LINDY®

CONNECTION PERFECTION

KVM over IP SWITCH

User Manual   *English*

LINDY No. 39414, 39636, 39432

www.lindy.com

CE For Commercial Use Only
Tested to comply
with FCC Standards

PREFACE

This manual refers to the stand-alone **KVM OVER IP SWITCH** (No.39414) as well as to the **KVM over IP modules** (No. 39432, 39636) that can be installed into the relevant KVM Switches CAT32, COMBO and U-Series.

In January 2014, we introduced some important software changes:
- We have issued a LINDY certificate for the JAVA applet required to run the JAVA based browser tools to access the KVM Switch. Since Oracle has issued the Java 7.51 update unsigned applets cannot be used any further
- VNC support has been added to the KVM over IP Switches
- French language option has been added

The **LINDY KVM OVER IP SWITCH** features the latest and most technologically advanced SoC (System on Chip) IP KVM solution, based on Raritan / Peppercon's latest IP-KVM engine technology.

Some screenshots may display a slightly different design referring to an older firmware version. Due to constant technological advances and further development, changes to this product may be introduced without further notice.

The LINDY team, January 2014

Contents

1. Introduction

Thank you for purchasing the LINDY KVM OVER IP SWITCH. This device allows operators to monitor and access their computers from remote locations. The KVM OVER IP SWITCH connects to the internet, intranet, LAN or WAN using standard CAT5 or higher cable. The modular version is installed into the back of a KVM switch directly.

The stand-alone version then uses a KVM cable to connect a local KVM switch or server. It supports PS/2 as well as USB keyboard/mouse and 15-way VGA type monitor connections. However please note that when using a USB mouse and keyboard from the local console you have to use the USB connection to the server/KVM switch too. And when using PS/2 keyboard and mouse also the PS/2 connection to the server/KVM Switch has to be used.

The KVM OVER IP SWITCH combines convenient digital remote KVM access and control with integrated system management. It captures, digitizes and compresses the video signal and transmits it alongside the keyboard and mouse signals, to and from a remote computer. The KVM OVER IP SWITCH provides a non-intrusive solution for remote access and control. Remote access and control software runs on its embedded processors only – so there is no interference with server operation, or impact on network performance.

The KVM OVER IP SWITCH automatically detects the video mode of the console and allows manual fine tuning for improved video quality.

The KVM OVER IP SWITCH also features remote mass storage support – the unit connects via a USB connection to the server/KVM switch and allows virtual storage devices located at the remote users computer to provide data and a virtual drive to the server.

1.1 Features

- Remote access of KVM switches or servers via LAN, WAN, or the internet; control your installation from almost anywhere in the world
- KVM (keyboard, video, mouse) access over IP and analogue telephone line (requires modem)
- BIOS level access also for remote computers
- 256-bit SSL encryption, SSL Certificate Management
- No impact on server or network performance
- Automatically senses video resolution for best possible screen capture
- High-performance mouse tracking and synchronisation
- Local mouse suppression
- Remote mass storage virtual media feature
- Compatible with Windows, Mac OS 10 and Linux Red Hat/Fedora/Knoppix

1.2 Package Contents

- KVM OVER IP SWITCH (stand-alone or module version)
- Power Adapter, Multi Country for EURO, UK, US, AUS (stand-alone version only)
- 19" Rack mount kit and set of 4 rubber feet for desktop use (stand-alone version only)
- RS-232 Serial cable
- USB 2.0 A to Mini B type Cable
- 3-in-1 KVM Cable, 1m (stand-alone version only)
- Software CD including tools and this manual
- Printed Quick Start Manuals
- 3 product labels (incl. 1 spare) with S/N & MAC (module version only)

2. Hardware Installation

2.1 Operation Overview

The pictures below show the connection options of the KVM OVER IP SWITCH.

The KVM OVER IP SWITCH redirects local keyboard, mouse, and video signals to a remote administration console. All data is transmitted using the TCP/IP protocol.

Administrator (Client) — IP Network — IP Access Switch — Server (Host)

Controlling a single computer
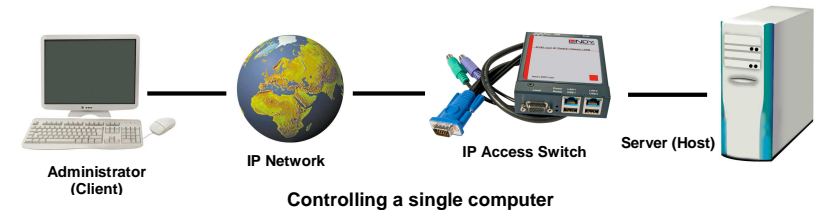
The KVM OVER IP SWITCH can be used in a multi administrator and multi-server environment as well. Attaching one or more KVM OVER IP SWITCH units to a KVM switch matrix allows multiple server access via a single remote console.

IP Network — IP Access Switch OR — KVM Switch

Administrator (Client)

Controlling multiple computers via a KVM Switch
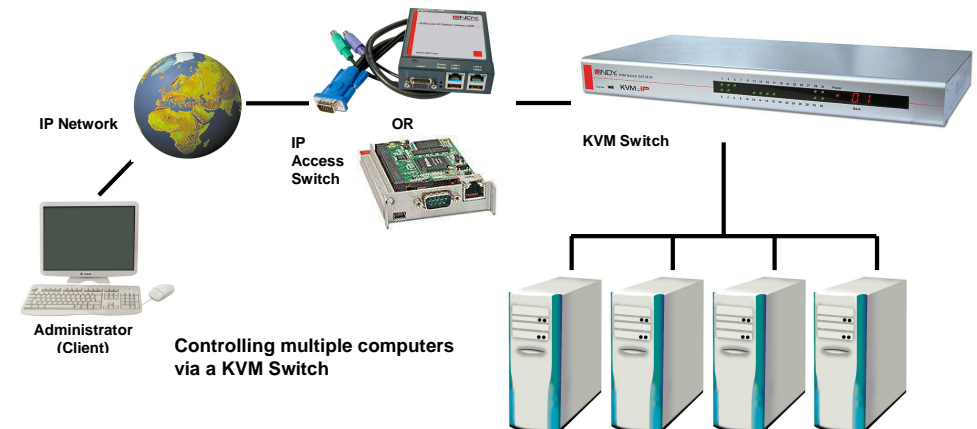
2.2 Connections

2.2.0 KVM over IP Access Module Installation - Module version only!

Before you install the KVM over IP Access module into the KVM switch ensure the KVM Switch is switched off and the power supply is unplugged. Proceed to unscrew and remove the small metal cover on rear of the KVM switch. Carefully slide the module into the slot and secure in place with the screw previously removed.

You may either use PS/2 or USB mouse and keyboard.
However, please note that USB mouse and keyboard signals from your local console will not be converted and output as PS/2 signals to your server/KVM switch!

2.2.1 Host or KVM Switch Connection Side - Stand-alone version only!

Use the 3in1 KVM cable (VGA & 2x PS/2) attached to the KVM Switch to make the connections to the host computer. If you want to use the USB mouse and keyboard, or the USB virtual media feature, use the supplied USB A-Mini B cable to connect the USB Mini B port on the back of the KVM OVER IP SWITCH to a USB port on your server or KVM switch.

2.2.2 Console Connection Side - Stand-alone version only!

Connect your local keyboard, monitor and mouse console using the short VGA and PS/2 3in1 KVM splitter cable - connected to the KVM over IP SWITCH port labelled **Local** - if you want to use PS/2 peripherals – if you want to use USB peripherals only you may connect your monitor directly to the HD15 connector on the IP KVM Switch. If you want to use a USB mouse and keyboard connect them to the ports labelled **USB** located below the RJ45 ports. However, please note that USB mouse and keyboard signals from your local console will not be converted and output as PS/2 signals to your server/KVM switch.

2.2.3 Network Connection

The stand-alone KVM OVER IP SWITCH provides two RJ45 ports for Ethernet connection - the second port can be used to cascade multiple KVM IP Switches. The module version only provides one RJ45 port.
The ports can be used with a 100Mbps, 100Base-TX connection or a 10Mbps, 10Base-T connection. The KVM OVER IP SWITCH will sense the connection speed and automatically adjust to the appropriate operation mode.

10Mbps Connection, 10Base-T

Please note that this slow connection may not provide sufficient performance for the compressed video data traffic and will result in low video and colour resolution and significantly delayed reaction time for remote connections!

2.2.4 Dial up Line / Modem Connection

The RS232 port of the KVM OVER IP SWITCH can either be used to connect to an external Modem i.e. to set up a dial up line connection or can be used to connect to an external RS232 managed power switch. Use the supplied cable to connect the appropriate unit.

2.2.5 Connecting an External Power Switch option

At the time of writing (October 2009) the KVM OVER IP SWITCH supports the following external power switch options: Peppercon IPM-220L, Avocent SPC1 800/1600, Sentry In-Line Power Module, Leaning ePowerSwitch.

However, we strongly suggest to use a directly IP managed power switch such as the LINDY IPower Switches No.s 32657, 32658, 32652 or 32656

2.2.6. LED indicators and Switches

LED	Indication
Power - Stand-alone version only!	**RED** – On when power is applied
LAN **Ethernet Link/Act** **10/100Mbps**	**Orange (10)** -- 10BaseT Ethernet connection established **Green (100)** -- 100BaseT Ethernet connection established *Blinking*: Activity *ON*: When no data activity and link is connected
Link	**Green** -- Blinking when data is being transmitted

■ **RESET** button - Stand-alone version only: on the rear panel, hidden behind the small hole, press the button to reboot the IP-KVM unit

3. Configuration

The KVM OVER IP SWITCH communication interface is based on TCP/IP. The switch comes pre-configured with the IP configuration detailed here:

Parameter	Value
IP auto configuration	none
IP-Address	192.168.0.70
Net-mask	255.255.255.0
Default-Gateway	none

If this initial configuration does not meet your requirements, the following section describes the configuration that is necessary to access the KVM over IP SWITCH for the first time.

3.1 Initial IP Configuration via Network

If DHCP mode is enabled (IP auto configuration = DHCP), the KVM over IP Switch will try to contact a DHCP server in the subnet to which it is physically connected. If a DHCP server is found, it may provide a valid IP address, gateway address and net mask. Before you connect the device to your local subnet, be sure to complete the corresponding configuration of your DHCP server. It is recommended to configure a fixed IP assignment to the MAC address of the KVM over IP SWITCH. You can find the MAC address labelled on the bottom side of the metal housing and on the separate labels provided with the modules.

There is a Network Setup Software tool (PSetup) for setting up the network configuration (IP Address, Subnet mask, DHCP, etc). It is useful when you want to change the network settings or when you cannot access to the unit due to not knowing the network settings of the unit. In this case, you can view or change the settings via this utility. Follow the procedure described on the next page *(Section 3.3.)*

3.2 Initial Configuration via Serial Console

The KVM OVER IP SWITCH has a serial line interface (host side) for connecting a serial terminal. This connector is compliant with the RS-232 serial line standard. The serial line has to be configured with the parameters given in this table:

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

When configuring with a serial terminal, reset the KVM OVER IP SWITCH and immediately press the **ESC** key. You will see some device information and a **"=>"** prompt. Type **config** and press the **Enter** key. Wait a few seconds for the configuration questions to appear.

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

IP auto configuration (non/dhcp/bootp) [dhcp]:
IP [192.168.0.70]:
Net mask [255.255.255.0]:
Gateway (0.0.0.0 for none) [0.0.0.0]:

3.3 KVM OVER IP SWITCH Setup Tool

3.3.1 MAC Address Detection

Connect the KVM OVER IP SWITCH to your computer either via a local network, or via USB. If you use a USB connection Windows will detect the KVM OVER IP SWITCH as a '**Removable Disk**' and an appropriate drive letter will be assigned.

psetup   Start the setup tool from the CD ROM.

A window opens as shown below:

On the upper left corner, the MAC address of the KVM OVER IP SWITCH is displayed. To detect the MAC address, press the **Refresh Devices** button. The displayed MAC address is the same as that printed on the sticker on the base of the unit.

On the lower right corner of the window, there are two buttons: **Query Device** and **Setup Device**. Press the **Query Device** button to display the preconfigured values of the network configuration. The values are displayed in the text fields located above. If necessary, adjust the network settings to your needs. To save the changes enter a user login and a password *(see 3.3.2 Authentication, on page 9)* and then press the **Setup Device** button.

3.3.2 Authentication

To adjust the authentication settings, enter your login as a super user and change your password.

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

Super user password
Enter the current password for the super user. This initial value is **pass**. All of the characters are lower case. Please change the password when configuring the KVM over IP SWITCH for the first time. Not to change the default password may cause some unauthorized access to the switch and the servers connected! Please make sure to store the new password in a secure place you easily can find once you forget it.

New super user password
Enter the new password for the super user.

New password (confirm)
Re-type the new password for the super user.

To close the window and accept the changes, press the **OK** button, otherwise press the **Cancel** button.

3.3.3 IP Auto Configuration

With this option, you can specify whether the KVM OVER IP SWITCH should obtain its network settings from a DHCP or BOOTP server. From the drop down list select either **DHCP** or **BOOTP**. If you select **NONE**, the IP auto configuration is disabled and you should manually input the following network settings:

IP address
The IP address the KVM OVER IP SWITCH uses.

Net mask
The net mask of the connected IP subnet.

Gateway address
The IP address of the default router for the connected IP subnet. If you do not have a default router, enter **0.0.0.0**.

3.4 Keyboard, Mouse and Video configuration

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

3.4.1 KVM OVER IP SWITCH Keyboard Settings

The KVM OVER IP SWITCH settings for the host's keyboard type have to be correct in order to make the remote keyboard work properly. The settings can be checked using the KVM OVER IP SWITCH web front-end.

3.4.2 Remote Mouse Settings

A common problem with KVM devices is the synchronization between the local and remote mouse cursors. The KVM OVER IP SWITCH addresses this problem with an intelligent synchronization algorithm. There are two mouse modes available on the KVM OVER IP SWITCH CLASSIC USB: **Auto mouse speed** and **Fixed mouse speed**.

Auto mouse speed
The automatic mouse speed mode tries to detect the speed and acceleration settings of the host system automatically. Speed detection is performed during mouse synchronization. If the mouse does not move correctly, there are two ways to re-synchronize the local and remote mouse:

Fast Sync: Fast synchronization is used to correct a temporary, but fixed skew. Choose this option using the Remote Console options menu or by pressing the mouse synchronization hotkey sequence - **[ALT] + [F12]**

Intelligent Sync: If the fast sync does not work correctly or the mouse settings have been changed on the host system, you can use the intelligent resynchronization option. This method can be accessed from the **Mouse Handling** sub menu of the Remote Console **Option** menu.

Intelligent synchronization requires a correctly adjusted picture. Use the auto adjustment function or manual correction in the Video Settings panel to setup the picture. **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 was recently changed.

Tip: When first started, if the local mouse pointer is not synchronized with the remote mouse pointer, click the **Auto Adjust Button** once. If the mouse is still not synchronized select **Intelligent Sync** from the **Mouse Handling** sub menu of the Remote Console **Option** menu.

Fixed mouse speed
This mode just translates the mouse movements from the Remote Console in a way that one pixel move will lead to '**n**' pixel moves on the remote system. This parameter '**n**' is adjustable. However, it should be noted that this works only when mouse acceleration is turned off on the remote system.

3.4.3 Host System Mouse Settings

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

> **Note:** The following limitations do not apply when using USB mice and Windows 2000 and higher!

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

Windows XP Mouse Settings
If using Windows XP, disable the **enhance pointer precision / improve mouse acceleration** setting.

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

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

3.4.4 Single and Double Mouse Mode

The information above applies to **Double Mouse Mode**, where both remote and local mouse pointers are visible and need to be synchronized. The KVM OVER IP SWITCH also features another mode - **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, use the hotkey combination **[ALT] + [F12]** to free the captured local mouse pointer.

3.4.5 Recommended Mouse Settings

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

MS Windows 2000/2003 (Professional and Server), XP, …
In general, we recommend the use of a USB mouse. Choose USB without Mouse Sync. For a PS/2 mouse choose Auto Mouse Speed. For XP disable the option called **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
We recommend using the Single Mouse Mode.

3.4.6 Video Modes

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

4. Usage

4.1 Prerequisites

The KVM OVER IP SWITCH features an embedded operating system offering a variety of standardized interfaces. This section will describe these interfaces, and the way to use them in a more detailed manner. The interfaces are accessed using the TCP/IP protocol family.

The following interfaces are supported:
Telnet
A standard Telnet client can be used to access an arbitrary device connected to the KVM OVER IP SWITCH CLASSIC USB's serial port via a terminal.

HTTP/HTTPS
Full access is provided by the embedded web server. The KVM OVER IP SWITCH environment can be entirely managed using a standard web browser. You can access the KVM OVER IP SWITCH using the insecure HTTP protocol, or using the encrypted HTTPS protocol. Whenever possible, use HTTPS.
The primary interface of the KVM OVER IP SWITCH is the HTTP interface. This is covered extensively in this section. Other interfaces are addressed in the relevant subsections.
In order to use the Remote Console window of your managed host system, the browser must feature Java Runtime Environment. If the browser has no Java support (such as on a small handheld device), you can still maintain your remote host system using the administration forms displayed by the browser itself.

> **Important: We recommend you install the latest version of Sun's Java Virtual Machine which can be downloaded from the following web site:**
> **www.java.com**

Java configuration
Oracle has stopped support for **unsigned applets** starting with version 7.51 in January 2014, it is required that the LINDY KVM Java certificate issued January 2014 be installed in every computer's Java runtime environment used to access the KVM OVER IP SWITCH. The certificate can be downloaded from the KVM OVER IP SWITCH (Menu Maintenance / Device Info / Download CA Root …. / right click on the page and save as KVM_Certificate_Authority.p12) or from the LINDY product websites. To install it open the Java console (i.e. Windows: Start > Control Panel > Java) select tab Security > Manage Certificates > Select: **Signer CA** > Import and select the downloaded certificate file (.p12) KVM_Certificate_Authority.p12 .
In the Firefox browser you may eventually have to add another JAVA setting: Click on the Firefox logo on top left resp. the Extras menu, select Add-ons and Plugins, and set the JAVA(TM) Platform SE to "Always active".

VNC
The new firmware also includes the option to access the KVM over IP switch via VNC. VNC does not require Java, however it does not have the comfort features offered by Java-based Web browser access. The performance is also sluggish as reflected by the slow response time. Most widely-used VNC viewers can be used. For instance, Tight VNC has been tested without any problems. For Real VNC, the video must be set to color mode 3, other VNC viewers may require other extra settings.

4.2 Logging In

4.2.1 Login to the KVM OVER IP SWITCH

Launch your web browser. Direct it to the address of your KVM OVER IP SWITCH which you configured during the installation process. The address used might be a plain IP address or a host and domain name if you have given your KVM OVER IP SWITCH a symbolic name in the DNS.

Example: Type the following in the address line of your browser when establishing an unsecured connection:

http://<IP address of KVM OVER IP SWITCH >

When using a secure connection, type in:

https://<IP address of KVM OVER IP SWITCH >

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

The KVM OVER IP SWITCH has a built-in super user account that has all the permissions enabled to administrate your KVM OVER IP SWITCH:

| Login name	super (factory default)
Password	pass (factory default)

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

Note: The user "super" is not allowed to login via the serial interface of the IP-KVM switch.

Please make sure you change the super user password immediately after you have installed and accessed your KVM OVER IP SWITCH for the first time. Not changing the password for the super user is a severe security risk and could result in unauthorized access to the switch and to the host system(s) to which it is connected.

4.3 Navigation

Once logged into the KVM OVER IP SWITCH successfully, the main page appears. This page consists of three parts; each of them contains specific information. The buttons in the upper area allow you to navigate within the front end. The lower left area contains a navigation bar and allows you to switch between the different sections of the KVM OVER IP SWITCH. Within the main area, task-specific information is displayed.
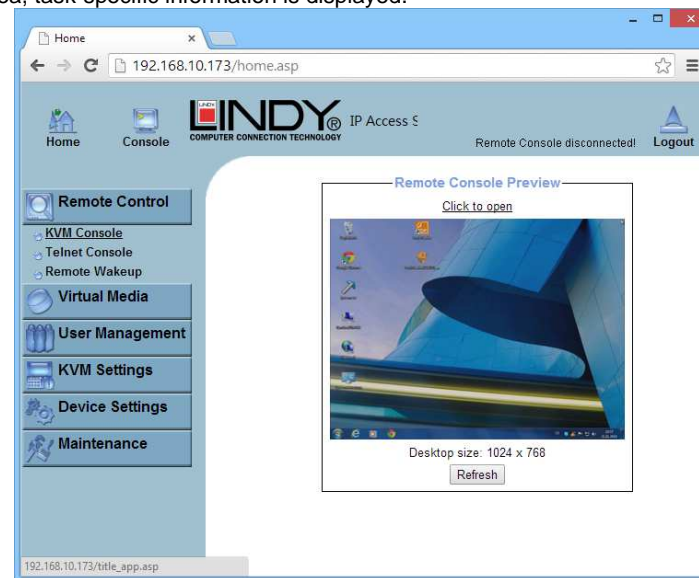
Return to the main page of the KVM OVER IP SWITCH

Logout from the KVM OVER IP SWITCH

This link logs out the current user and presents a new login screen. Please note that an automatic logout will be performed if there is no activity for half an hour. Clicking one of the links will bring you back to the login screen.

Access the Remote Console

The Remote Console is the redirected screen, keyboard and mouse of the remote host system that the KVM OVER IP SWITCH controls. Selecting this button opens the **Remote Console Main Window.**

The Remote Console window is a Java Applet that establishes its own TCP connection to the KVM OVER IP SWITCH. The protocol that runs over this connection is neither HTTP nor HTTPS, but RFB (Remote Frame Buffer Protocol). RFB needs to establish a connection to port

number 443. Your local network environment has to allow this connection to be made, i.e. your firewall and, if you have a private internal network, your NAT (Network Address Translation) settings have to be configured accordingly.

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

If you experience problems, please consult your network administrator in order to provide an appropriate network environment.

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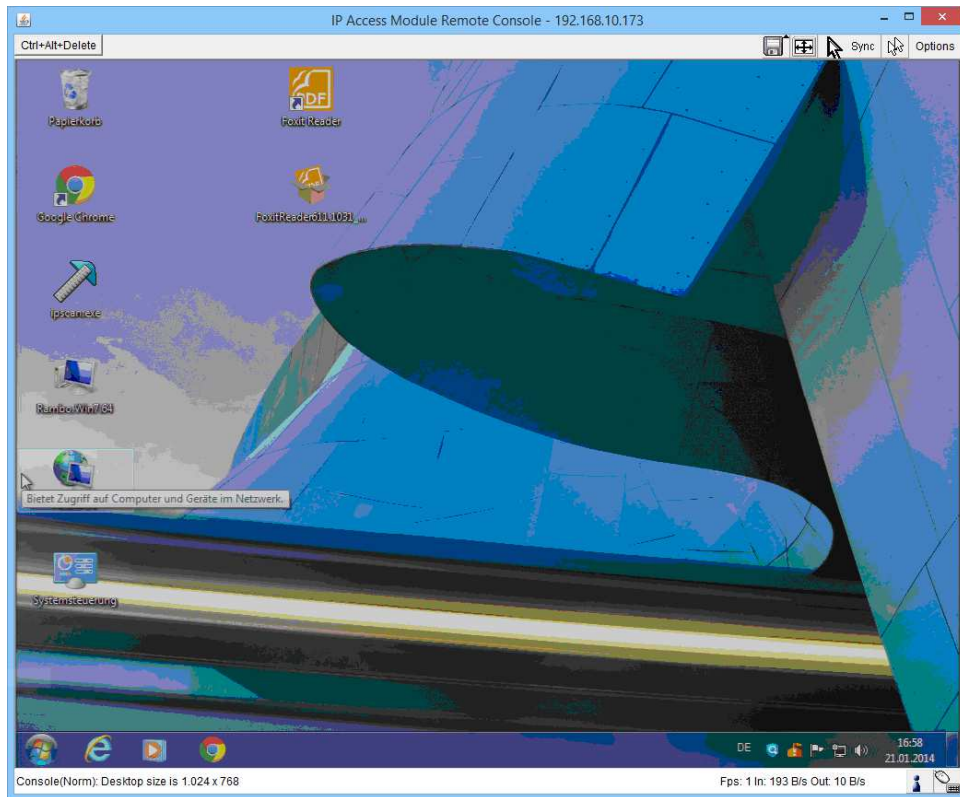
Starting the Remote Console opens an additional window. It displays the screen content of your host system. The Remote Console will behave in exactly the same way as if you were sitting directly in front of the screen of your host system. This means that the keyboard and mouse can be used in the usual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

Note: Your local keyboard changes its keyboard layout according to the remote host system. If you use a German administration system and your host system uses a US English keyboard layout for instance, some special keys on the German keyboard will not work as expected. Instead, the keys will result in their US English counterpart, i.e Z>Y and Y>Z. You can circumvent such problems by adjusting the keyboard of your remote system to the same mapping as your local one. Also see OSD KVM Settings: Keyboard/Mouse and section 5.4.2.

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

4.3.2 Remote Console Control Bar

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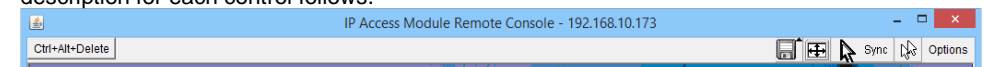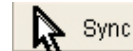

 Ctrl+Alt+Delete
Sends the 'Control Alt Delete' key combination to the remote system

 Auto Adjust button
If the video display is poor quality or distorted in some way, click this button and wait a few seconds while the KVM OVER IP SWITCH tries to adjust itself for the best possible video quality.

 Sync mouse
Activates the mouse synchronization process. Choose this option in order to synchronize the local AND remote mouse cursors. 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) Single mouse mode is only available if using SUN JVM 1.3 or higher.

Tip: When in single mouse mode use the hotkey combination **[ALT] + [F12]** to release mouse control and access the menus etc.

Options Options

Opens the Options menu. A short description of each 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 but monitoring is.

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

A change in the access mode is also visible in the status line indicated by this icon.

Scaling
Allows you to scale down the Remote Console window: 25% / 50% / 100% / *Scale to fit*. You can still use both mouse and keyboard; however the scaling algorithm will not preserve all display details.

Mouse Handling
The submenu for mouse handling offers three options for synchronizing the local and the remote mouse pointer.

Mouse Mode
Allows switching between Single Mouse Mode and Double Mouse Mode

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

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

Video Settings
Opens a panel for changing the KVM OVER IP SWITCH video settings. The KVM OVER IP SWITCH features two different dialogs, which influence the video settings:

Video Settings in the KVM section in the front end menu:
The Noise Filter option defines how the KVM OVER IP SWITCH reacts to small changes in the video input signal. 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:
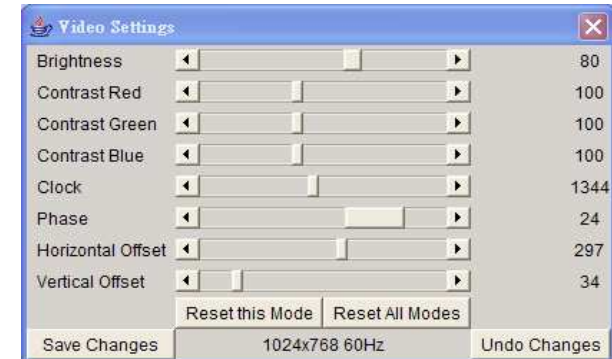
Brightness
Controls the brightness of the picture

Contrast
Controls the contrast of the picture

Clock
Defines the horizontal frequency for a video line and depends on the video mode. Different video card types may require different values here. The default settings in conjunction with the auto adjustment procedure should be adequate for most common configurations. If the picture quality is still bad after auto adjustment you may 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 Offset
Use the left and right buttons to move the picture in a horizontal direction

Vertical Offset
Use the left and right buttons to move the picture in a vertical direction

Reset this Mode
Reset mode specific settings to the factory-made defaults.

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

Save Changes
Save changes permanently

Undo Changes
Restore last settings

Soft Keyboard
Opens up the sub-menu for the Soft-Keyboard:

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

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

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

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

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


4.3.3 Remote Console Status Line

Status line
Shows both console and the connection state. The size of the remote screen is displayed. The example below was taken from a Remote Console with a resolution of 1024 x 768 pixels. The value in brackets describes the connection to the Remote Console. **Norm** means a standard connection without encryption, **SSL** indicates a secure connection.
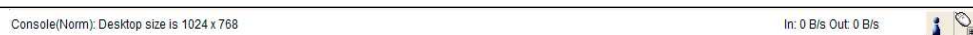
Furthermore, both the incoming (**In:**) and the outgoing (**Out:**) network traffic are visible (in kb/s). If compressed encoding is enabled, a value in brackets displays the compressed transfer rate.
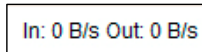
For more information about **Monitor Only** and **Exclusive Access** settings, see the relevant sections.

5. Menu Options

5.1 Remote Control

5.1.1 KVM Console

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

For the **Remote Power** settings see *Section 2.2.5 on page 6.*

5.1.2 Telnet Console

To use Telnet it must be enabled in Device Settings > Network, see section 5.5.1

The KVM OVER IP SWITCH firmware features a Telnet server that enables a user to connect via a standard Telnet client. If the Telnet program is using a VT 100, VT 102 or VT 220 terminal or appropriate emulation, it is even possible to perform a console redirection, as long as the KVM OVER IP SWITCH host is using a text mode screen resolution.

Connecting to the KVM OVER IP SWITCH is done as usual and as required by the Telnet client, for instance in a UNIX shell:

      telnet [your device's IP]

Replace the IP address by the one that is actually assigned to the KVM OVER IP SWITCH . This will prompt for the 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 appropriate functions of the web interface.

Once you have successfully logged into the KVM OVER IP SWITCH a command line will be presented and you can enter 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 made 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 command mode 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 pass-through mode for the serial port. The key sequence 'esc exit' switches back to the command mode.

5.2 Virtual Media

5.2.1 Drive Redirection

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

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. 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. *Therefore, we recommend to use the Drive Redirection with care, especially the write support.*

Disable Drive Redirection
    If enabled the Drive Redirection is switched off.
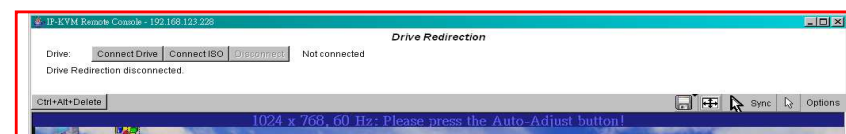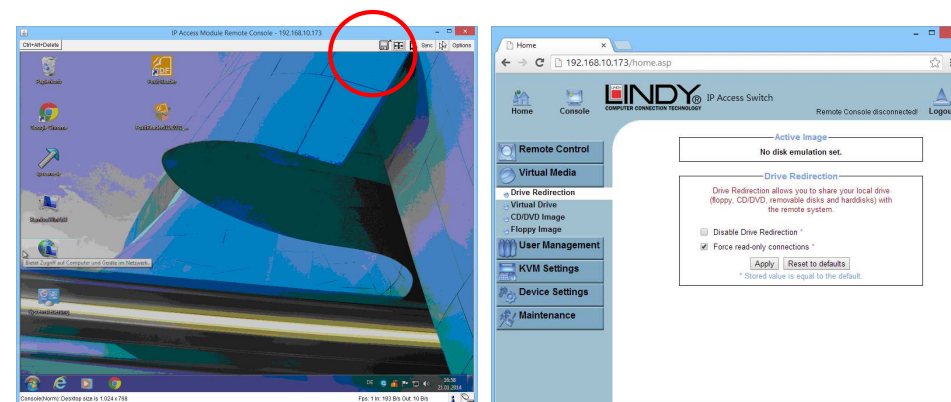
Force read-only connections
    If enabled the Write Support for the Drive Redirection is switched off. It is not possible to write on a redirected device.
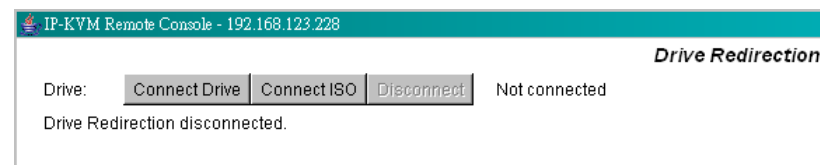
Click **Apply** to submit your changes.

The method of Drive Redirection:

Built-in Java Drive Redirection function in Remote Console
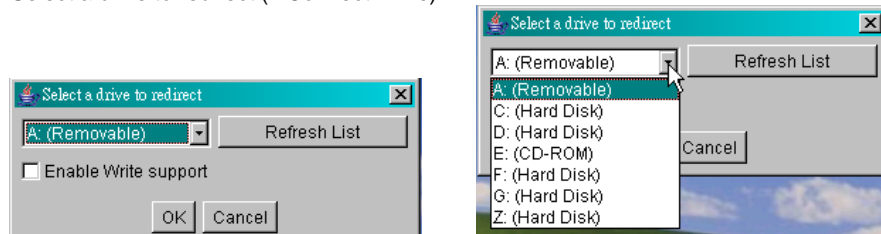
1. Run Remote Control > KVM Console.

2. Click "Floppy" icon

3. Click on the floppy icon on the remote console screen **Connect Drive** or **Connect ISO**

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

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

IMPORTANT

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

5.2.2 Create a CD-ROM/ISO Image
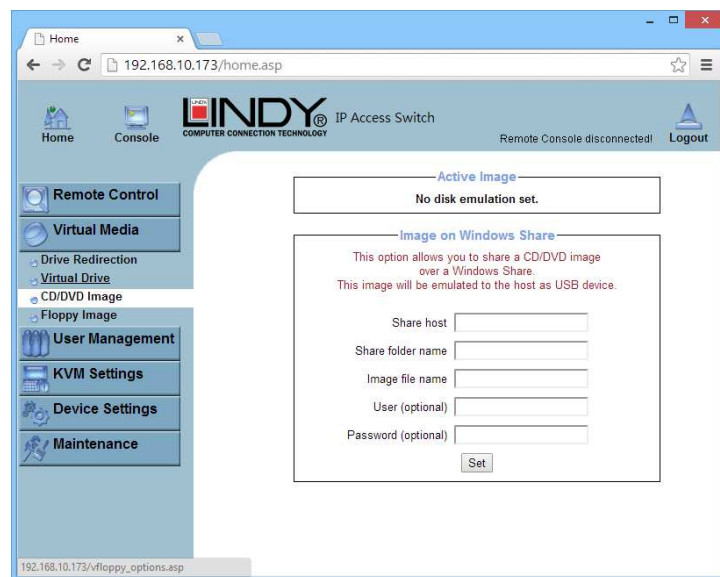
Follow the procedure below to create a CD-ROM image which can be accessed by the host system via the KVM OVER IP SWITCH .

First, on your client PC you must create an image of your CD which can be accessed by the host system.

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 CD-ROM to a file. You can use the following command:

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

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

Windows
To create the image file, use your favourite 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.

Example:

1. Create a CD image and name it **image.iso**

2. Create a folder on your client PC and name it **Test.** Copy the file **image.iso** to the folder **Test**.

3. Now you need to 'share' this folder. Right click on the folder and select the option **Sharing and Security**. Select **Share this folder** and ensure the **Share Name** is set to **Test**. Click **Permissions** to set permissions for users who access this folder, according to your requirements. Click **Apply** then **OK** to complete.

4. Next you need to mount the image via a Windows Share. In the KVM OVER IP SWITCH menu on the left hand side of the browser select **Virtual Media** and from the sub menu select **CD-ROM Image**.
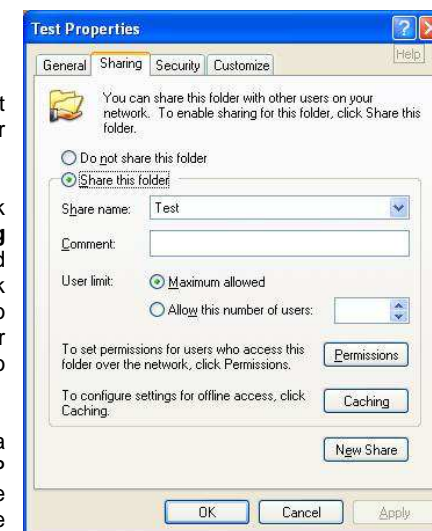
5. Input the following parameters:

Share host:	Enter the IP address of your Console PC here *(e.g. 192.168.2.103)*
Share name:	Test *(The share name of the previously created folder)*
Path to image:	image.iso *(the name of the CD image)*
User:	super *(Your user name, the default is super)*
Password:	pass *(Your password, the default is pass)*

6. Click **Set**

7. You will see the dialog below detailing the active image:

Image file set successfully

8. Click **Reactivate**. Access the console window and you will see that another CD drive has been installed on the host computer. This is the virtual drive you have just set up. You can access the uploaded CD image as though it were a regular CD. Click **Unset** to remove the image.

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

5.2.3 Floppy Disk

Follow the steps below to upload a virtual floppy image to the KVM OVER IP SWITCH and create a virtual floppy drive on the host system

Create a Floppy Image

First, on your client PC you must create an image of your floppy disk which can be uploaded to the KVM OVER IP SWITCH 's built in memory.

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.)

Windows
Windows users should use the tool **RawWrite for Windows** which is included on the supplied CD.

Launch **RawWrite**, you will see the window opposite:

Insert your floppy disk into your floppy drive. Click the **Read** tab and then click on [...]

Select a name and destination for the floppy image file and click the **Read** button. As the image is written, you will see the progress as a percentage figure in the bottom left hand corner.

When the image has been written you can upload it to the KVM OVER IP SWITCH .
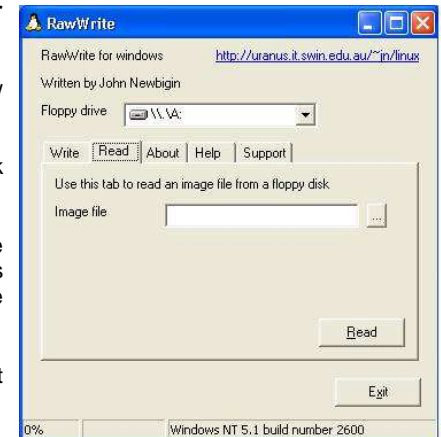
Uploading a Floppy Image

Click the **Browse** button and navigate to the location of the image file, then click the **Upload** button.

After the image has uploaded you will see the dialog below:

Click **Reactivate**. A virtual floppy drive will be installed on the host system and the image will be downloaded to the virtual floppy drive from the KVM OVER IP SWITCH . You can access the virtual floppy drive in the same way you would a regular drive.

You can download the image from the KVM OVER IP SWITCH to your remote system by clicking the **Download** button.

Clicking **Discard** removes the virtual floppy image from the KVM OVER IP SWITCH and from the hosts system.

5.2.4 Virtual Drive Options

This option allows you to disable the mass storage emulation (and hide the virtual drive) if no image file is currently loaded. To set this option, press the button **Apply**.

5.3 User Management

5.3.1 Change Password

To change your password, enter the new password in the upper entry field. Retype the password in the lower field. Click **Apply** to submit your changes.

5.3.2 Users And Groups

The KVM OVER IP SWITCH comes with 2 pre-configured user accounts that have fixed permissions. The **super** account has all possible rights to configure the device and to use all functions. The **user** account has only the permission to open and use the Remote Console. The default password for both accounts is **pass**. Ensure you change the passwords as soon as you have installed and accessed the KVM OVER IP SWITCH for the first time.

While the **user** account never sees the following options, the **super** account can change the name and password for both accounts.

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 four characters long.

Confirm password
Confirmation of the above password.

5.4 KVM Settings

5.4.1 User Console

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

User select box
This 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 necessary access rights.

Transmission Encoding
The Transmission Encoding setting allows you to change the image-encoding algorithm that is used to transmit the video data to the Remote Console window. It is possible to optimize the

speed of the remote screen depending on the number of users working at the same time and the bandwidth of the connection line (Modem, ISDN, DSL, LAN, etc.).

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

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

Manually
Allows adjustment of both compression rate and colour depth individually. Depending on the selected compression rate the data stream between the KVM OVER IP SWITCH and the Remote Console will be compressed in order to save bandwidth. Since high compression rates are very time consuming, they should not be used when several users are accessing the KVM OVER IP SWITCH simultaneously.

The standard colour depth is 16 bit (65536 colours). The other colour 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 colour depth. At lower bandwidths only 4 bit (16 colours) and 2 bit (4 grey scales) are recommended for typical desktop interfaces. Photo-like pictures have best results with 4 bit (16 grey scales). 1 Bit colour depth (black/white) should only be used for extremely slow network connections.

Remote Console Type
Specifies, which Remote Console Viewer to use.

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

Sun Microsystems Java Browser Plug-in
Instructs the web browser of your administration system to use Sun's JVM. The JVM in the browser is used to run the code for the Remote Console window which is actually a Java Applet. If you check this box for the first time on your administration system and the appropriate Java plug-in is not already installed on your system, it will be downloaded and installed automatically. The advantage of Sun's JVM is in providing a stable and identical Java Virtual Machine across different platforms. The Remote Console software is optimized for Sun JVM versions and offers wider range of functionality when run with JVM.

The KVM Java applet is issued and certified by LINDY. Therefore you have to install the LINDY certificate in every computer that you want to use to access the KVM switch. The installation process is described in section 4.1

Miscellaneous Remote Console Settings

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

Start in Exclusive Access Mode Enables the exclusive access mode immediately at Remote Console start-up. 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 the user 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
This allows 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** in Windows and DOS, which is always caught, or **Control+Backspace** on Linux 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 joined 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 will be released in reversed sequence. So the minus sign builds single, separate key presses and releases. The star inserts a pause with duration of 100 milliseconds.

5.4.2 Keyboard/Mouse

This section is slightly different for the stand-alone units 39415 and 39414 compared to the modular versions 39430, 39432, 39522 and 39636

Modular version
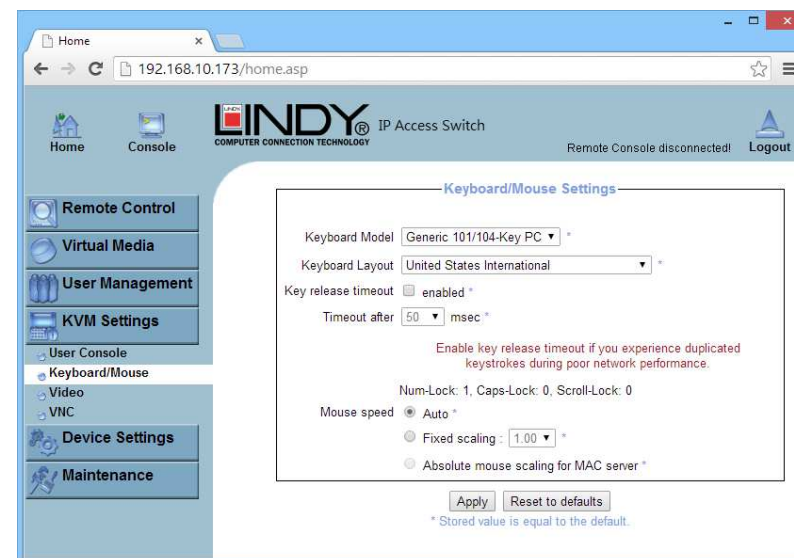
Stand-alone version – additional Host Interface menu

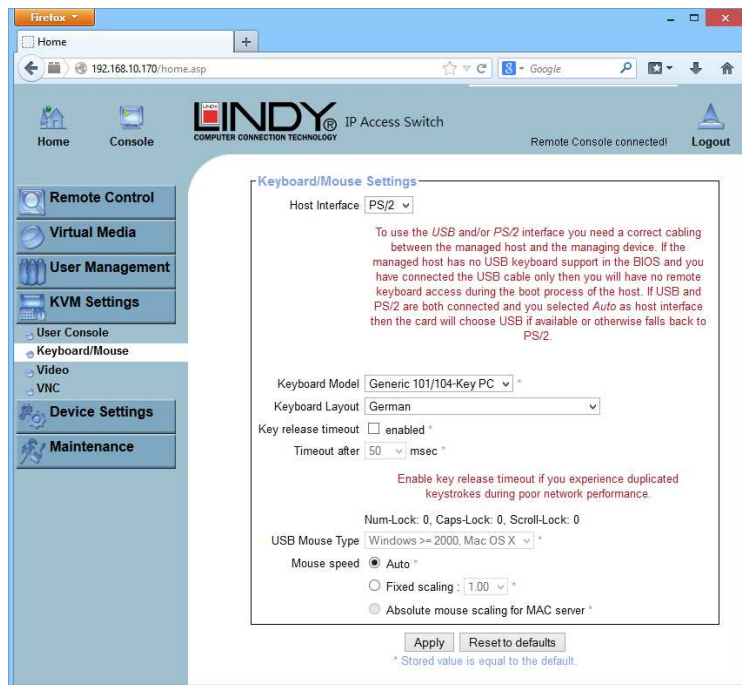The stand-alone version has the option to use either PS/2 or USB keyboard and mouse host interface. This additional option can be configured in the OSD menu:

Host Interface
Enables the interface the mouse is connected to. You can choose between **Auto** for automatic detection, **USB** for a USB mouse, or **PS/2** for a PS/2 mouse.

> *Note:* To use the USB and/or PS/2 interface you need the 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 **USB** will be selected if available, otherwise it will revert to **PS/2**.

To enable USB remote keyboard access during the boot process of the host, the following conditions must be fulfilled:
- the host BIOS must have USB keyboard support
- the USB cable must be connected or must be selected in the Host interface option

USB Mouse Type
Enables USB mouse type. Choose between **MS Windows 2000 or newer** for MS Windows 2000 or Windows XP, or **Other Operating Systems** for MS Windows NT, Linux, or OS X. In **MS Windows 2000 or newer** mode the remote mouse is always synchronized with the local mouse.

Both versions – continued

PS/2 Keyboard Model
Enables a certain keyboard layout. You can choose between **Generic 101-Key PC** for a standard keyboard layout, **Generic 104-Key PC** for a standard keyboard layout extended by three additional windows keys, **Generic 106-Key PC** for a Japanese keyboard, and **Apple Macintosh** for the Apple Macintosh.

Mouse Speed

- *Auto mouse speed* Use this option if the mouse settings on the host use an additional acceleration setting. The KVM OVER IP SWITCH tries to detect the acceleration and speed of the mouse during the mouse sync process.
- *Fixed mouse speed* Use a direct translation of mouse movements between the local and the remote pointer.

You may also set a fixed scaling which determines the amount the remote mouse pointer is moved when the local mouse pointer is moved by one pixel. This option only works when the mouse settings on the host are linear. This means that there is no mouse acceleration involved.

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

5.4.3 Video
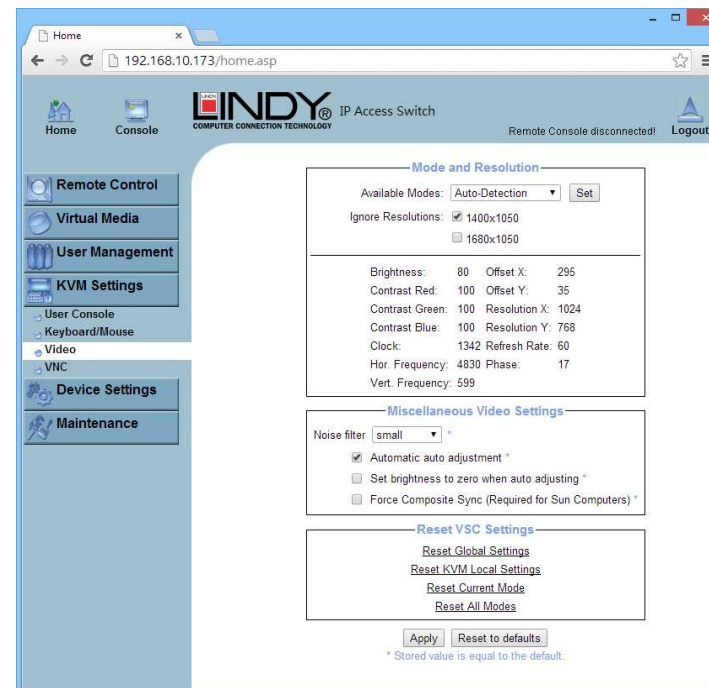
Video Settings

the If there are no video problems leave the mode in Auto-Detection

Noise filter

This option defines how the KVM OVER IP SWITCH reacts to small changes in the video input signal. 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.

5.4.4 VNC
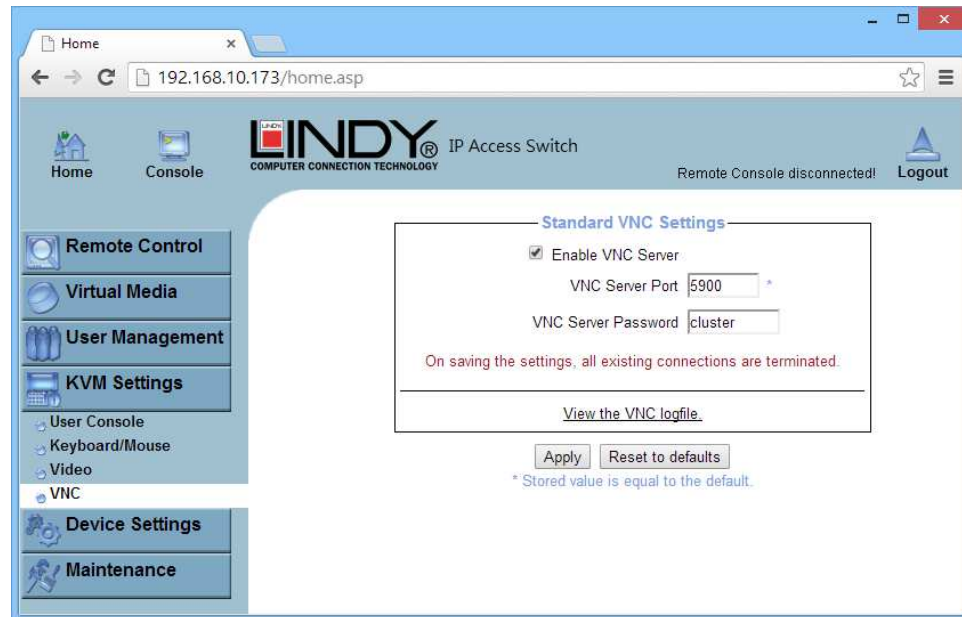
Video Settings

To use a VNC viewer to access the KVM over IP Switch the VNC server as to be enabled. Please make sure youtr firewall does not block the relevant ports.

We have tested Tight VNC that works without any problems.
Most common VNC viewers can be used, however, some may use special settings. If you want to use Real VNC please set it to video mode 3.

5.5 Device Settings

5.5.1 Network

The Network Settings panel allows network related parameters to be changed. Each parameter will be explained below. Once applied the new network settings will immediately come into effect.
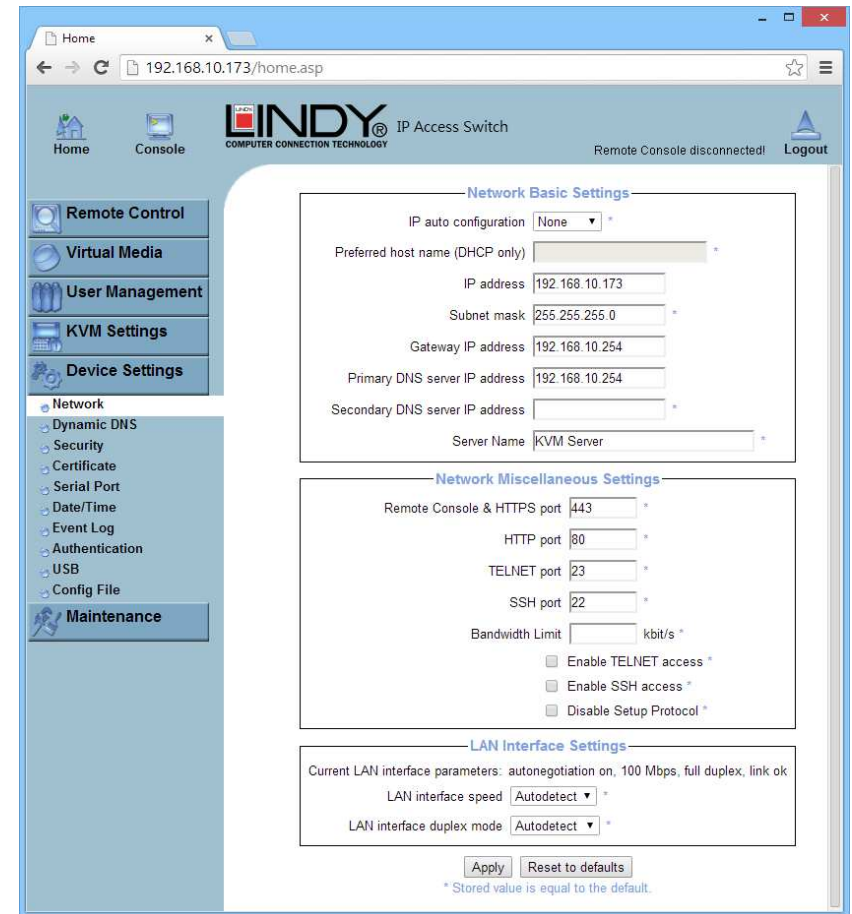
Note: The initial IP configuration is usually done directly at the host system using the special procedure described in **Section 3.**

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

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

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 OVER IP SWITCH is 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 OVER IP SWITCH 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 OVER IP SWITCH '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 OVER IP SWITCH 's HTTP server is listening. If left empty the default value will be used.

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

Bandwidth limitation
The maximum network traffic generated through the KVM OVER IP SWITCH 's Ethernet device. Value in Kbit/s.

Enable Telnet access
Set this option to allow access to ARA express using the Telnet Gateway **(see the Section called Telnet Console on page 23).**

Disable Setup Protocol
Enable this option to exclude the KVM OVER IP SWITCH from the setup protocol.

5.5.2 Dynamic DNS

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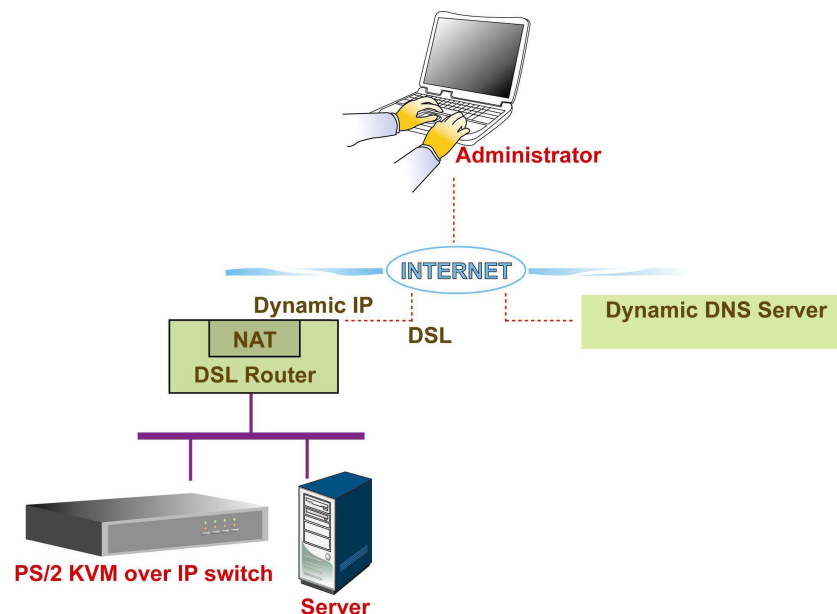

The KVM OVER IP SWITCH is reachable via the IP address of the DSL router, which is dynamically assigned by the provider. Since the administrator does not know the IP address assigned by the provider, the KVM OVER IP SWITCH connects to a special dynamic DNS server in regular intervals and registers its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

The administrator has to register an KVM OVER IP SWITCH 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. This account information, together with the hostname, is needed in order to determine the IP address of the registered KVM OVER IP SWITCH .

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

- Make sure that the LAN interface of the KVM OVER IP SWITCH is properly configured.
- Open the Dynamic DNS Settings configuration dialog
- Enable Dynamic DNS and change the settings according to your needs (see the next page).
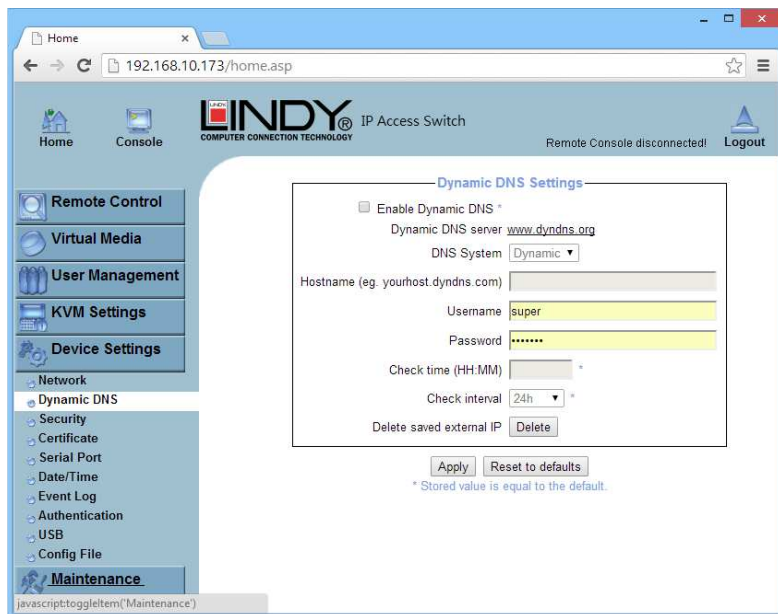
Enable Dynamic DNS
Enables the Dynamic DNS service. This requires a configured DNS server IP address.

Dynamic DNS server
This is the server name where the KVM OVER IP SWITCH registers itself in regular intervals. At the time of writing, this is a fixed setting since only dyndns.org is currently supported.

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

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

Password
The password used during manual registration with the Dynamic DNS Server.

Check time
The KVM OVER IP SWITCH registers itself in the Dynamic DNS server at this time.

Check interval
This is the interval for reporting again to the Dynamic DNS server by the KVM OVER IP SWITCH .

> *Note:* The IP ACCESS KVM SWITCH CLASSIC has its own independent real time clock.
> Make sure the time setting of the IP ACCESS KVM SWITCH CLASSIC switch is correct.
> **(See the Section called Date and Time on page 50)**

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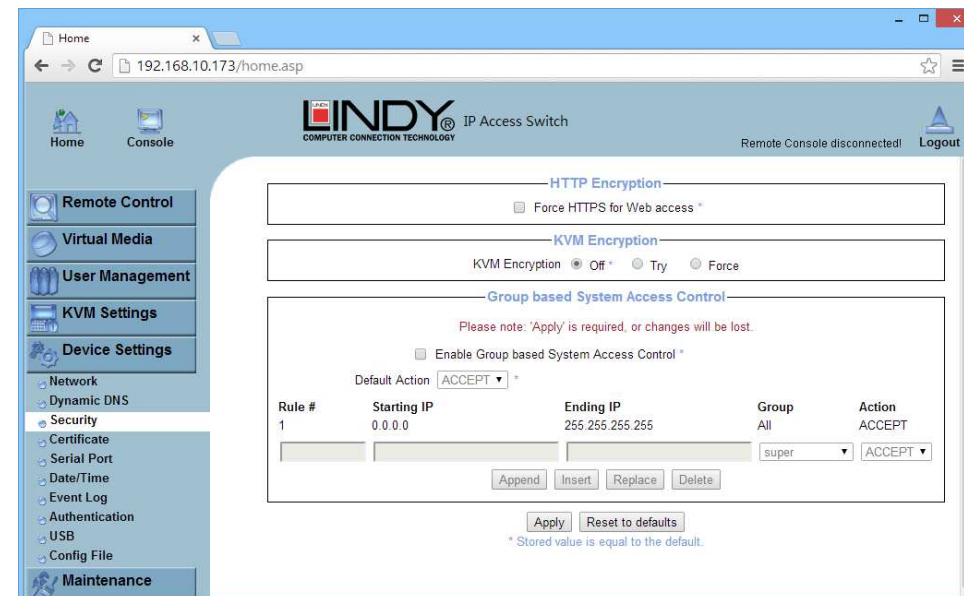
Force HTTPS
If this option is enabled, access to the web front-end is only possible using an HTTPS connection. The KVM OVER IP SWITCH will not listen on the HTTP port for incoming connections.

If you want to create your own SSL certificate that is used to identify the KVM OVER IP SWITCH **please refer to the section called Certificate on page 45.**

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's machine and the keyboard and mouse data back to the host. If set to **Off** no encryption will be used. If set to **Try**, the applet tries to make an encrypted connection. If connection establishment fails for any reason an unencrypted connection will be used. If set to **Force** the applet tries to make an encrypted connection. An error will be reported if connection establishment fails.

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

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

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

When the IP-KVM receives a TCP packet, it will process the packet with the chain rule depicted below. The process ordering is important; the packet will enter the chain at rule 1 first, if it meets the rule then take action directly, otherwise go to chain rule 2.
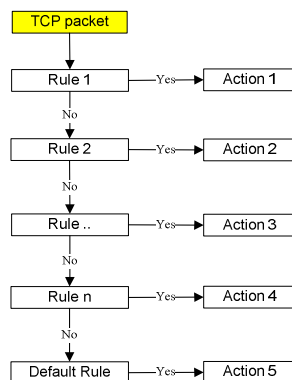
Check the "Enable Group based System Access Control" to edit the rules

Users can add a new IP filtering rule by populating the fields in the new line by using Append or Insert. Users can remove a rule by using Replace or Delete. Use Apply to save your changes.

5.5.4 Certificate

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

This certificate and the underlying secret key is the same for all KVM OVER IP SWITCH units and certainly will not match the network configuration that will be applied to the KVM OVER IP SWITCH by its user. The certificate's underlying secret key is also used for securing the SSL handshake. Hence, this is a security risk (but far better than no encryption at all).

However, it is possible to generate and install a new certificate that is unique for a particular KVM OVER IP SWITCH . In order to do this, the KVM OVER IP SWITCH 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 you claim you are, and signs and issues a SSL certificate to you.

The following steps are necessary to create and install an SSL certificate for the KVM OVER IP SWITCH :

1. Create an SSL Certificate Signing Request using the panel shown in the screen shot above. You need to fill out a number of fields that are explained on the next page. Once this is done, click on the **Create** button to initiate the Certificate Signing Request generation. The CSR can be downloaded to your administration machine with the **Download CSR** button (see the illustration on the next page).
2. Send the saved CSR 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).
3. Upload the certificate to the KVM OVER IP SWITCH switch using the **Upload** button.

After completing these three steps, the KVM OVER IP SWITCH has its own certificate that is used to identify it to its clients.

> *Note:* If you destroy the CSR on the IP ACCESS KVM SWITCH CLASSIC there is no way to get it back! In case you deleted it by mistake, you have to repeat the three steps as described previously.

Common name
This is the network name of the KVM OVER IP SWITCH once it is installed in the user's network It is identical to the name that is used to access the KVM OVER IP SWITCH 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 OVER IP SWITCH is accessed using HTTPS.

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

Organization
The name of the organization to which the KVM OVER IP SWITCH 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.

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 OVER IP SWITCH and its security.

Key length
This is the length of the generated key in bits. 1024 bits are sufficient for most cases. Longer keys may result in slower response time by the KVM OVER IP SWITCH during connection establishment.

5.5.5 Serial Port

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

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

Modem
The KVM OVER IP SWITCH 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 OVER IP SWITCH.

Connecting to the KVM OVER IP SWITCH using a telephone line allows you to set up a dedicated point-to-point connection from your console computer to the KVM OVER IP SWITCH. In other words, the KVM OVER IP SWITCH 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 OVER IP SWITCH, make sure you 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 remote access to the KVM OVER IP SWITCH 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 OVER IP SWITCH is communicating with the modem. Most 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 used by the KVM OVER IP SWITCH 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 entering a new string. Refer to your modem's manual about the AT command syntax.

- **Modem server IP address**
  This IP address will be assigned to the KVM OVER IP SWITCH 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 OVER IP SWITCH 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 OVER IP SWITCH switch and your console computer. The default value will work in most cases.

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

5.5.6 Date And Time
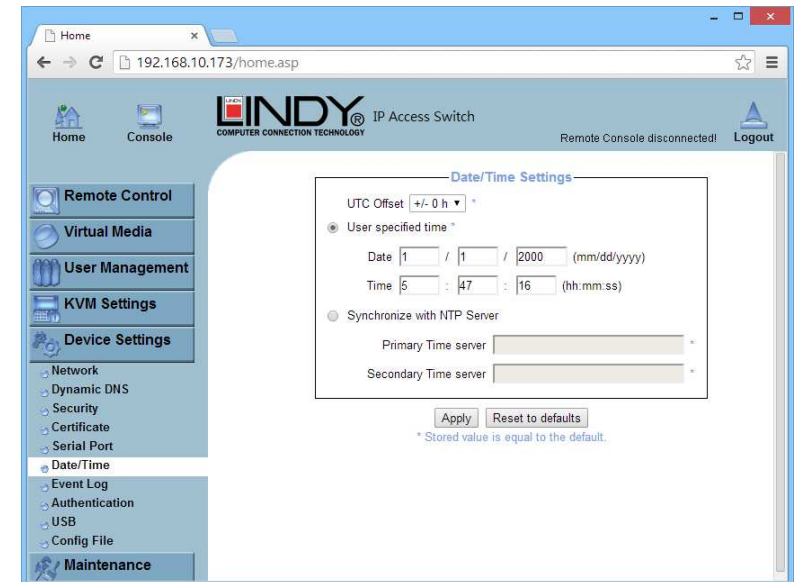
Here you can set the internal real-time clock of the KVM OVER IP SWITCH . You can adjust the clock manually or use an NTP timeserver. Without a timeserver your time setting will be lost if the KVM OVER IP SWITCH is powered down for more than a few minutes. To avoid this, you can use an NTP timeserver which sets up the internal clock automatically to the current UTC time. Because the NTP server time is always UTC, there is a setting that allows you to set up a static offset to get your local time.

Note: The IP ACCESS KVM SWITCH CLASSIC does not adjust to daylight saving time automatically. So you have to set up the UTC offset according to the local conventions of your country.

5.5.7 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.

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

List logging enabled

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

Since the KVM OVER IP SWITCH 's system memory is used to save all the information, the maximum number of possible log list entries is restricted to 1000 events. Every entry that exceeds this limit overrides the oldest one.

> *Note:* If the reset button on the HTML front end is used to restart the IP ACCESS KVM SWITCH CLASSIC all logging information is saved permanently and is available after the IP ACCESS KVM SWITCH CLASSIC has been started. If the IP ACCESS KVM SWITCH CLASSIC loses power or a hard reset is performed, all logging data will be lost. To avoid this, use one of the log methods described below.

NFS Logging enabled
Defines an NFS server to write all logging data to a file that is located there. To write logging data from multiple KVM OVER IP SWITCH units 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 **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.

SMTP Logging enabled
With this option, the KVM OVER IP SWITCH 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 an SMTP server that has to be reachable from the KVM OVER IP SWITCH and that needs no authentication at all (<serverip>:<port>).

SNMP Logging enabled
If this is activated, the KVM OVER IP SWITCH sends an 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 a trap class that consists of several fields with detailed information about the occurred event. To receive these SNMP traps, any SNMP trap listener may be used.

Warning In contrast to the internal log file on the KVM OVER IP SWITCH , 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, so you may have to delete it or move it from time to time.

5.5.8 USB Protocol Version 2.0/1.1

Here you can force the USB function to USB 1.1 version protocol. Some KVM switches may not be fully compatible with USB 2.0 protocols.

5.5.9 Configuration File
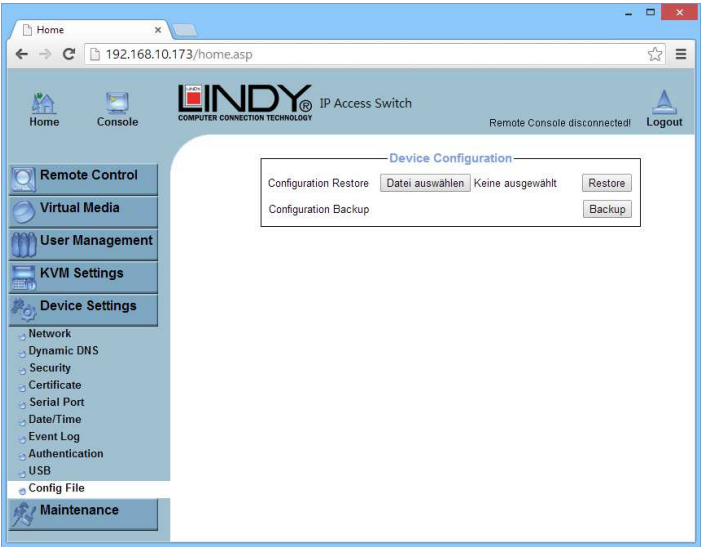
Here the device configuration can be backed up and restored in case you want to replace one unit with another one.

5.6 Maintenance

5.6.1 Device Information

This section contains a summary with various information about the KVM OVER IP SWITCH and its current firmware. It also allows you to reset the unit.
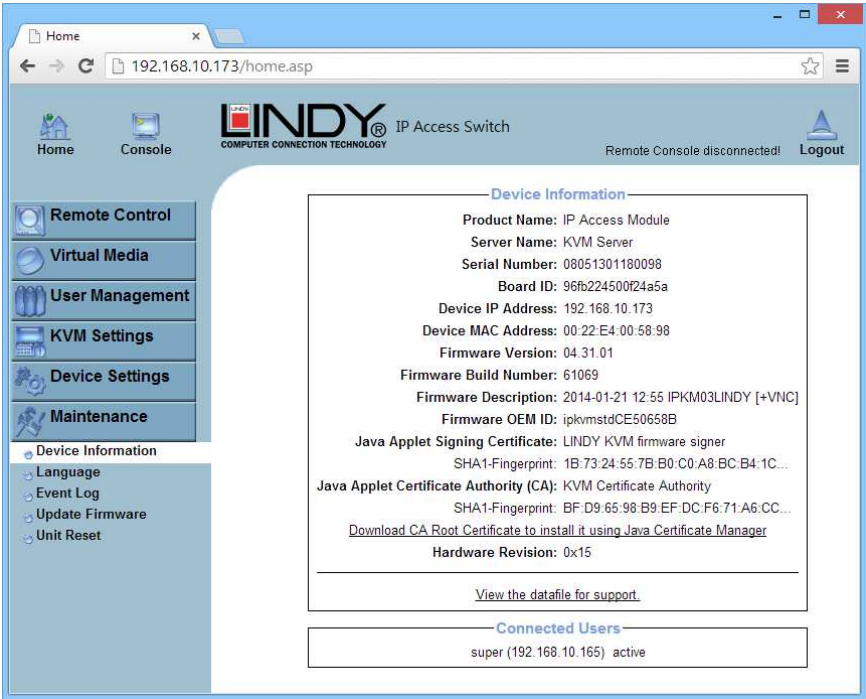
View the data file for support
Allows you to download the KVM OVER IP SWITCH data file with specific support information. This is an XML file with certain customized support information like the serial number etc. You can send this information if you contact LINDY technical support. It may help us solve any problems.

Connected Users
The example below displays the KVM OVER IP SWITCH 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) is added. For more information about this option **see the section called Remote Console Control Bar on page 17.**

To display the user activity, the last column contains either the term **active** for an active user or **20 min idle** for a user who is inactive for a certain amount of time.

5.6.2 Language Selection Menu

Select between the langauges English – French - German

5.6.3 Event Log

Displays the log list including the events that are logged by the KVM OVER IP SWITCH
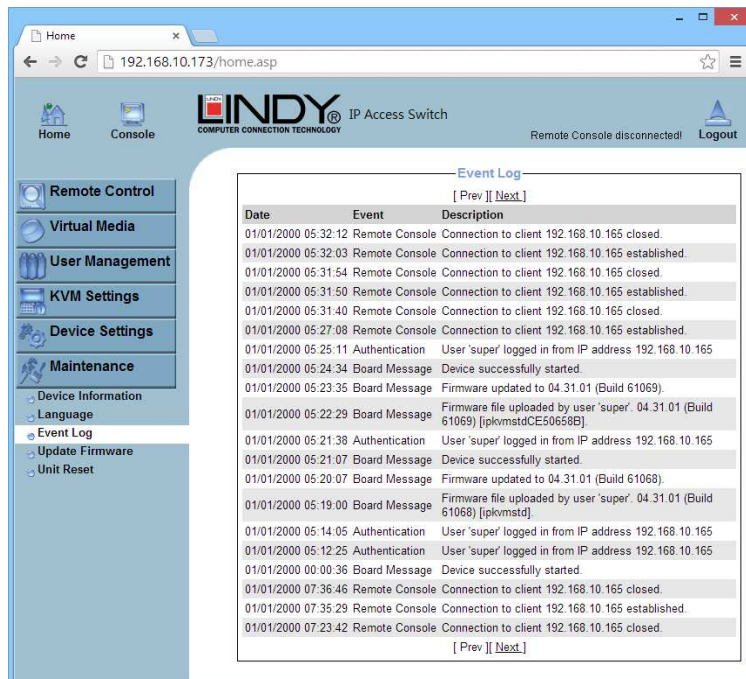
5.6.4 Update Firmware

The KVM OVER IP SWITCH is a complete standalone computer. The software it runs is called the firmware. The firmware of the KVM OVER IP SWITCH can be updated remotely in order to install new functionality or special features.
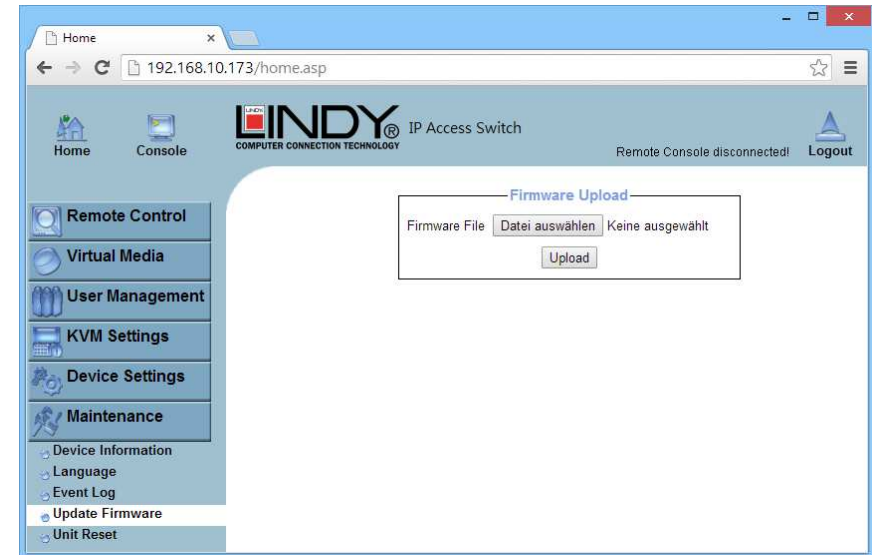
A new firmware update is a binary file which can be sent to you by email from the Technical Support team of LINDY.

1. The new firmware file is uploaded to the KVM OVER IP SWITCH. In order to do this you need to select the file on your local system using the **Browse** button on 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.

Update January 2014: Due to the large size of these upgrade files, this firmware update must be done in two steps, Step 1 and Step 2. Future updates may again be provided as a single update file. The January 2014 2-step upgrade must be performed on all units having firmware older than January 2014! This is a requirement.

2. If everything went well you will 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 **Update** button will replace the old version with the new one.

Note: This process is not reversible and may take some minutes. Make sure the KVM over IP SWITCH's power supply will not be interrupted during the update process.

The update runs fully automatically and the Login screen will automatically re-open after a few minutes. Do not interrupt this process.

5.6.5 Unit Reset

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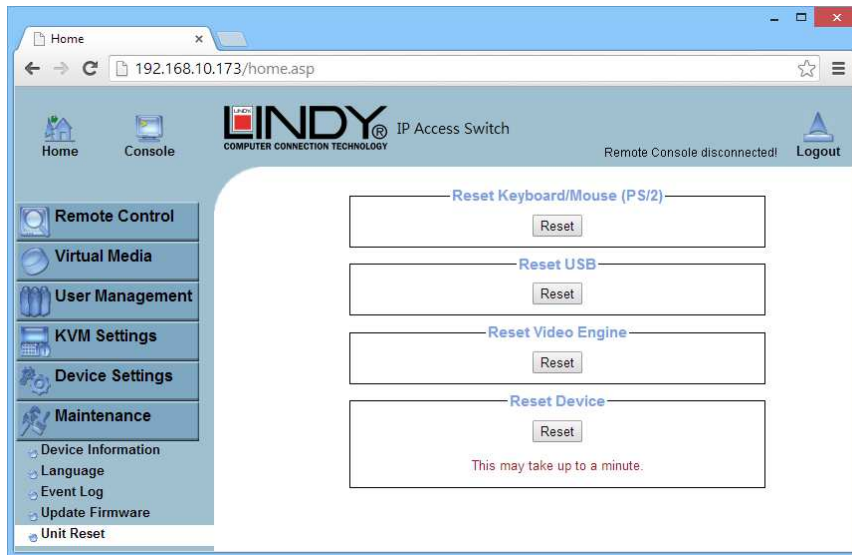
Resetting the unit itself is mainly needed to activate a newly updated firmware. It will close all current connections to the administration console and to the Remote Console.

The whole process will take about half a minute. Resetting sub devices (e.g. the video engine) will take a few seconds only and does not result in connections closing. To reset individual KVM OVER IP SWITCH functionality, click on the Reset button.

Note: Only the super user is allowed to reset the KVM OVER IP SWITCH .

6. Troubleshooting

Q 001: The remote mouse doesn't work or is not synchronized

A 001: Make sure the mouse settings in KVM OVER IP SWITCH match the mouse model. Use the **Intelligent Sync** option from the **Mouse Handling** sub menu of the Remote Console **Options** menu.

Q 002: The video quality is bad or the picture is grainy

A 002: Try to correct the brightness and contrast settings **(see Page 19)** until they are out of a range where the picture looks grainy. Use the auto adjustment feature to correct a flickering video.

Q 003: Login on KVM OVER IP SWITCH fails.

A 003: Was the correct combination of user and password given? The default user name is **super** and the password is **pass**. Furthermore, your browser must be configured to accept cookies.

Q 004: The Remote Console window can't connect to the KVM OVER IP SWITCH.

A 004: Possibly a firewall prevents access to the Remote Console. Make sure the TCP port numbers 443 or 80 are open for incoming TCP connections. Install the latest version of Java Virtual Machine,

Q 005: No connection can be established to the KVM OVER IP SWITCH.

A 005: Check whether the network connection is working in general (ping the IP address of KVM OVER IP SWITCH). If not, check the network hardware. Is the KVM OVER IP SWITCH powered on? Check whether the IP address of KVM OVER IP SWITCH and all other IP related settings are correct! Also verify that all the IP infrastructure of your LAN, like routers etc., is correctly configured.

Q 006: Special key combinations, e.g. ALT+F2, ALT+F3 are intercepted by the console system and not transmitted to the host.

A 006: You have to define a so-called **Button Key**. This can be done in the Remote Console settings.

Q 007: In the browser the KVM OVER IP SWITCH pages are inconsistent.

A 007: Check your browser cache settings. Especially make sure that the cache settings are not set to something like 'never check for newer pages'. Otherwise the KVM OVER IP SWITCH pages may be loaded from your browser cache and not from the unit.

Q 008: Windows XP doesn't awake from standby mode

A 008: This could be a Windows XP problem. Try not to move the mouse while XP goes into standby mode.

Q 009: Using MacOS X an HTTPS connection fails

A 009: You have to install the KVM OVER IP SWITCH certificate using our certificate installer, available on the utility CD. Please refer to the instructions on this CD for further information on how to install the certificate.

Q 010: Can't upload the signed certificate in Mac OS X

A 010: If an 'internal error' occurs while uploading the signed certificate either change the extension of the file to .txt or add a file helper using the Internet Explorer preferences for this type of file. Make sure that the encoding is plain text and the checkbox 'use for outgoing' is checked. Another possibility is to use a Mozilla based browser.

Q 011: Every time I open a dialog box with some buttons the mouse pointers are not synchronous anymore

A 011: 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.

7. Key Codes

This table shows the key codes used to define keystrokes or hotkeys for several functions. Please note that these key codes do not necessarily represent key characters that are used on international keyboards. They name a key on a standard 104 key PC keyboard with US English language mapping.

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

The layout for this keyboard is also shown. However, most modifier keys and other alphanumeric keys used for hotkey purposes in application programs are in an identical position, no matter what language mapping you are using. Some of the keys have aliases also; they can be named by 2 key codes (separated by a comma in the previous table).

8. Video Modes & User Permissions

Video Modes supported

The table below lists the video modes that the KVM OVER IP SWITCH supports. Please do not use any other custom video settings; the KVM OVER IP SWITCH 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, 67, 72, 75, 85, 90, 100, 120
720 x 400	70, 85
800 x 600	56, 60, 70, 72, 75, 85, 90, 100
832 x 624	75
1024 x 768	60, 70, 72, 75, 85, 90, 100
1152 x 864	75
1152 x 870	75
1152 x 900	66
1280 x 960	60
1280 x 1024	60, 75
1600 x 1200	60 (moving 1280x1024 window)

User Role Permissions

The table below lists the user role permissions granted for three user role groups: "Superuser", "Administrator" and "User"

Function	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 Firmware	-	-	x
Maintenance: Unit Reset	Keyboard/ Mouse, Video	Keyboard/ Mouse, Video	Keyboard/ Mouse, Video, Device

9. Technical Specifications

Model No.	KVM over IP SWITCH
Target Device Connection	1 x Keyboard PS/2 Mini Din 6 Pin 1 x Mouse PS/2 Mini Din 6 Pin 1 x VGA HDDB 15 Pin 1 x USB 2.0 Type B receptacle
Local Access Connection	1 x PS/2 Keyboard Mini Din 6 Pin 1 x PS/2 Mouse Mini Din 6 Pin 1 x VGA HDDB 15 Pin
Remote Access Connection	1 x RJ-45
Network Connection	10/100 Ethernet, telephone line (modem needed)
Firmware Upgrade Port	1 x Serial DB9 Pin
Max. Video Resolution	Local- 1600 x 1200 Remote- 1280 x 1024
OS Compatibility	MS Windows family, Unix, Sum Solaris, Linux, Mac OSX
Browser Compatibility	IE 6.0, Netscape 7.0, Mozilla 1.6 (or above)
IP Setting	DHCP, Bootp, Fixed IP (DDNS supported)
Management Interface	Web, Utility, Telnet, Serial port
Event Log	NFS, SMTP, SNMP trap
Housing Material	Metal
Power adaptor	Dual input- 5V/2.6A x 2 (Redundancy)
Operating Temperature	0-50 degrees C
Storage Temperature	-20 – 60 degrees C
Weight	0.7 kg , incl. accessories and packaging 2.2 kg
Size (mm)	192 (L) X 120 (W) X 44 (H)

Bandwidth Consumption

The preconfigured network speed selection simply results in a different Compression and Colour 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 IP-KVM installation is from the test results with 3D-Labyrinth screen saver at Resolution 800x600, the worst case consuming the highest network bandwidth.

	Compression	Colour 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 colour)	Video Optimized	16 bit	4.3 - 5.0 MB/s	uncompressed, synchronized video data, most bandwidth needed
LAN (high colour)	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 colours
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

Well-Known TCP/UDP Port Numbers

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

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

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

IP-KVM TCP port number

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

Remark for older versions purchased before March 2014

Note referring to Java Update 7.51 problem for already installed devices

With Java update 7.51 mid-January 2013 Oracle has enabled new security features. This update prevents to run unsigned Java applets. To resolve this problem for our KVM over IP switches No. 39414, 39415, 39432 and 39636 we have published LINDY signed KVM tools and certificates, together with a new firmware for our KVM over IP switches. For already installed as well as older devices please download the new firmware from the following link
39414 and 39415:
http://download.lindy.com/download/de/KVM_over_IP/KVMoverIPFirmwareUpgrade.zip
39432 and 39636:
http://download.lindy.com/download/de/KVM_over_IP/KVMoverIPMudolesFirmwareUpgrade.zip
and follow exactly the included installation instructions.

Alternatively, users who have installed the Java Update 7.51, can still for some time run the old tools following Oracle's workaround: https://blogs.oracle.com/java-platform-group/entry/upcoming_exception_site_list_in
Open your local Java Console and add the URL of your KVM over IP switches to the exception_site_list (Java / Security: Exception Site List). Anyhow, you will receive various Java security warnings at the start of each session and Oracle may close this option by one of the next updates.

27 January 2014.

10. Radio Frequency Energy, Certifications

GPL Remark - Open Source Software Statement

These products contain Open Source Software. They include software based on the Linux kernel as well as the following additional software/modules:

USB/IP, BOA, BUSYBOX, Brctl, network bridge, lwpriv, iwconfig, wirelees tools, HOSTAPD, wirelss tools, iptables, netfilter tools, NTPCLIENT, network tools, libminigui.so, libasound.so, ALSA library, Libpng.so, PNG library, snmpd, SNMT service, libusb, USB/IP, Mini-XML, (bind)nsupdate, dns tools.

The detailed information about the included software, including version information and source code can be found on our respective product web page at www.lindy.com, after entering the article number in the search field, as well as on our general information page to open source software
www.lindy-international.com/open_source_software and
www.lindy.co.uk/open-source-software-i403

The software mentioned is licensed under the various open source licenses. Please refer to the respective software/module/library for the respective software GPL license.

We provide this software under exclusion of any liability.

You can find and download all relevant information and source code from our websites at no cost. You can also request a CD with the souce codes of the software from us. In this case, for customers based in the UK please send a cheque issued to LINDY Electronics LTD for the amount of £80.00 to LINDY Electronics LTD, Teesside Industrial Estate, Thornaby, TS17 9JY if you are outside of the UK please send a cheque issued to LINDY-Elektronik GmbH with the amount of €95.00 to LINDY-Elektronik GmbH, Markircher Str. 20, DE-68229 Mannheim, with reference "open source software CD for No. *****", where ***** stands for the 5 digit LINDY article number. This fee applies only to the incurred cost for duplicating and shipping. Your source code request must specify the LINDY product article number clearly. Please give us a 4 to 12 weeks processing time in order for us to provide you with the latest and correct source code information.This product uses Open Source Software!

March 2014

CE Statement
This equipment complies with the requirements relating to Electromagnetic Compatibility Standards EN55022/EN55024 and the further standards cited therein.
It must be used with shielded cables only.
It has been manufactured under the scope of RoHS compliance.

CE Konformität
Dieses Produkt entspricht den einschlägigen CE Richtlinien der EU für IT-Equipment und darf nur zusammen mit abgeschirmten Kabeln verwendet werden. Diese Geräte wurden unter Berücksichtigung der RoHS Vorgaben hergestellt.
Die formelle Konformitätserklärung können wir Ihnen auf Anforderung zur Verfügung stellen

LINDY Herstellergarantie (Nur für Deutschland)
LINDY gewährt Endkunden für dieses Produkt zusätzlich und über die gesetzliche Regelung in Deutschland hinaus eine zweijährige Herstellergarantie ab Kaufdatum. Die detaillierten Bedingungen dieser Garantie finden Sie auf der LINDY Website aufgelistet bei den AGBs.

FCC Statement
Shielded cables must be used with this equipment to maintain compliance with radio frequency energy emission regulations and ensure a suitably high level of immunity to electromagnetic disturbances.
This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications.
Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at their own expense.

WEEE (Waste of Electrical and Electronic Equipment),
Recycling of Electronic Products

Europe
In 2006 the European Union introduced regulations (WEEE) for the collection and recycling of all waste electrical and electronic equipment. The Wheelie bin symbol shown indicates that this product must not be disposed of with household waste. Instead the product must be recycled in a manner that is environmentally friendly. For more information on how to dispose of this product, please contact your local recycling centre or your household waste disposal service. Each individual EU member state has implemented the WEEE regulations into national law in slightly different ways. Please follow your national law when you want to dispose of any electrical or electronic products.

Germany / Deutschland
Die Europäische Union hat mit der WEEE Direktive umfassende Regelungen für die Verschrottung und das Recycling von Elektro- und Elektronikprodukten geschaffen. Das ElektroG – Elektro- und Elektronikgerätegesetz verbietet das Entsorgen von entsprechenden, auch alten, Elektro- und Elektronikgeräten über die Hausmülltonne! Diese Geräte müssen den lokalen Sammelsystemen bzw. örtlichen Sammelstellen zugeführt werden! Dort werden sie kostenlos entgegen genommen. Die Kosten für den weiteren Recyclingprozess übernehmen die Gerätehersteller.

France
En 2006, l'union Européenne a introduit la nouvelle réglementation (DEEE) pour le recyclage de tout équipement électrique et électronique. Chaque Etat membre de l' Union Européenne a mis en application la nouvelle réglementation DEEE de manières légèrement différentes. Veuillez suivre le décret d'application correspondant à l'élimination des déchets électriques ou électroniques de votre pays.

Italy
Nel 2006 l'unione europea ha introdotto regolamentazioni (WEEE) per la raccolta e il riciclo di apparecchi elettrici ed elettronici. Non è più consentito semplicemente gettare queste apparecchiature, devono essere riciclate. Ogni stato membro dell' EU ha tramutato le direttive WEEE in leggi statali in varie misure. Fare riferimento alle leggi del proprio Stato quando si dispone di un apparecchio elettrico o elettronico. Per ulteriori dettagli fare riferimento alla direttiva WEEE sul riciclaggio del proprio Stato.

LINDY No. 39414, 39432, 39636

www.lindy.com

For Commercial Use Only
Tested to comply
with FCC Standards