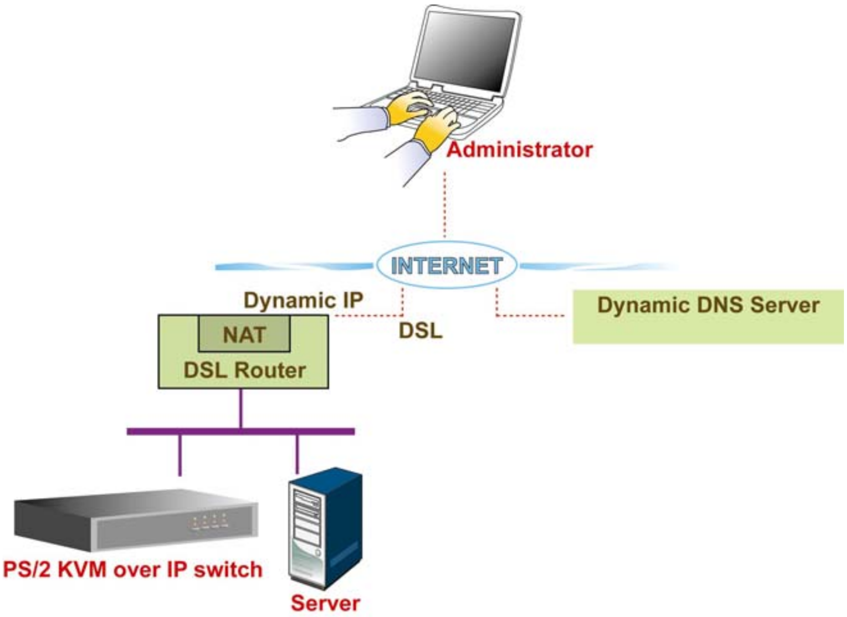
Check interval 24h *

Delete saved external IP

* Stored value is equal to the default.

Dynamic DNS

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



Dynamic DNS Scenario

The KVM IP Console Module 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 KVM IP Console Module 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 belonging to his card.

The administrator has to register an KVM IP CONSOLE MODULE 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 KVM IP Console Module.

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

- Make sure that the LAN interface of the KVM IP Console Module is properly configured.
- Enter the Dynamic DNS Settings configuration dialog as shown in above 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 KVM IP Console Module 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.

Hostname

This is the hostname of the KVM IP Console Module 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

User must register the username during this manual registration with the Dynamic DNS Server. Spaces are not allowed in the Nickname.

Password

User must use the password during this manual registration with the Dynamic DNS Server.

Check time

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

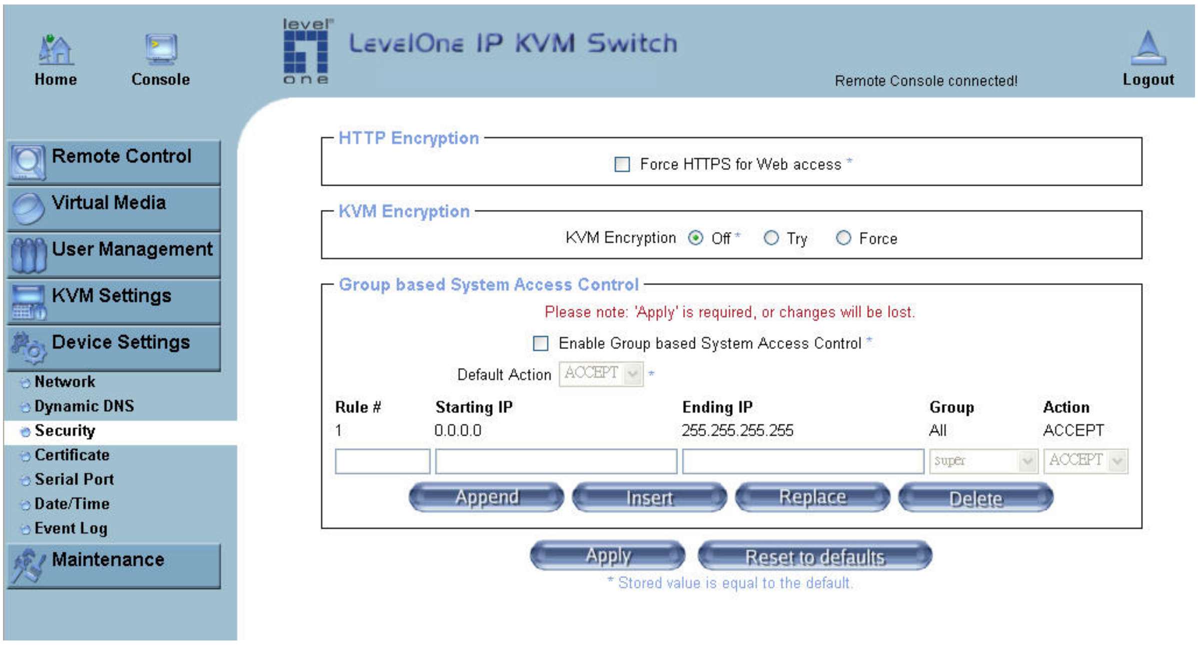
Check interval

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

Note

The KVM IP Console Module has its own independent real time clock.
Make sure the time setting of the KVM IP Console Module is correct.

5.6.3 Security



HTTP Encryption

□ Force HTTPS for Web access *

KVM Encryption

KVM Encryption ● Off * ○ Try ○ Force

Group based System Access Control

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

□ Enable Group based System Access Control *

Default Action ACCEPT *

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

* Stored value is equal to the default.

Device Security

Force HTTPS

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

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

KVM encryption

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

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

Group-based System Access Control

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

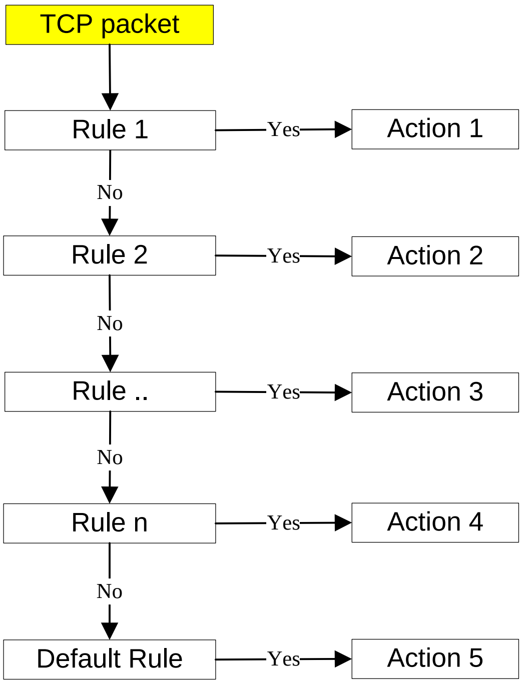
Chain rule

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

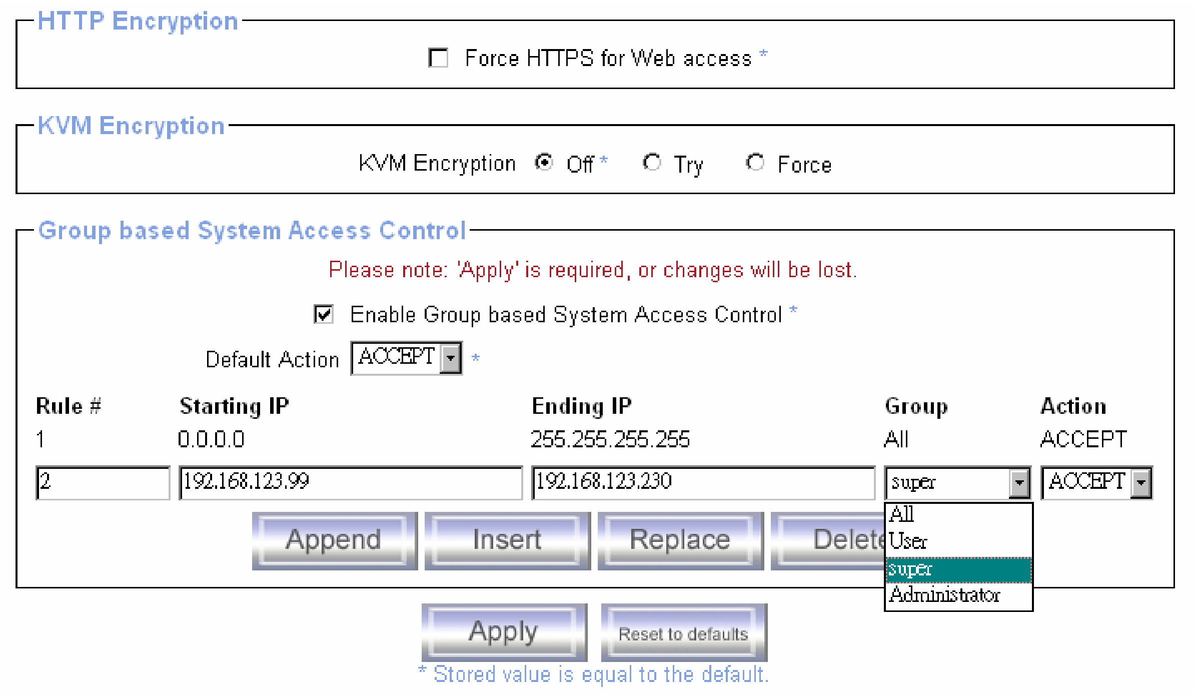
- ACCEPT : access allowed
- DROP : access not allowed

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

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



Check the “Enable Group based System Access Control” to edit the rules
Users can add a new IP filtering rule by setting the properties at adding line by **Append** or **Insert**. User can remove a rule by **Remove** or **Delete**.



HTTP Encryption

□ Force HTTPS for Web access *

KVM Encryption

KVM Encryption ● Off * ○ Try ○ Force

Group based System Access Control

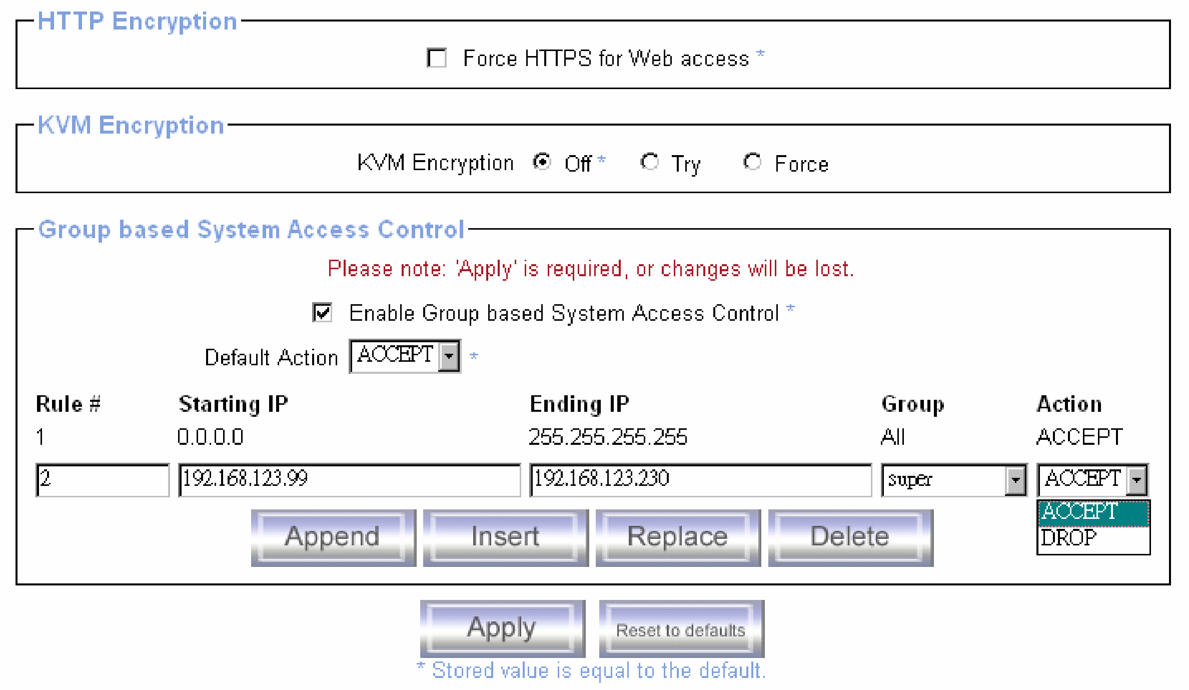
Please note: 'Apply' is required, or changes will be lost.

☑ Enable Group based System Access Control *

Default Action ACCEPT *

Rule #	Starting IP	Ending IP	Group	Action
1	0.0.0.0	255.255.255.255	All	ACCEPT
2	192.168.123.99	192.168.123.230	super	ACCEPT

* Stored value is equal to the default.



HTTP Encryption

□ Force HTTPS for Web access *

KVM Encryption

KVM Encryption ● Off * ○ Try ○ Force

Group based System Access Control

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

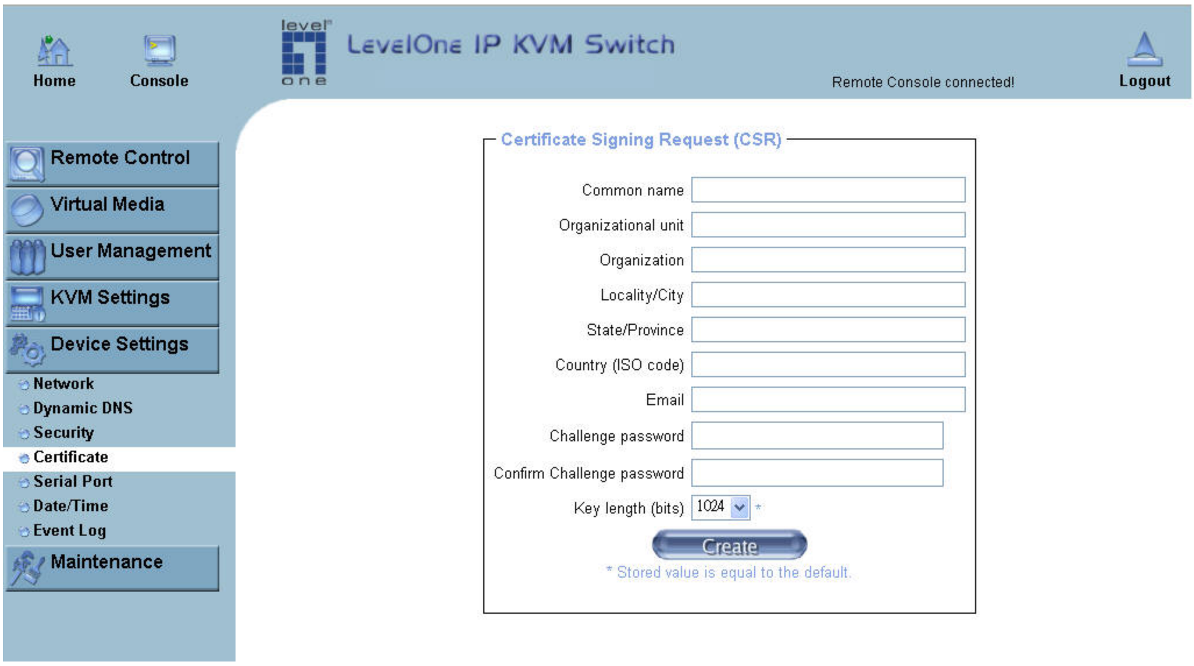
☑ Enable Group based System Access Control *

Default Action ACCEPT *

Rule #	Starting IP	Ending IP	Group	Action
1	0.0.0.0	255.255.255.255	All	ACCEPT
2	192.168.123.99	192.168.123.230	super	ACCEPT

* Stored value is equal to the default.

5.6.4 Certificate



Certificate Signing Request (CSR)

Common name	
Organizational unit	
Organization	
Locality/City	
State/Province	
Country (ISO code)	
Email	
Challenge password	
Confirm Challenge password	
Key length (bits)	1024 *

Create

* Stored value is equal to the default.

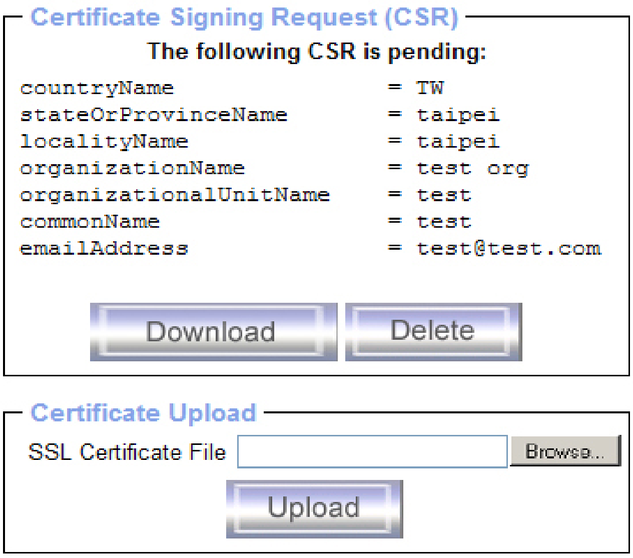
Certificate Settings

The KVM IP Console Module uses the Secure Socket Layer (SSL) protocol for any encrypted network traffic between itself and a connected client. During the connection establishment the KVM IP Console Module has to expose its identity to a client using a cryptographic certificate. The default certificate comes with KVM IP Console Module 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 KVM IP Console Module. In order to do that, the KVM IP Console Module 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 KVM IP Console Module:

- Create a SSL Certificate Signing Request using the panel shown in Figure 6-28. 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 (see Figure 6-29).
- 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 KVM IP Console Module using the “Upload” button as shown in below figure.



Certificate Signing Request (CSR)

The following CSR is pending:

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

Certificate Upload

SSL Certificate File

SSL Certificate Upload

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

Note

If user destroys the CSR on the KVM IP Console Module, please notice that there is no way to get it back. If user deleted it by mistake, please perform the three steps as described above.

Common name

This is the network name of the KVM IP Console Module 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 KVM IP Console Module 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 KVM IP Console Module is accessed using HTTPS.

Organizational unit

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

Organization

The name of the organization to which the KVM IP Console Module 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.)

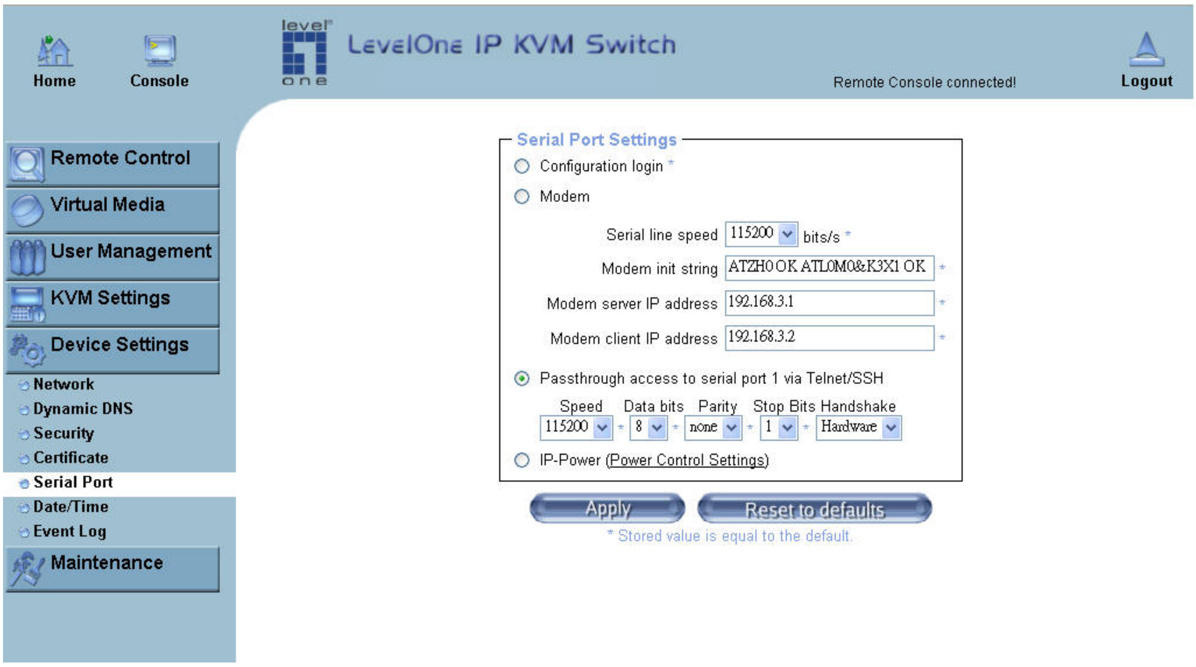
Challenge Password
Some certification authorities require a challenge password to authorize later changes on the certificate (e.g. revocation of the certificate). The minimal length of this password is 4 characters.

Confirm Challenge Password
Confirmation of the Challenge Password

Email
The email address of a contact person that is responsible for the KVM IP Console Module 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 KVM IP Console Module during connection establishment.

5.6.5 Serial Port



Serial Port Settings

○ Configuration login *

○ Modem

Serial line speed 115200 bits/s *

Modem init string ATZH0 OK ATL0M0&K3X1 OK *

Modem server IP address 192.168.3.1 *

Modem client IP address 192.168.3.2 *

● Passthrough access to serial port 1 via Telnet/SSH

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

○ IP-Power (Power Control Settings)

* Stored value is equal to the default.

Serial Port

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

Configuration login (or console login)

Do not use the serial port for any special function, use it only for the initial configuration.

Modem

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

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

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

Serial line speed

The speed the KVM IP Console Module is communicating with the modem. Most of all modems available today will support the default value of 115200 bps. In case you are using an old modem and discovering problems try to lower this speed.

Modem Init String

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

Modem server IP address

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

Modem client IP address

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

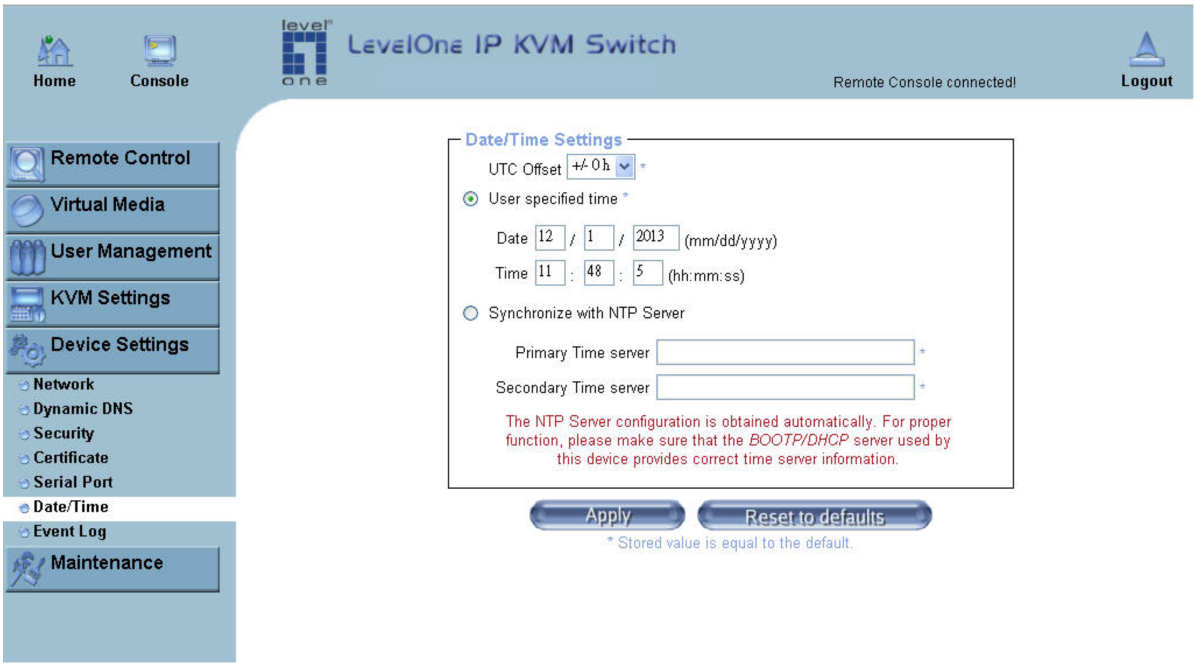
Passthrough access to serial port via Telnet

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

IP-Power (Power Control Settings)

For controlling Serial Power Controller.

5.6.6 Date / Time



Date/Time Settings

UTC Offset +/- 0 h *

● User specified time *

Date 12 / 1 / 2013 (mm/dd/yyyy)

Time 11 : 48 : 5 (hh:mm:ss)

○ Synchronize with NTP Server

Primary Time server *

Secondary Time server *

The NTP Server configuration is obtained automatically. For proper function, please make sure that the *BOOTP/DHCP* server used by this device provides correct time server information.

* Stored value is equal to the default.

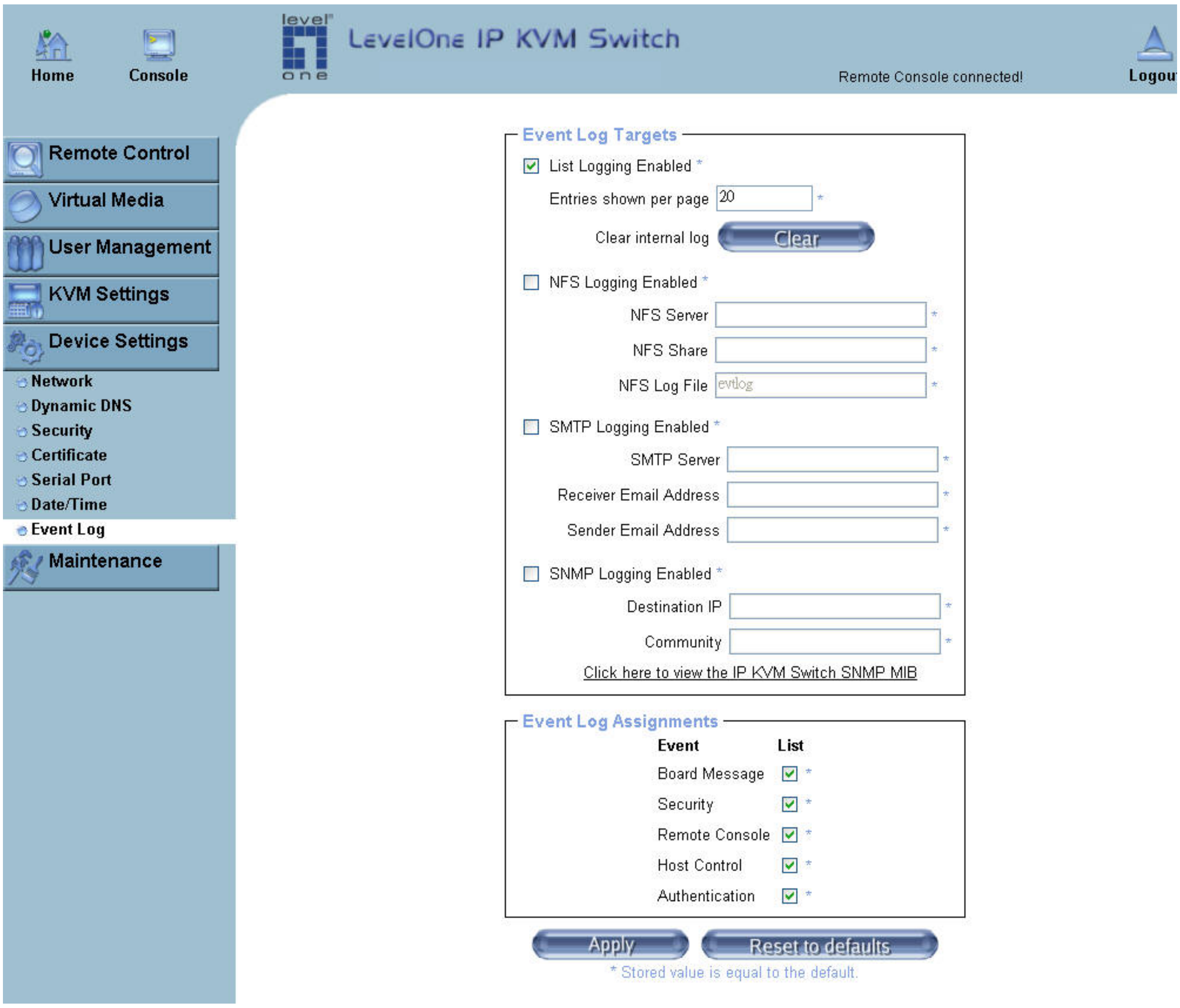
Date / Time

This link refers to a page, where the internal real-time clock of the KVM IP Console Module can be set up. User has the possibility to adjust the clock manually, or to use a NTP timeserver. Without a timeserver, the time setting will not be persistent, so user has to adjust it again, after KVM IP Console Module loses power for more than a few minutes. To avoid this, user 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 user to set up a static offset to get the local time.

Note

There is currently no way to adjust the daylight saving time automatically. Therefore, user must set the UTC offset twice a year properly according to the local rules.

5.6.7 Event Log



Event Log Targets

☑ List Logging Enabled *

Entries shown per page: 20 *

Clear internal log [Clear]

☐ NFS Logging Enabled *

NFS Server: *

NFS Share: *

NFS Log File: evtlog *

☐ SMTP Logging Enabled *

SMTP Server: *

Receiver Email Address: *

Sender Email Address: *

☐ SNMP Logging Enabled *

Destination IP: *

Community: *

Click here to view the IP KVM Switch SNMP MIB

Event Log Assignments

Event	List
Board Message	☑ *
Security	☑ *
Remote Console	☑ *
Host Control	☑ *
Authentication	☑ *

[Apply] [Reset to defaults]

* Stored value is equal to the default.

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 KVM IP Console Module. To show the log list, click on "Event Log" on the "Maintenance" page. In the Event Log Settings user can choose how many log entries are shown on each page. Furthermore, user can also clear the log file here.

List logging enabled

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

Since the KVM IP Console Module'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.

Note

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

NFS Logging enabled

Define a NFS server, where a directory or a static link have to be exported, to write all logging data to a file that is located there. To write logging data from more than one KVM IP Console Module 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 KVM IP Console Module 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 KVM IP Console Module device and that needs no authentication at all (<serverip>:<port>).

SNMP Logging enabled

If this is activated, the KVM IP Console Module 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

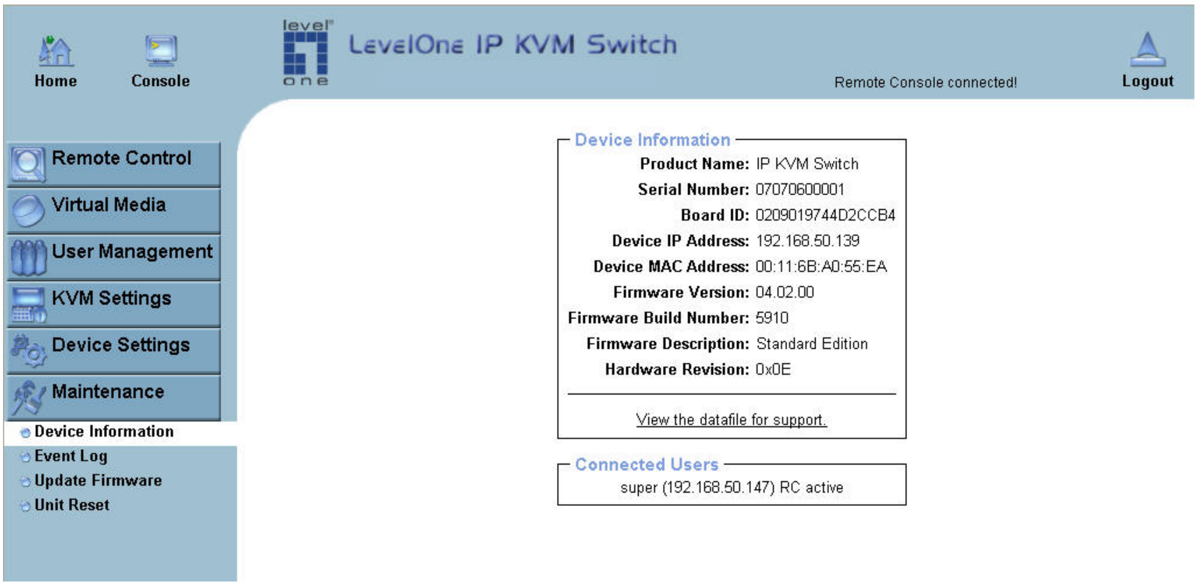
Firmware updated by user...	device
Internal log file cleared by user...	device
Security Violation	security
Host Power	host
Host Reset	host
Connection to Remote Console failed: reason.	console (several)
Connection to client ... established.	console
Connection to client ... closed.	console
Login failed.	auth
Login succeed.	Auth

Note

In contrast to the internal log file on the KVM IP Console Module, 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 user may have to delete it or move it away from time to time.

5.7 Maintenance

5.7.1 Device Information



Device Information

Product Name: IP KVM Switch
Serial Number: 07070600001
Board ID: 0209019744D2CCB4
Device IP Address: 192.168.50.139
Device MAC Address: 00:11:6B:A0:55:EA
Firmware Version: 04.02.00
Firmware Build Number: 5910
Firmware Description: Standard Edition
Hardware Revision: 0x0E

View the datafile for support.

Connected Users

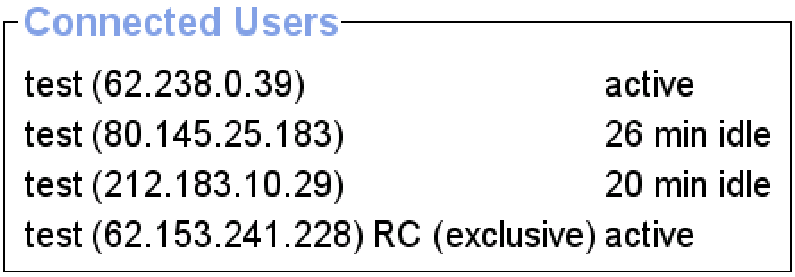
super (192.168.50.147) RC active

Device Information

Device Summary

This section contains a summary with various information about this KVM IP Console Module and it’s current firmware and allows you to reset the card.

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



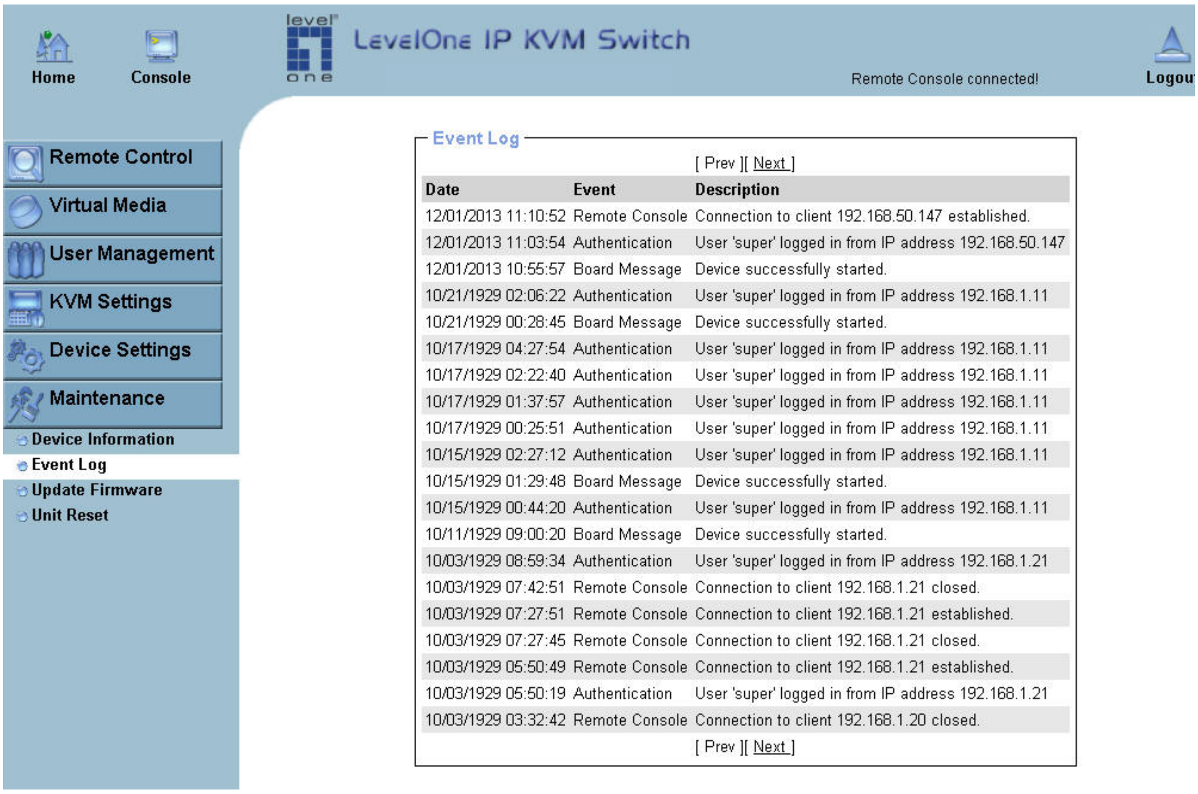
Connected Users

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

Connected Users

The above figure displays the KVM IP Console Module 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 in Chapter 5.
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.

5.7.2 Even log

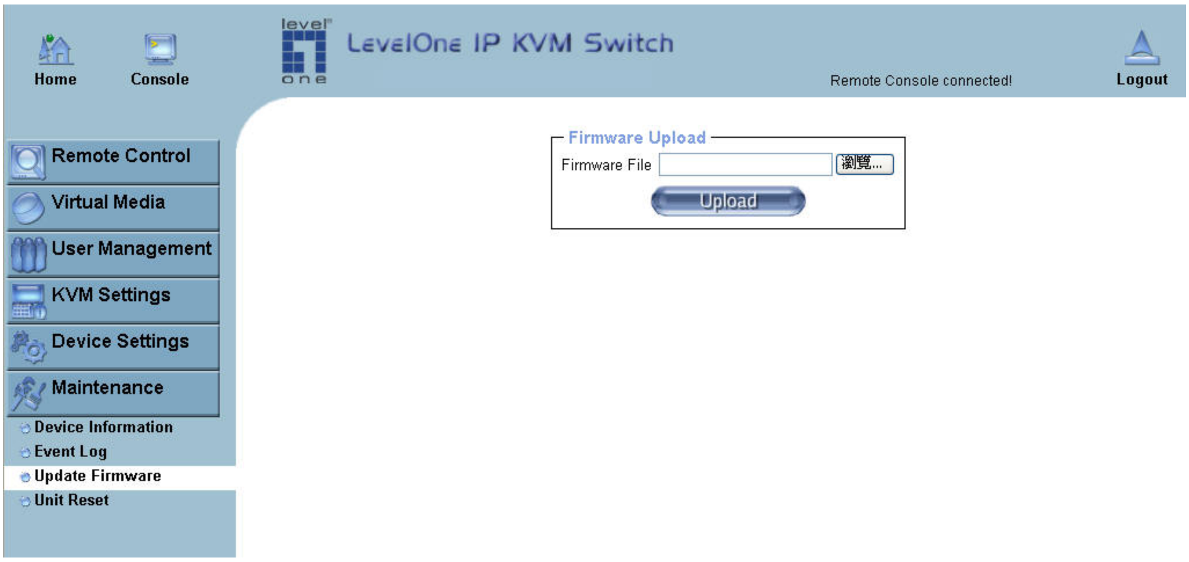


Date	Event	Description
12/01/2013 11:10:52	Remote Console	Connection to client 192.168.50.147 established.
12/01/2013 11:03:54	Authentication	User 'super' logged in from IP address 192.168.50.147
12/01/2013 10:55:57	Board Message	Device successfully started.
10/21/1929 02:06:22	Authentication	User 'super' logged in from IP address 192.168.1.11
10/21/1929 00:28:45	Board Message	Device successfully started.
10/17/1929 04:27:54	Authentication	User 'super' logged in from IP address 192.168.1.11
10/17/1929 02:22:40	Authentication	User 'super' logged in from IP address 192.168.1.11
10/17/1929 01:37:57	Authentication	User 'super' logged in from IP address 192.168.1.11
10/17/1929 00:25:51	Authentication	User 'super' logged in from IP address 192.168.1.11
10/15/1929 02:27:12	Authentication	User 'super' logged in from IP address 192.168.1.11
10/15/1929 01:29:48	Board Message	Device successfully started.
10/15/1929 00:44:20	Authentication	User 'super' logged in from IP address 192.168.1.11
10/11/1929 09:00:20	Board Message	Device successfully started.
10/03/1929 08:59:34	Authentication	User 'super' logged in from IP address 192.168.1.21
10/03/1929 07:42:51	Remote Console	Connection to client 192.168.1.21 closed.
10/03/1929 07:27:51	Remote Console	Connection to client 192.168.1.21 established.
10/03/1929 07:27:45	Remote Console	Connection to client 192.168.1.21 closed.
10/03/1929 05:50:49	Remote Console	Connection to client 192.168.1.21 established.
10/03/1929 05:50:19	Authentication	User 'super' logged in from IP address 192.168.1.21
10/03/1929 03:32:42	Remote Console	Connection to client 192.168.1.20 closed.

Event Log List

Above figure displays the log list including the events that are logged by the KVM IP Console Module.

5.7.3 Update Firmware



Update Firmware

The KVM IP Console Module is a complete standalone computer. The software it runs is called firmware. The firmware of the KVM IP Console Module 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 user by email or which user can download from the supplier web site. If the firmware file is compressed (file suffix .zip) then user must unzip it before he/she can proceed. Under the Windows operating system user may use WinZip from http://www.winzip.com/ for decompression. Other operating systems might provide a program called unzip.

Before user can start updating the firmware of KVM IP Console Module the new uncompressed firmware file has to be accessible on the system that user uses for connecting to the KVM IP Console Module.

Updating the firmware is a three-stage process:

• Firstly, the new firmware file is uploaded onto the KVM IP Console Module. In order to do that you need to select the file on your local system using the button “Browse” of the Upload Firmware panel. 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.

• Secondly, 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 the button “Update” will store the new version and substitute the old one completely.

Note

This process is not reversible and might take some minutes. Make sure the KVM IP Console Module’s power supply will not be interrupted during the update process because this may cause an unusable card.

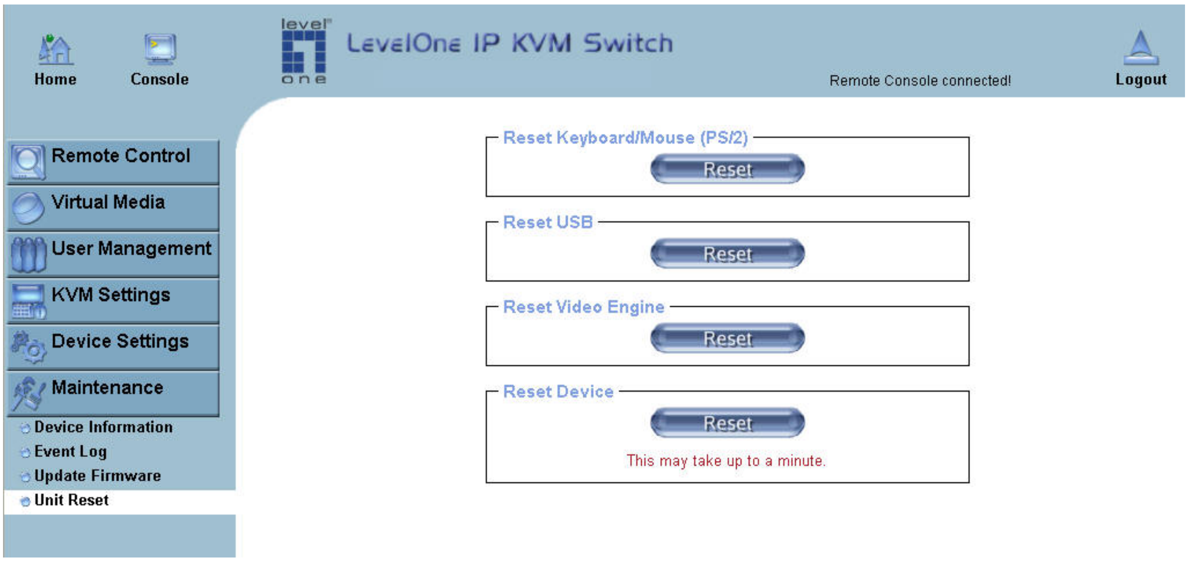
•

Thirdly, after the firmware has been stored, the panel will request you to reset the KVM IP Console Module manually. Half a minute after the reset, the KVM IP Console Module will run with the new firmware version and should be accessible. However, you are requested to login once again.

Note

The three-stage firmware update process and complete consistency check are making a mistake in updating the firmware almost impossible. However, only experienced staff members or administrators should perform a firmware update. Make sure the KVM IP Console Module’s power supply will not be interrupted during the update process.

5.7.4 Unit Reset



Reset Keyboard/Mouse (PS/2)

Reset

Reset USB

Reset

Reset Video Engine

Reset

Reset Device

Reset

This may take up to a minute.

Unit Reset

This section allows user to reset specific parts of the device. This involves the both keyboard and mouse, the video engine and the KVM IP Console Module itself. Resetting the card itself is mainly needed to activate a newly updated firmware. It will close all current connections to the administration console and to the Remote Console.

The whole process will take about half a minute. Resetting sub devices (e.g. video engine) will take some seconds only and does not result in closing connections. To reset a certain KVM IP Console Module functionality click on the button Reset as displayed in above figure.

Note

Only the system administrator user is allowed to reset the KVM IP Console Module.

6. Technical specifications

Function		Specification
VGA Resolution		1600 x 1200
OS supported		Windows (98/ME/2000/XP), Unix, Unix-like OS(Sun Solaris, Linux). Mac OSX
Browser supported		IE6.0 , Netscape7.0, Mozilla 1.6 (or above)
IP setting		DHCP, Bootp, Fix IP (DDNS supported)
Network Connection		10/100 Ethernet Telephone line (modem needed)
Management Interface		Web , Utility, Telnet, Serial Port
Event log		NFS, SMTP, SNMP trap
Hardware		
Host side	USB	USB 2.0 Type B
Console Side	Keyboard	PS/2 Mini Din 6-pin (female)
	Mouse	PS/2 Mini Din 6-pin (female)
	LAN	Standard RJ-45 Connector
	Serial Port	DB9 (male)

7. Troubleshooting

The remote mouse doesn’t work or is not synchronous
Make sure the mouse settings in KVM IP Console Module match the mouse model. There are some circumstances where the mouse synchronization process could behave incorrectly, refer to Sections 5.4.1 & 6.5.22 for further explanation.

The video quality is bad or the picture is grainy
Try to correct the brightness and contrast settings (see Sections 5.4.1 & 6.5.3) until they are out of a range where the picture looks grainy. Use the auto adjustment feature to correct a flickering video.

Login on KVM IP Console Module fails.
Was the correct combination of user and password given? On delivery, the user ”super” has the password ”pass”. Moreover your browser must be configured to accept cookies.

The Remote Console window can’t connect to KVM IP Console Module.
Possibly a firewall prevents access to the Remote Console. Make sure the TCP port numbers 443 or 80 are open for incoming TCP connection establishments.

No connection can be established to KVM IP Console Module.
Check whether the network connection is working in general (ping the IP address of KVM IP Console Module). If not, check network hardware. Is KVM IP Console Module powered on? Check whether the IP address of KVM IP Console Module and all other IP related settings are correct! Also verify that all the IP infrastructure of your LAN, like routers etc., is correctly configured. Without a ping functioning, KVM IP Console Module can’t work either.

Special key combinations, e.g. ALT+F2, ALT+F3 are intercepted by the console system and not transmitted to the host.
You have to define a so-called ’Button Key’. This can be done in the Remote Console settings.

In the browser the KVM IP Console Module pages are inconsistent or chaotic.
Make sure your browser cache settings are feasible. Especially make sure the cache settings are not set to something like ”never check for newer pages”. Otherwise KVM IP Console Module pages may be loaded from your browser cache and not from the card.

Windows XP doesn’t awake from standby mode
This is possibly a Windows XP problem. Try not to move the mouse while XP goes in standby mode.

Can’t upload the signed certificate in MacOS X
If an ’internal error’ occurs while uploading the signed certificate either change the extension of the file to .txt or add a file helper using the Internet Explorer preferences for this type of file. Make sure that the encoding is plain text and the checkbox ’use for outgoing’ is checked. Another possibility is to use a Mozilla based browser.

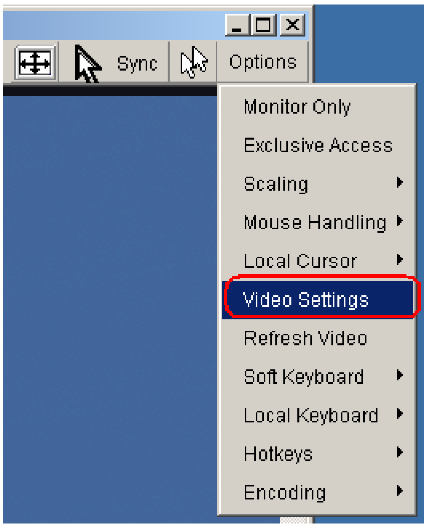
Every time I open a dialog box with some buttons the mouse pointers are not synchronous anymore

Please check, if you have an option like ”Automatically move mouse pointer to the default button of dialog boxes” enabled in the mouse settings of the operating system. This option needs to be disabled.

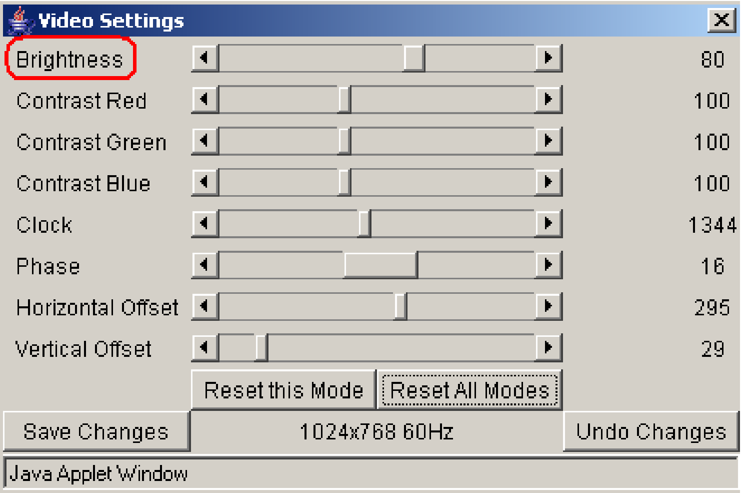
8. FAQs

The color of remote console displaying a pinkish tint.
If you are experiencing the **remote control screen displaying a pinkish tint** with some graphic cards, please try adjusting the brightness of the remote console by following steps below.

(1) Click **Video Settings** in Options menu of the remote console.



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


Video Settings

Brightness	80
Contrast Red	100
Contrast Green	100
Contrast Blue	100
Clock	1344
Phase	16
Horizontal Offset	295
Vertical Offset	29

Does any software require on servers which connect to the KVM IP Console Module?
No, the KVM IP Console Module is a 100% hardware solution. No extra software require on servers.

What operating systems does KVM IP Console Module support?
The KVM IP Console Module supports Windows 98, Windows ME, Windows 2000, Windows XP, Unix, Unix-like Operating System (Sun Solaris, Linux) and Mac OSX.

What browsers does KVM IP Console Module support?
The KVM IP Console Module support Microsoft Internet Explorer version 6.0 or higher, Netscape 7.0 and Mozilla 1.6

Does the KVM IP Console Module work with other brand's KVM switch?
Yes, the KVM IP Console Module can work with most standard KVM.

How many letters the username and password can be set on KVM IP Console Module?
The KVM IP Console Module accepts 32 letters of username and password.

How many concurrent user of KVM IP CONSOLE MODULE?
The KVM IP Console Module accepts 15 concurrent users.

How many bits of connection encrypted of KVM IP Console Module?
The KVM IP Console Module provides AES 256 bits connection encrypted.

Local mouse and remote mouse didn't sync after doing mouse Intelligent Sync.
Please don't put window on left-up corner of remote console of KVM IP Console Module. Intelligent Sync has to re-calculate the coordinate of mouse from left-up corner on remote console.

9. Addendum

A. Key Codes

Table A.1 shows the key codes used to defines keystrokes or hotkeys for several functions. Please note that these key codes do not represent necessarily key characters that are used on international keyboards. They name a key on a standard 104 key PC keyboard with an US English language mapping. The layout for this keyboard is shown in Figure A.1. However, most modifier keys and other alphanumeric keys used for hotkey purposes in application programs are on an identical position, no matter what language mapping you are using. Some of the keys have aliases also, means they can be named by 2 key codes (separated by comma in the table).

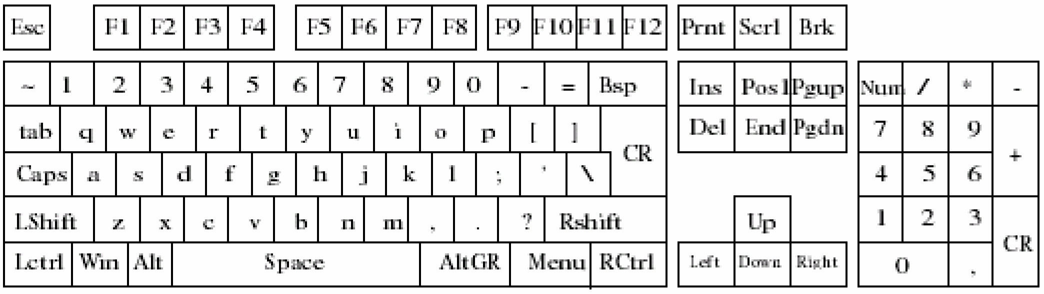

Esc F1 F2 F3 F4 F5 F6 F7 F8 F9 F10 F11 F12 Prnt Scrl Brk
~ 1 2 3 4 5 6 7 8 9 0 - = Bsp Ins Pos1 Pgup Num / * -
tab q w e r t y u i o p [ ] CR Del End Pgdn 7 8 9 +
Caps a s d f g h j k l ; ' \ 4 5 6
LShift z x c v b n m , . ? Rshift Up 1 2 3 CR
Lctrl Win Alt Space AltGR Menu RCtrl Left Down Right 0 .

Figure A.1: English (US) Keyboard Layout, used for key codes

Key (and aliases)		
0 - 9	SPACE	PAGE DOWN
A - Z	ALTGR	UP
, TILDE	ESCAPE, ESC	LEFT
-, MINUS	F1	DOWN
=, EQUALS	F2	RIGHT
;	F3	NUM LOCK
'	F4	NUMPAD0
<, LESS	F5	NUMPAD1
,	F6	NUMPAD2
.	F7	NUMPAD3
/, SLASH	F8	NUMPAD4
BACK SPACE	F9	NUMPAD5
TAB	F10	NUMPAD6
[	F11	NUMPAD7
]	F12	NUMPAD8
ENTER	PRINTSCREEN	NUMPAD9
CAPS LOCK	SCROLL LOCK	NUMPADPLUS,NUMPAD PLUS
\, BACK SLASH	BREAK	NUMPAD/
LSHIFT, SHIFT	INSERT	NUMPADMUL,NUMPAD MUL
RCTRL	HOME	NUMPADMINUS,NUMPAD MINUS
RSHIFT	PAGE UP	NUMPADENTER
LCTRL, CTRL	DELETE	WINDOWS
LALT, ALT	END	MENU

Table A.1: Key Names

B. Video Modes

Table B.1 lists the video modes KVM IP Console Module supports. Please don't use other custom video settings besides of these. If done so, KVM IP Console Module may not be able to detect them.

Resolution (x, y)	Refresh Rates (Hz)
640 x 350	70, 85
640 x 400	56, 70, 85
640 x 480	60, 72, 75, 85, 90, 100, 120
720 x 400	70, 85
800 x 600	56, 60, 70, 72, 75, 85, 90, 100
832 x 624	75
1024 x 768	60, 70, 72, 75, 85, 90, 100
1152 x 864	75
1152 x 870	75
1152 x 900	66
1280 x 960	60
1280 x 1024	60, 75

Table B.1 Video mode

C. User Role Permissions

Table C.1 lists the user role permissions granted for three user role groups: "Superuser", "Administrator", and "User"

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

Firmware			
Maintenance: Unit Reset	Keyboard/ Mouse, Video	Keyboard/ Mouse, Video	Keyboard/ Mouse, Video, Device

Table C.1 User Role Permissions

D. KVM IP Console Module port table

Port	Protocol	Purpose
23	Telnet over TCP	Web & Telnet client
80	HTTP over TCP	Web
443	HTTPS over TCP	Web
443	RFB over TCP	Remote Console
443	HTTPS over TCP	Drive Redirection
139	SMB over TCP	CD-ROM Image (Samba Service)
139	SMB over TCP	Floppy disk(Samba Service)
1024	SMB over TCP	Samba Service source port
162	SNMP over TCP	SNMP trap reception port
1024	SNMP over TCP	SNMP source port
443	RFB over TCP	Remote Keyboard and Mouse data

E. Bandwidth Consumption

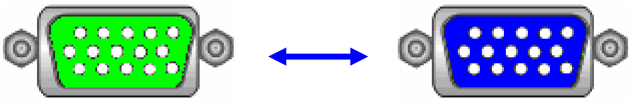
The preconfigured network speed selection simply results in a different Compression and Color Depth configuration in order to match the different bandwidth limitations of the network type (UMTS, ISDN, etc.)

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

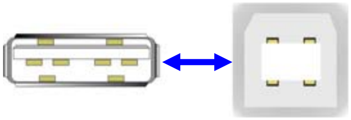
	Compression	**Color Depth**	**Used Bandwidth**	**Comment**
Video Optimized	Video Optimized	8 bit	3.0 - 3.3 MB/s	uncompressed, synchronized video data, most bandwidth needed
Video Optimized (high color)	Video Optimized	16 bit	4.3 - 5.0 MB/s	uncompressed, synchronized video data, most bandwidth needed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

F. Cable Connectors

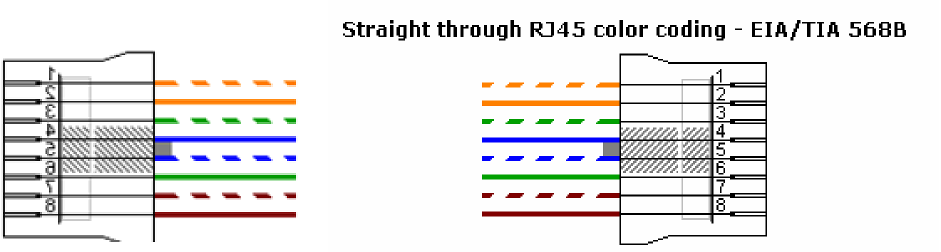
VGA Cable: HDDB15 Male to Male



USB 2.0 Cable: USB A-B cable



CAT5/5E/6 Straight Through UTP/STP Cable



GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the soft-ware or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all. The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE

Terms and Conditions For Copying, Distribution And Modification

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it. Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and condi-tions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms

and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consis-tent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and condi-tions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES

PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING,

REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

All the source code of LevelOne GPL products are uploaded to http://www.level1.com

All the users can download freely.