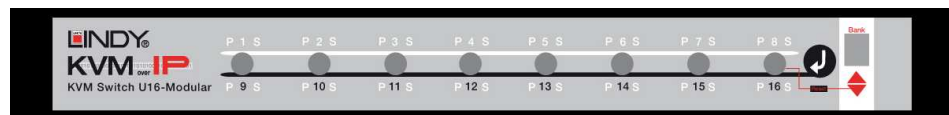# LINDY®

COMPUTER CONNECTION TECHNOLOGY

U8/16-Modular KVM Switch with modules:
Cat.5 Extender and IP Access Modules

User Manual   *English*

LINDY No. 32530, 32531

www.lindy.com

CE For Commercial Use Only
Tested to comply
with FCC Standards

CONNECTED BY LINDY®

The modular LINDY KVM Switch series U8/16

The U8/16 KVM switch series provides either 8 or 16 KVM server ports supporting both PS/2 and USB keyboard and mouse connections. This KVM switch series incorporates a modular concept design which allows for dual console access. The local console port allows direct access whilst a second console option permits remote access either via remote IP or via a remote Cat.5 extender Unit. This option allows system administrators to access and administrate their servers and KVM switches from a remote office workstation. The required optional IP or Cat.5 access modules can be purchased separately and are simply installed into the back of a U8/16-Modular KVM Switch.

This manual also covers the *KVM Switch U8/16-C*, another version of this modular KVM switch series that is used only in conjunction with the modular LINDY *KVM LCD Terminals U8/16-C*. U8/16-C models can only be installed in the back of an appropriate 19" LCD drawer and do not have a display or front panel controls fitted. Any references to front panel display and switch buttons in this manual does not apply to the modular version U8/16-C.

About this manual

This manual is divided into five sections.
- The first section is an introduction to the U8/16, U8/16-C, U8/16-C5 and U8/16-IP
- The second section deals with installing and connecting the switch
- The third section describes the basic operation of the KVM switch from the locally connected console
- The fourth section describes operation via the remote Cat.5 Extender
- The fifth section describes operation and access via remote IP

Contents

Section 1

Introducing the U8/16

1.1. About the U8/16 concept

The U8/16 series KVM switch supports traditional PS/2 mouse and keyboard connections as well as modern USB connections. The U8/16 series supports the following computer platforms, PC, Mac and SUN.

Combined KVM cables are used to connect the servers to the KVM switch's computer ports. Connections to the servers use a traditional VGA connector, one PS/2 mouse connector and one USB mouse & keyboard connector. To connect a server via USB only the PS/2 connector is not used; to connect the server via PS/2 the green PS/2 mouse connector is plugged into the servers mouse port and a special USB to PS/2 keyboard adapter is attached to the USB cable and then plugged into the server's PS/2 port.

The U8/16 series KVM switch introduces a modular concept for dual console operation. In addition to the local console port the switch also offers a secondary remote access option either via IP or via a remote Cat.5 extender unit. Using this method, system administrators are able to access and administrate their servers and KVM switches from a remote office workstation. Depending on your application the appropriate optional access modules can be purchased separately and are simply installed into the back of the U8/16-Modular KVM Switch.

This advanced 8/16 port KVM switch allows direct control of up to 16 computers from a single KVM (Keyboard, Video, and Mouse) console. The switch can also be daisy chained with further KVM Switch U8/16 to control up to 128 servers/workstations from 8 daisy chained 16 port KVM switches.

Three methods of switching between the connected computers are available: 1. by pressing the front panel push buttons; 2. by using keyboard hotkeys; or 3. via OSD (On Screen Display).

1.2. U8/16-Modular with IP Access module: U8/16-IP

KVM over IP technology allows a simple web browser interface to be used to access the switch and the connected computers via a local area network (LAN) or, when connected to a wide area network (WAN), access to the switch and the connected computers can be achieved from almost anywhere in the world.

Remote & local control of multiple computers
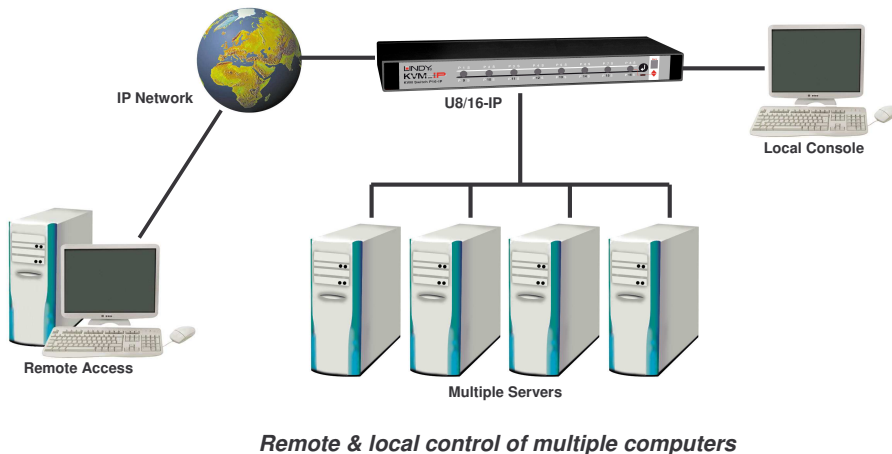
The U8/16-IP provides a non-intrusive solution for remote access and control because the software runs on its embedded processors only, so there's no interference with computer operation, or impact on network performance. The U8/16-IP also features remote mass storage support; a USB connection from the switch to one of the connected computers allows virtual storage to be set up on the host and accessed from the client.

1.3. U8/16-Modular with Cat.5 Access module: U8/16-C5

If the Cat.5 KVM Extender module is installed it will allow remote access to the KVM switch U8/16 and its connected servers via a dedicated Cat5e/6 RJ45 cable with a maximum length of up to 100m @ 1024 x 768. The remote console consists of a Cat.5 Extender receiver unit which is situated at the remote administrator's desk. The remote receiver unit also includes a KVM switch function which allows the administrator to either work on his local workstation or alternatively switch to access the KVM switch and its connected servers.

The Cat5e/6 KVM Extender provides real time access without any signal conversion and delays, whilst the IP Access module converts the VGA and keyboard/mouse signals into a TCP/IP data stream and sends them via the LAN/WAN connection to the remote user. The performance of the IP access connection and response time will vary depending upon available bandwidth and traffic throughput.

1.4. KVM compatibility and backward compatibility with LINDY P-series KVM switches

The U8/16 series KVM switches are compatible with almost any KVM switches using STANDARD VGA, keyboard and mouse signals. The U8/16 is also compatible with older LINDY P-Series KVM switches. Please note compatibility is only provided via the server ports of the U8/16 series KVM switch but not via the daisy chain ports! Therefore when customers are willing to mix U- and P-series KVMs (or other brand KVMs) it has to be done via port cascading because daisy chain configuration of mixed U- and P-series KVMs cannot work. When using the port cascading the main hotkey of the U-series KVM has to be changed (to an available hotkey from the KVM OSD menu) so it will not conflict with the SCROLL LOCK hotkey of the P-series KVMs or third party KVM switches.

1.5. Product Features

- 8/16 port KVM switch in a 1U, 19" rackmount size design
- Built-in daisy chain port allows daisy chaining of up to 8 LINDY KVM switches U or P series to be connected to support up to 128 computers
- Local console operation plus optional KVM over IP or KVM over Cat.5 control
- Remote mass storage device support for KVM over IP access for version U8/16-IP
- Supports all commonly used operating systems
- Support for PC, Mac and Sun computers with USB ports
- Hot Plug Support - add or remove computers and KVM switches for maintenance without powering down the switch or the connected computers
- High Quality Video – Local console supports display resolutions of up to 1920x1440
- No Software Required for local or Cat.5 KVM access - easy PC selection via On Screen Display Menu, Push Buttons or Keyboard Hot Keys
- Provides various Hotkeys (Scroll-Lock/ Caps-Lock/ Num-Lock/ L-Alt/ L-Ctrl/ L-Win/ R-Alt/ R-Ctrl/ R-Win) for switching computer port and other control functions
- Integrated password security protection for up to 8 users + admin with access control list restrictions for the users
- Eight character password protection and search function for server name
- Remote IP enterprise security architecture, password protected using encrypted data transmission either via secured web browser session
- Auto Scan Mode for monitoring computers with adjustable scan time from 5~99 seconds
- Keyboard status is automatically restored when switching between computers
- LED Display for easy status monitoring
- Buzzer sound for port switching confirmation
- Uses special single connector USB/PS/2 + VGA KVM cables with 15 Way Hi-Density connectors at the KVM Switch end
- Maintains continuous keyboard and mouse emulation

1.6. Package Contents

- LINDY KVM Switch U8/16 modular KVM switch
- Power Adapter
- 19" Rackmount Kit
- KVM Daisy Chain Cable
- Utility & Manual CD
- Printed Quick Start Guides

1.7. Optional Cables and Accessories (not included)

This KVM switch requires a standard VGA monitor, USB keyboard and mouse for direct connection to the local console port.

To connect each individual computer to the switch, you will need to purchase special LINDY KVM system cables as listed below. If the connected computers are PS/2 only then you can use the PS/2 version P16 and P-XT/-IP series system connection cables.
To connect a USB computer you will require an additional PS/2 female to USB male adapter available as LINDY part No. 70510.

U8/16 KVM Cable (15 Way HD Male to 15 Way HD Male + 2x PS/2 Male) + USB Adapter

+ Adapter keyboard PS/2 female
→ USB A male

- U8/16, P16, P8/16XT, P16-IP series KVM Cable **with PS/2 only**
  - 1m   LINDY No. 32510
  - 2m   LINDY No. 32506
  - 3m   LINDY No. 32507
  - 5m   LINDY No. 32508
- U8/16 series PS/2 keyboard female to USB male adapter LINDY No. 70510

Daisy Chain Cable (included)
One special HD-15 system KVM daisy chain cable with all pins connected is included with the switch. This cable must be used to daisy chain multiple U-series KVM switches – standard VGA cables may not work correctly as not all cables support all pins connected.
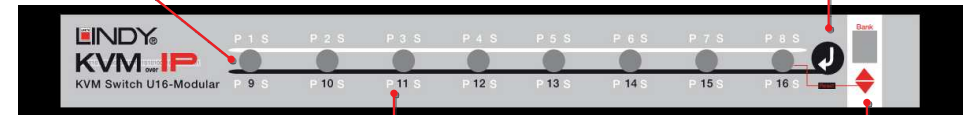
Section 2

Hardware Installation

2.1. Product Information & Connection Guide

Port Select Button
Used for direct port selection. To access ports 1 to 8 simply press the button; for ports 9 to 16, press the '⏎' button on the front panel and the required port button simultaneously.

Shift Button
This button allows ports 9 to 16 to be selected.

Port LED Display
When the LED labelled '**P**' is illuminated **green** a computer attached to this port is powered on. When the LED labelled '**S**' is illuminated **red**, the KVM console is connected to this port. If this LED flashes, the console is connected to this port, but either no computer is attached, or the attached computer is not switched on.

Bank Select Button
Pressing this button switches 'banks' and allows the computers connected to 'slave' switches in a cascaded installation to be selected. The LED above will display the selected bank. Pressing this button at the same time as the port 8 button resets the switch.

Make your connections to the switch as detailed below.
Ensure all devices are switched off before connecting. Once all connections have been made, power on the switch, your monitor, and then the connected computers in that order.

Local Console Ports
Connect your USB keyboard, VGA monitor and USB mouse here. (Not for models U8/16-C)

Computer Connection Ports
You can connect up to 16 computers to these ports using dedicated KVM cables. '**PC1**' refers to the first port, '**PC2**' to the second and so on...

Daisy Chain Ports
Allows a slave U-Series KVM switch to be connected to the U8/16 using a special KVM daisy chain cable.

Cat.5 Extender Port (only when equipped with Cat.5 KVM Extender Module!)
Use an appropriate length RJ45 cable to connect to the remote Cat.5 KVM Extender Receiver unit at the remote location. This module port may be equipped either with Cat.5 or IP remote access module or remain empty.

Power Connection
Connect the supplied power adapter here. Although the computers connected to the switch may be able to supply enough power to the unit, erratic operation may occur if the power supply is not used.

Optional remote access Cat.5 or IP module installation
If you want to use an optional remote access Cat.5 or IP module, please install it in the slot at the rear of the switch prior to powering up the switch and the connected computers.

2.2. Rackmount Installation

Before you start installation please verify that all parts are included according to the package contents.

If you want to install the KVM Switch in a 19" server rack please attach the enclosed 19" rackmount brackets using the screws provided.
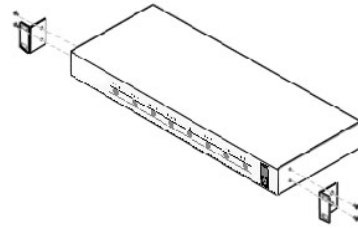
2.3. Cascading / Daisy Chaining of multiple KVM Switches

At the time this manual was written (September 2007) the U8/16 KVM switch range may be cascaded with other LINDY U-Series KVM switches only. Later versions of the new C5-8/16 series KVM switches will be introduced that will also be daisy chainable with the U series. All other brands and models of KVM switches may be cascaded with LINDY U-series KVM switches via the computer ports 1-16 of the U-series KVM switch.

To connect an additional **SLAVE** switch to the **MASTER** (or previous) switch, you must use the included special KVM system daisy chain cable. Standard VGA cables may not work correctly as not all cables support all pins connected.

Step 1 - Connect the local console

Connect your keyboard, mouse and monitor to the console ports of the U8/16 **MASTER** KVM Switch.

Step 2 – Connect the first Slave

Use the daisy chain cable to connect the *daisy chain port* of the **MASTER**/previous KVM Switch and the other end to the *local console port* of the next **SLAVE** switch.

Step 3 – Cascading / Daisy chaining

Repeat the previous step to daisy chain mores switches. Each individual switch in the chain represents a different *Bank.* The **MASTER** switch is Bank 1 and each cascaded **SLAVE** follows on as Bank 2, 3, 4 etc. **You may cascade a maximum of eight switches/banks.**

Bank 1 (Master)

Bank 3... to a maximum of 8

Cascading KVM Switches by daisy chaining
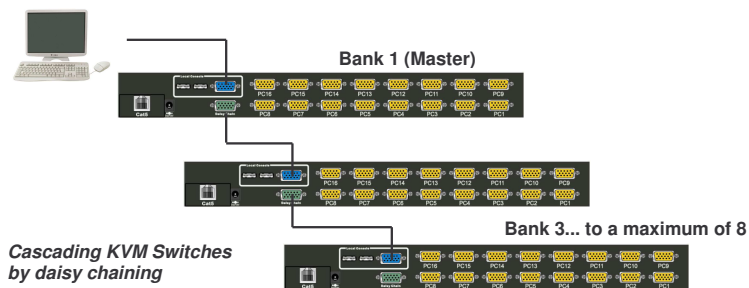
Step 4 – Resetting the Switches

After you have connected and switched on the **SLAVE** switches and computers, all of the KVM switches may need to be reset. First, reset the **SLAVE** switch at the end of the daisy chain and then reset all of the other **SLAVE** switches up to the **MASTER** U8/16 switch.

To reset the switch, press and hold the Bank button and port 8/16 button on the front panel of the switch.

Each **SLAVE** switch should now show a dash in its BANK display.

Now, reset the **MASTER** switch - it will show a 1 in the BANK display. Each **SLAVE** switch BANK display will now change to a number according to its position in the daisy chain.

Section 3

KVM Switch Operation

3.1. KVM Switch Operation

> *Important note:* Your monitor will only display one PC signal at any one time. All keyboard and mouse commands are sent to this PC only. After initial power up, port 1 is active by default.
>
> **When a PC is connected to the currently selected port and it is not switched on, or is in sleep mode, the monitor will not display any signal.**

3.1.1. Password Security

When you power on the U8/16 it will ask you for a user name and a password. The **default user name and default password for both is eight zeros –"00000000"**. Please key in eight zeros in the password field. You may use the "0" from the standard keypad but not from the numeric keypad.

Note: Please don't change the password until you are familiar with the operation of the OSD menu – i.e. keep the default password "00000000". Otherwise, if you forget the password, you will need to send the switch back to LINDY for maintenance to clear the password.

The U8/16 OSD security feature offers up to 8 users + 1 SUPERVISOR.
A user specific access control list is available from the OSD of the KVM switch and can be configured by the supervisor.

3.1.2. Hot Plug Support

The U8/16 supports a "Hot Plug" function for easy addition or removal of computers. The user can arrange or maintain the computers and daisy chained KVM Switches as follows:

a. A computer can be disconnected and reconnected to the same or a different port of the KVM switch without having to power it off as long as it is currently not connected to the console. In most cases the PS/2 mouse and keyboard signals will be maintained and will not be lost.

b. The mouse driver of the computer has to support the hot plug function or the computer may need to be rebooted when it is reconnected.

c. You can unplug your mouse or keyboard from the console port and plug it back in at any time. You should not use different types of mice when performing this.

d. A SLAVE KVM switch can be added or removed at any time, but after adding or removing a switch it may be required to reset all of the KVM switches. But you DO NOT need to reboot the computers.

> *Please note:* Some Operating Systems such as certain Unix versions are unable to support the "Hot Plug" function. If you Hot Plug when using this kind of O.S., it may cause unpredictable operation or may shut down the computer. Before attempting to use the Hot Plug feature, please check that the O.S. and mouse driver support this function.

3.1.3. Computer / Port Selection

You can select the computer you want to access in one of three different ways:

- Front panel push button selection
- Keyboard hotkey selection
- On screen display menu selection

3.1.4. Port LED Display

The front panel of the switch has two LEDs for each port.

When the LED labeled "**P**" is illuminated **GREEN** a computer attached to this port is powered on. When the LED labeled "**S**" is illuminated **RED,** the KVM console is connected to this port. If this LED flashes, the console is connected to this port but either no computer is attached, or the attached computer is not switched on.

3.1.5 Front panel push button selection

You can select a computer by pressing the appropriate port push button. Each push button refers to two ports. To access ports 1 to 8 simply press the button; to access ports 9 to 16 you must push the button marked "↵" and the required port button simultaneously.
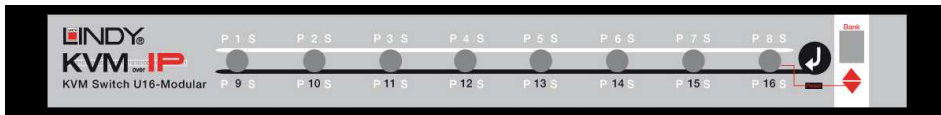
For cascaded KVM Switches you can ONLY use the port selection push buttons on the MASTER U8/16 Switch to switch the SLAVES. You may also switch via OSD or keyboard hotkey.

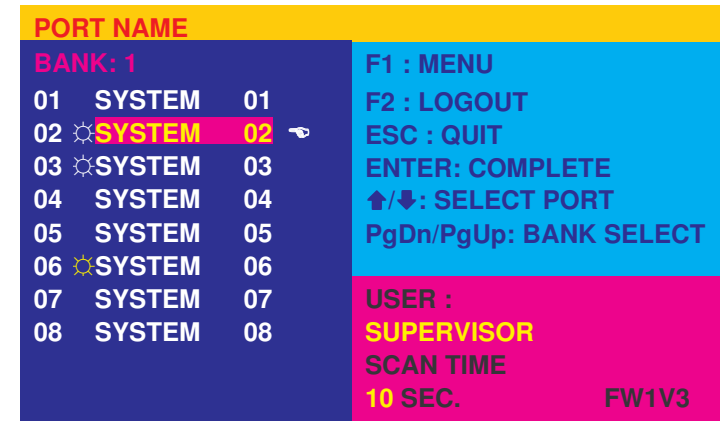
3.2. Keyboard Hotkey Selection

You can also conveniently select the computer to be accessed and displayed by switching ports through simple keyboard key sequences. To send commands to the KVM switch, **the "SCROLL LOCK" key must be pressed twice within 2 seconds.** You will hear a beep to confirm that the keyboard is in hotkey mode. If you have not pressed any key in hotkey mode within 2 seconds, the keyboard will return back to Operating System control status.

For the U-series KVM switches it is possible to change the "SCROLL LOCK" hotkey to certain other hotkeys by selection from the OSD menu. This can help to prevent hotkey collisions with other hotkeys from other devices. To do so you have to enter the Main OSD Menu by typing SCROLL LOCK twice and then pressing the SPACEBAR within 2 seconds.
To invoke the On Screen Display Menu press the following hotkeys:

If the KVM switch prompts for your user name and password while no user names and passwords have been assigned you may use eight zeros "00000000" for each, user name and password.

PORT NAME		
BANK: 1		**F1 : MENU**
01 SYSTEM 01		**F2 : LOGOUT**
02 ☼SYSTEM 02		**ESC : QUIT**
03 ☼SYSTEM 03		**ENTER: COMPLETE**
04 SYSTEM 04		**⬆/⬇: SELECT PORT**
05 SYSTEM 05		**PgDn/PgUp: BANK SELECT**
06 ☼SYSTEM 06		
07 SYSTEM 07		**USER :**
08 SYSTEM 08		**SUPERVISOR**
		SCAN TIME
		10 SEC. FW1V3

Select **F1: MAIN** from the MAIN OSD Menu and then **06 HOTKEY** to go to the hotkey selection menu. Select any of the available hotkeys: Scroll Lock / Caps Lock / Left Ctrl / Right Ctrl / Left Alt / Right Alt / Left Win / Right Win. Confirm your selection by pressing the ENTER key. From now on the new hotkey is permanently changed.

**Direct Port Selection / Keyboard Hot Key Commands:**
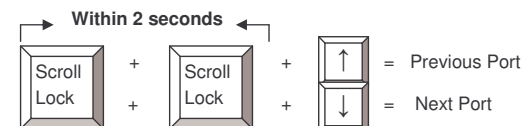
Tip: Hold the arrow key down, or press multiple times, to cycle through the ports
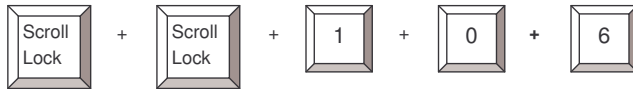
Please note: If you change the default hotkey always remember to enter the new hotkey!
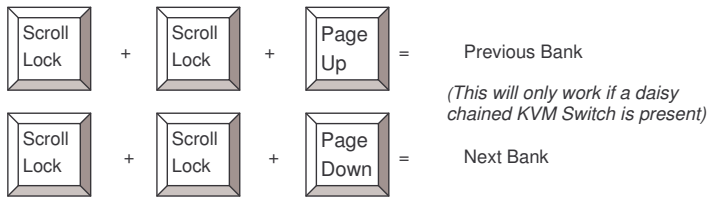
KVM Switch / Bank Selection:

The U8/16 supports daisy chaining of up to 8 KVM Switches (Banks). Therefore, when using direct hotkey port selection you must include the key sequence for the KVM Switch/Bank:
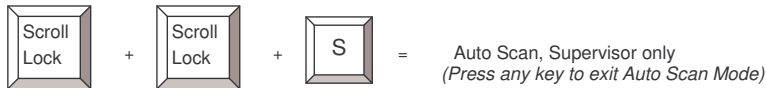
| Scroll Lock | + | Scroll Lock | + | Bank No 1~8 | + | Port No. 01~04 (4 port) 01~08 (8 port) 01~16 (16 port) |
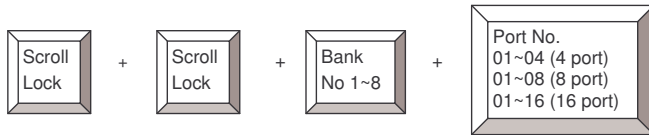
Example: To access a computer attached to Port 6 of the first KVM Switch you should press the following hotkeys:

| Scroll Lock | + | Scroll Lock | + | 1 | + | 0 | + | 6 |

To use hotkey switching to access another KVM Switch / Bank:

| Scroll Lock | + | Scroll Lock | + | Page Up | = | Previous Bank |

(This will only work if a daisy chained KVM Switch is present)

| Scroll Lock | + | Scroll Lock | + | Page Down | = | Next Bank |

Auto Scan mode:

| Scroll Lock | + | Scroll Lock | + | S | = | Auto Scan, Supervisor only *(Press any key to exit Auto Scan Mode)* |

Please note: If you change the default hotkey always remember to enter the new hotkey!

Available hotkey commands:

Command	Action
Space bar	Enter into OSD Main Menu
101 ………… 816	Bank + port number direct selection
P	user / supervisor log out
U	SUPERVISOR only: turn Security function ON / OFF. If security is OFF no password login is required and Access Control list is disabled!
R	SUPERVISOR only: Set the OSD back to factory default. Except User Security settings.

Important Note:

Always keep in mind to include leading zeros for all ports below 10! i.e.**104** for Port 4 of the first switch.

Bank no. and Port no. selection must be made using the numeric keys on the keyboard. Keys on the numeric keypad are not available as hot key commands!

3.3. On Screen Display Menu (OSD) Port Selection

The On Screen Display menu provides a lot of information about the U8/16 and the attached computers, and offers advanced administration features and full KVM Switch control to the user.

When you have logged into the KVM switch with your password a STATUS OSD display will be displayed:

102 = Bank 1, Port 02
Scroll Lock = recent hotkey

1 0 2   ☼ **SYSTEM 01**
Scroll Lock

System 02 :
System = PC name
02 = selected port

Auto-LOGOUT function
• During normal operation if no input from the keyboard or mouse is made for a period of 10 minutes the KVM switch will turn off the display. It will display the Login window asking for user name and password – as long as password security is not disabled - upon the next keyboard or mouse entry. After a minute of keyboard/mouse inactivity the monitor will be turned off (you may notice the monitor LED turning from green to orange color).

You now can enter the OSD Main Menu by typing the hotkey twice followed by SPACEBAR.

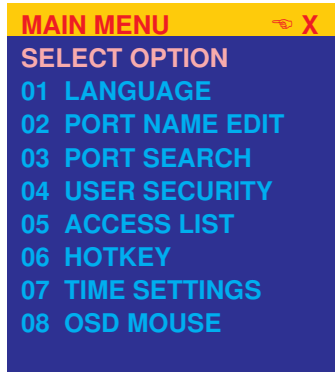| PORT NAME		
BANK: 1		**F1 : MENU**
01 SYSTEM 01		**F2 : LOGOUT**
02 ☼SYSTEM 02 ☜		**ESC : QUIT**
03 ☼SYSTEM 03		**ENTER: COMPLETE**
04 SYSTEM 04		**⬆/⬇: SELECT PORT**
05 SYSTEM 05		**PgDn/PgUp: BANK SELECT**
06 ☼SYSTEM 06		
07 SYSTEM 07		**USER :**
08 SYSTEM 08		**SUPERVISOR**
		SCAN TIME
		10 SEC. FW1V3

Using the cursor keys you now can toggle through the ports / computers connected on bank 1 and select any by pressing the ENTER key. Please note that the ▮ symbol indicates all active computers connected to the ports. Computers connected to ports not showing this symbol may be either switched off or in standby / power down mode. If you switch to any of these ports then you will not have a video signal displayed and will have to boot or wake up the connected computer. To access ports 9…16 simply scroll down with the cursor key below port 8.

To select any slave KVM switch select its bank number by pressing the Page Up / Down keys. The appropriate bank number will then be displayed on the left hand side near top and the connected computers to this slave KVM switch can be selected.

Or you can access any of the further OSD configuration menus from the right side of the main menu by typing the F1 command key. ESC quits from the OSD. F2 logs you out, either from the OSD only if no password security is disabled or totally into Logon screen if password security is enabled. F2 logout is only available from the main OSD menu.

The OSD Menu displays further OSD configuration menus when selecting F1 from the main OSD menu.

From the F1 Menu further submenus can be selected to configure the switch settings. In the submenus you can either use the cursor up/down keys or the mouse for navigation or simply press the number of the further option menu. You can go one layer back by clicking on the ☞ symbol with the mouse. ESC key quits the OSD completely.

MAIN MENU ☞ X
SELECT OPTION
01 LANGUAGE
02 PORT NAME EDIT
03 PORT SEARCH
04 USER SECURITY
05 ACCESS LIST
06 HOTKEY
07 TIME SETTINGS
08 OSD MOUSE

Select **01 LANGUAGE** – for Supervisor only – to set the OSD language to either: English, French, German, Italian, Spanish, Japanese, Chinese or Russian.

Select **02 PORT NAME EDIT** – for Supervisor only – to change / assign names to the computers attached to the appropriate ports. The names can be up to 10 characters long, all upper case.

Select **03 PORT SEARCH** – all users – to search for any computer name as assigned. If you type only a few characters, all computers and ports will be displayed that contain the typed characters.

Select **04 USER SECURITY** – for Supervisor only – to assign the Supervisor password and users and their passwords. For both up to 8 characters can be used.

Select **05 ACCESS LIST** – for Supervisor only – to assign access restrictions to users for certain ports. Default setting is no access restriction. To disable a user from access to a certain port go to the appropriate user and port and select the option with the ENTER key. The sign in the matrix list will change from 0 to X to indicate the access restriction.

Select **06 HOTKEY** – for Supervisor only – to change the hotkey to any of the following: Scroll Lock / Caps Lock / Left Ctrl / Right Ctrl / Left Alt / Right Alt / Left Win / Right Win. This hotkey will be permanently changed.

Select **07 TIME SETTINGS** – for Supervisor only – to set the Autoscan time interval from 5 seconds up to 99 seconds.

Select **08** OSD MOUSE – for Supervisor only – to set the speed of the mouse movement in OSD menu. There are 3 choices: slow, medium and fast. Use the appropriate setting for your mouse.

  You can close almost any OSD window by simply pressing the ESCAPE key.

  User and supervisor can only log out via OSD menu when pressing F2 key.

Section 4

Cat.5 Extender Access & Operation

4.1. Cat.5 KVM Extender Features

The modular KVM switch U8/16 offers the option to use it with or without a remote console access module. This module may either be a Cat.5 Extender or IP Access solution.
The Cat.5 Extender solution provides real time KVM access via a dedicated Cat5e/6 cable with a maximum length of 300m. When using higher resolutions we suggest the following maximum pixel resolution versus length: 1600x1200@75m/ 1280x1024@150m/1024x768@250m

Overall picture quality when using the Cat.5 extender will depend on the Cat.5/5e/6 cable quality and also on the signal quality generated by the graphics card used. To optimize the picture quality high quality amplifiers, equalizers and an auto skew compensation circuits are used in the Cat.5 Receiver unit to compensate for the attenuation and for the different lengths of the individual twisted pairs inside long Cat.5/5e/6 cables.

In comparison to the IP Access Extender solution the Cat.5 Extender provides a real time analog KVM signal. And the Cat.5 KVM Extender does not require any software for operation as it just operates as an analog KVM signal extender.

The Cat.5 KVM Extender module consists of two units: The local Cat.5 Extender Transmitter module fitted into the KVM Switch slot and the remote Cat.5 Extender Receiver unit installed at the remote user's location.

The remote Cat.5 Extender Receiver unit includes a local KVM switch which allows the remote user to also connect a local workstation to the receiver unit and switch between the local workstation and remote KVM Switch access.

4.2. Cat.5 KVM Extender Installation

Before you install the local Cat.5 Extender Transmitter module into the KVM switch ensure all connected computers are 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.

Now install the remote Cat.5 Extender Receiver unit at the remote user's location. You will need a VGA monitor and a USB mouse and keyboard to connect to the receiver unit. Connect your local workstation to the receiver unit if required using the dedicated KVM system cable included with the Cat.5 KVM Extender. Finally connect the Cat.5/5e/6 cable and the power supply unit.

The KVM cable provided can be used to connect either PS/2 or USB equipped computers in the same way as previously described for connecting computers to the KVM switch in section 1.6.

A dedicated Cat5/5e/6 cable with RJ-45 connectors is required to connect the Receiver unit and the Extender module located in the KVM switch. This connection must not be made via a "Live" Ethernet connection but only via multiple cable segments using patch cables, patch panels and wall sockets. Please consider the maximum resolution versus length limitations as mentioned previously. Please also try to limit the number of connections between the transmitter and receiver unit as this will help to reduce any signal loss introduced.

You may now proceed to power up all connected equipment and check for correct operation.

4.3. Cat.5 KVM Extender Operation

The Cat.5 Extender Receiver unit incorporates its own OSD menu which allows switching between the local workstation and remote KVM Switch as well as configuration of the unit.

To invoke the hotkey and OSD operation of the Cat.5 Receiver unit simply press the hotkey (factory default setting is Caps Lock) twice and press any other command from the list below within 2 seconds:

Command	Action
F1	Selects the OSD Help Menu of the receiver unit
F2	Selects the OSD Hotkey setting menu of the receiver unit
C	Toggle between local workstation and remote KVM switch access
Q	Turn ON / OFF the beep confirmation sound of the receiver unit
S	Turn ON Autoscan functions of the receiver unit. Display will switch at 5 second intervals between the local workstation and the KVM switch Press any key to stop scanning
A	Auto adjusts the amplifiers and equalizers of the remote Cat.5 Extender receiver unit. This auto adjustment is also performed automatically each time the receiver unit is powered on

To change the default hotkey simply activate the local OSD F2 menu. Choose a new hotkey by typing in the appropriate number key as listed in the local OSD F2 menu.

The following hotkeys are available: Scroll Lock / Caps Lock / Left Ctrl / Right Ctrl / Left Alt / Right Alt / Left Win / Right Win. When choosing a new hotkey try to avoid using a hotkey already used by any connected KVM switches as conflicts may arise when switching ports.

Section 5

IP Access Configuration & Operation

5.0.1. KVM over IP Access Features

The IP access module provides remote KVM over IP access to the KVM switch U8/16. It converts all keyboard video and mouse signals and sends them as TCP/IP signals over your LAN/WAN connection. The KVM switch U8/16 may be accessed from any computer connected to your network and provides full KVM access including BIOS level access to all the connected computers.

Please note that KVM over IP does not operate in a "real time" environment and that some degree of time delay will occur due to limiting factors such as available bandwidth and network traffic.

The KVM over IP Access module can be accessed via a simple web browser and via dedicated software tools included with the product. It uses secure encrypted sessions and password authentication protocols.

Please note that the conversion of video, mouse and keyboard signals requires a certain amount of CPU processing time. Transporting large amounts of data over TCP/IP requires a high bandwidth connection. Limited bandwidth may restrict or limit the possible screen resolutions and colour depths which can be transmitted over your LAN / WAN.

A connection which exhibits limited bandwidth will result in slower mouse reaction and cursor control. Also the available screen resolution, colour depth and refresh rates will also be affected. Ensure the connection you are using provides adequate bandwidth, some adjustment of screen resolution, colour depth and mouse cursor control may have to be made for satisfactory operation.

5.0.2 KVM over IP Access Module Installation

Before you install the IP Access module into the KVM switch ensure all connected computers are 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 now proceed to power up all connected equipment and check for correct operation.

For the remainder of this manual the U8/16 KVM switch with installed KVM over IP Module will be referred to as U8/16-IP.

5.1. Configuration

The U8/16-IP's communication interfaces are all based on TCP/IP. The switch comes pre-configured with the following IP configuration shown here:

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

Note: If the DHCP connection fails on boot-up, the U8/16-IP will not be assigned an IP address.

If this initial configuration does not meet your requirements, the following section describes the configuration that is necessary to access the U8/16-IP for the first time.

Initial Configuration via a DHCP Server

By default, the U8/16-IP will try to contact a DHCP server in the subnet to which it is physically connected. If a DHCP server is found, it will provide a valid IP address, gateway address and subnet mask. If a DHCP server is not available then you will need to assign a fixed IP assignment to the MAC address of the IP Access Module. You can find the MAC address details on the printed label on the underside of the IP Access module.

Before you connect the device to your local subnet, be sure to complete the corresponding configuration using the setup tool supplied on the CD ROM. Follow the procedure described on the next page *(Section 5.2)*

Initial Configuration via a Serial Console

The U8/16-IP 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 U8/16-IP 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 information 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 [192.168.1.22]:
Net mask [255.255.255.0]:
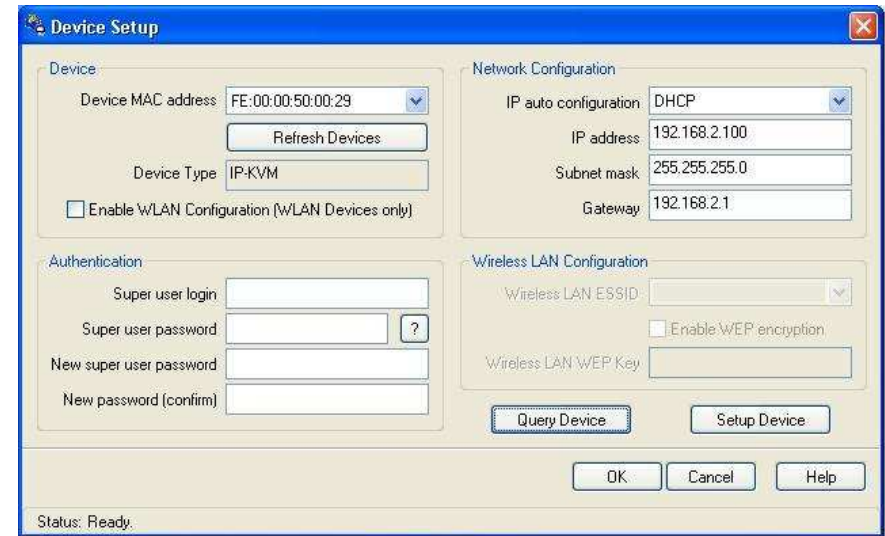**Gateway (0.0.0.0 for none) [0.0.0.0]:**

5.2 U8/16-IP Setup Tool

MAC Address Detection

Connect the U8/16-IP to your computer either via a local network, or via USB. If you use a USB connection Windows will detect the U8/16-IP as a '**Removable Disk**' and an appropriate drive letter will be assigned.

Start the setup tool from the CD ROM.

A window opens as shown below:

On the upper left corner, the MAC address of the U8/16-IP is displayed. To re-detect the MAC address, press the **Refresh Devices** button. The displayed MAC address should correspond to the printed address shown on the label on the base of the IP module.

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 Authentication, below)* and then press the **Setup Device** button.

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.

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.

IP Auto Configuration

With this option, you can specify whether the U8/16-IP 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 U8/16-IP 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**.

5.3. Keyboard, Mouse and Video Configuration

Between the U8/16-IP 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. Please see page 34 for details of how to make the specific changes to the mouse settings described below.

U8/16-IP Keyboard Settings

The U8/16-IP 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 U8/16-IP front-end, please see page 37 for details of how to make changes to the keyboard settings.

Remote Mouse Settings

A common problem with KVM devices is the synchronization between the local and remote mouse cursors. The U8/16-IP addresses this problem with an intelligent synchronization algorithm. There are two mouse modes available on the U8/16-IP: **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.

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** 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.

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 U8/16-IP 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.

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.

Video Modes

The U8/16-IP 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 U8/16-IP switch may not be able to detect them. We recommend using any of the standard VESA video modes instead.

5.4. Usage

Prerequisites

The U8/16-IP 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 U8/16-IP's serial port via a terminal.

HTTP/HTTPS
Full access is provided by the embedded web server. The U8/16-IP switch environment can be entirely managed using a standard web browser. You can access the U8/16-IP using the insecure HTTP protocol, or using the encrypted HTTPS protocol. Whenever possible, use HTTPS.

The primary interface of the U8/16-IP 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 version 1.1 or higher support. 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**

For a non-secure connection to the U8/16-IP, we recommend the following browsers:

- Microsoft Internet Explorer version 6.0 or higher

- Netscape Navigator 7.0 or Mozilla 1.6

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

5.5. Logging In

Login to the U8/16-IP

Launch your web browser. Direct it to the address of your U8/16-IP 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 U8/16-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 U8/16-IP>

When using a secure connection, type in:

https://<IP address of U8/16-IP>

This will lead you to the U8/16-IP login page as shown below:

The U8/16-IP has a built-in super user account that has all the permissions enabled to administrate your U8/16-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 U8/16-IP 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.

5.6. Navigation

Once logged into the U8/16-IP 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 U8/16-IP. Within the main area, task-specific information is displayed.
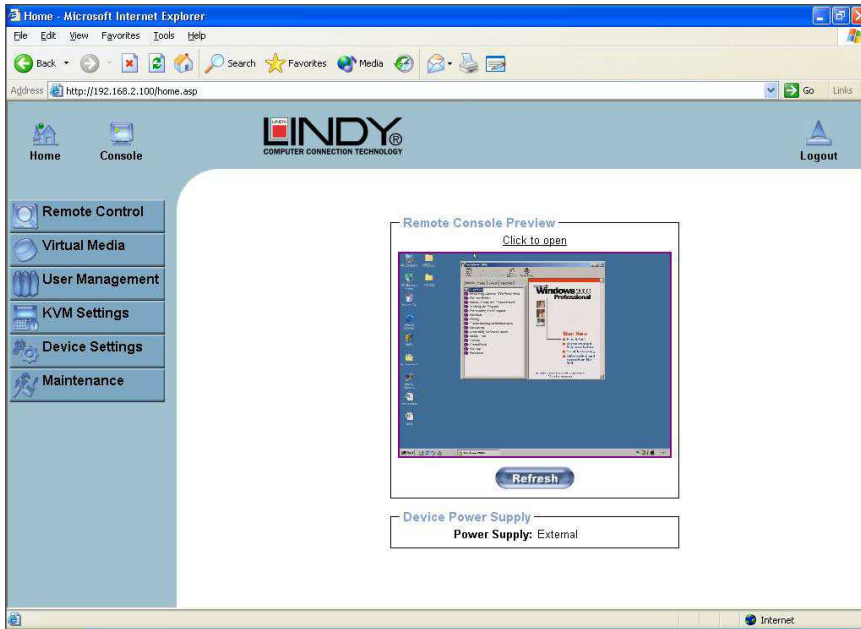
Return to the main page of the U8/16-IP

Logout from the U8/16-IP

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 U8/16-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 U8/16-IP. 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 U8/16-IP 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.

Remote Console Main Window
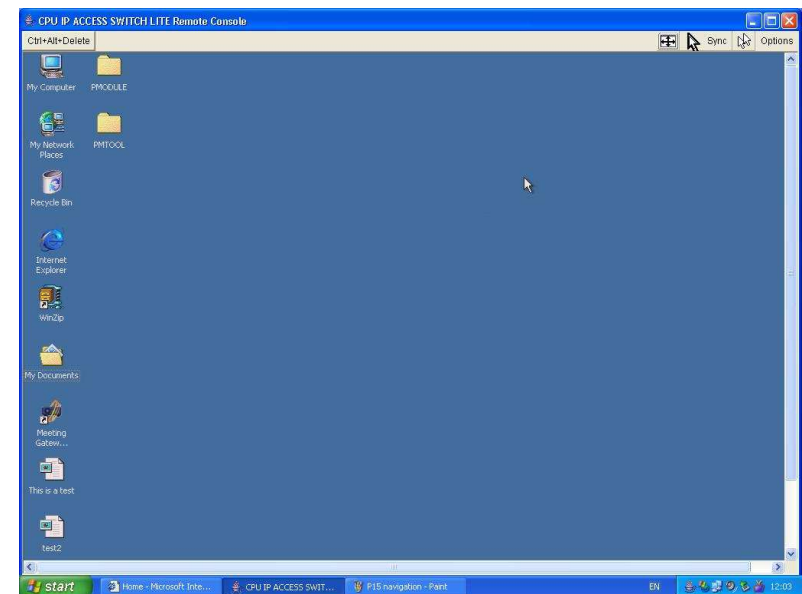
Starting the Remote Console opens an additional window. It displays the screen content of the currently selected computer connected to the U8/16-IP. The Remote Console will behave in exactly the same way as if you were using the local console. You can use the U8/16-IP keyboard hotkeys to switch between computers, activate the OSD etc., as well as control the currently selected computer. However, be aware that the host system will react to keyboard and mouse actions with a slight delay.

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. You can circumvent such problems by adjusting the keyboard of your remote system to the same mapping as your local one.

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

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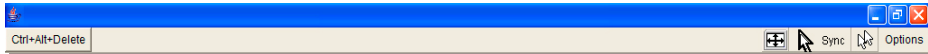
Ctrl+Alt+Delete
Sends the 'Control Alt Delete' key combination to the remote system

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 U8/16-IP 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
Opens the Options menu. A short description of the 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. 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 two options for synchronizing the local and the remote mouse pointer.

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. 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 U8/16-IP video settings. The U8/16-IP 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 U8/16-IP 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:
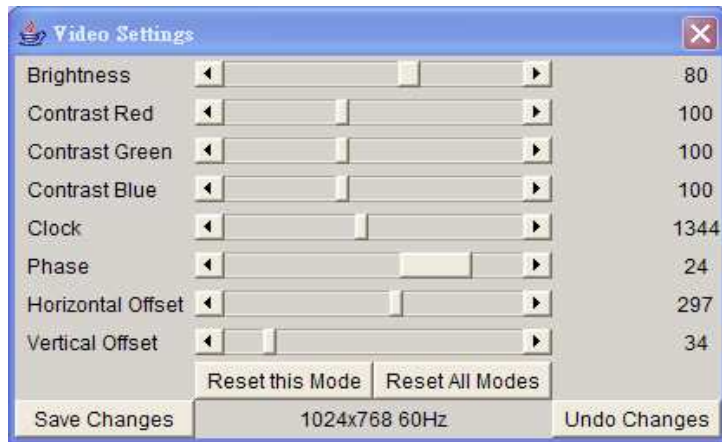
Brightness
Controls the brightness of the picture

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.
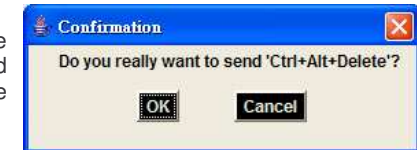
Remote Console Status Line

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.

Console(Norm): Desktop size is 1024 x 768	In: 0 B/s Out: 0 B/s

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

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

For more information about **Monitor Only** and **Exclusive Access** settings, see the relevant sections **on page 35.**

5.7. Menu Options

5.7.1. Remote Control

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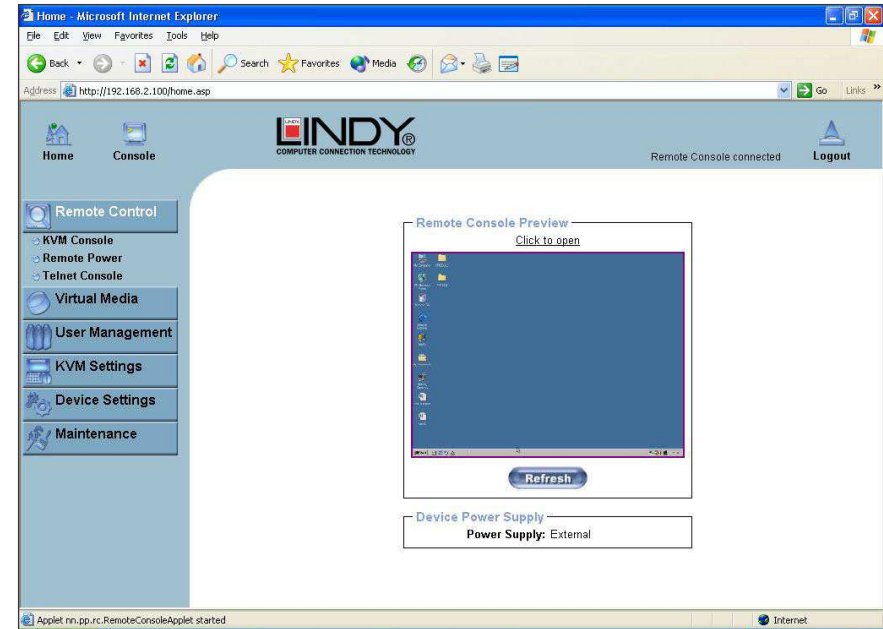
To open the KVM console, click either the menu entry on the left or on the console picture on the right. To refresh the picture, click on the **Refresh** button.

Remote Power

Future firmware updates will allow the P16-IP to control external RS-232 controlled power control distribution units. Please contact LINDY for further information regarding compatibility, connection and configuration of both LINDY and third party power control distribution units.

Telnet Console
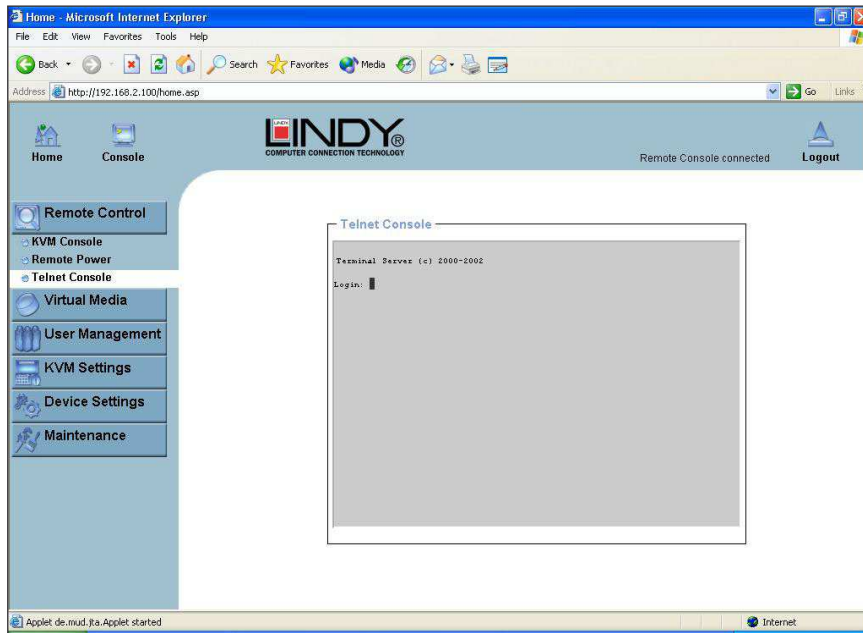
The U8/16-IP firmware features a Telnet server that enables a user to connect via a standard Telnet client. If the Telnet program is using a VT 100, VT 102 or VT 220 terminal or appropriate emulation, it is even possible to perform a console redirection, as long as the U8/16-IP host is using a text mode screen resolution.

Connecting to the U8/16-IP is done as usual and as required by the Telnet client, for instance in a UNIX shell:

       telnet 192.168.1.22

Replace the IP address by the one that is actually assigned to the U8/16-IP. 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 U8/16-IP 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 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.

5.7.2. Virtual Media

One of the computers connected to the U8/16-IP can also be set up for remote mass storage via a USB connection. Files can be uploaded to the switch, which the host computer 'sees' as virtual drives. This means the remote operator can remotely install software, drivers etc. without the need to be sat in front of the host computer.

Floppy Disk
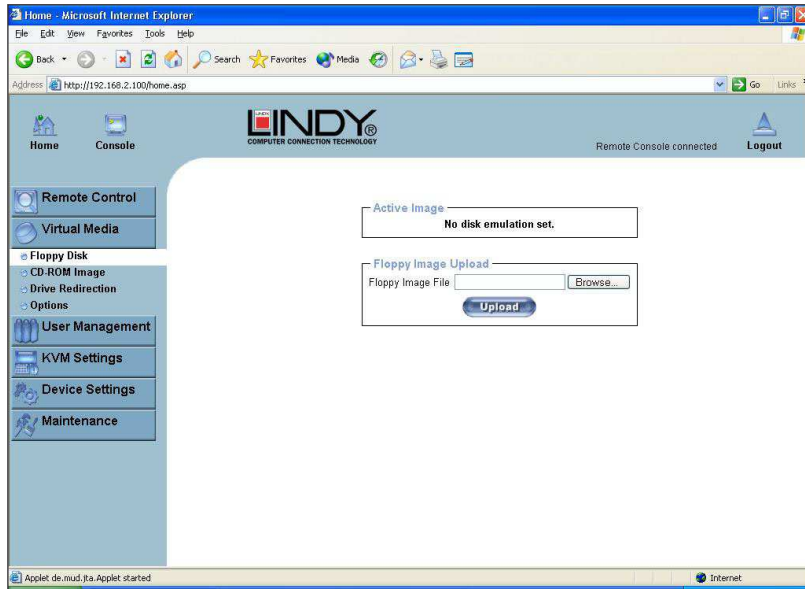
Follow the steps below to upload a virtual floppy image to the U8/16-IP and create a virtual floppy drive on the host system.

Create a Floppy Image

First, on your client PC you must create an image of your floppy disk which can be uploaded to the U8/16-IP'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:
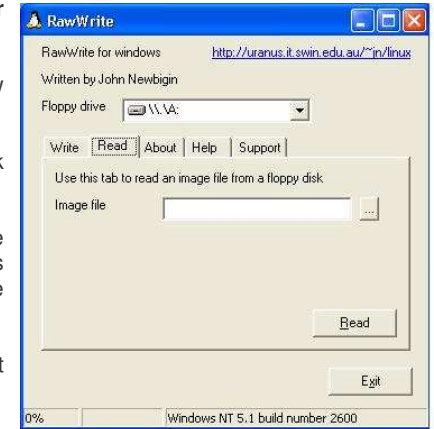
Insert your floppy disk into your floppy drive. Click the **Read** tab and then click on

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.

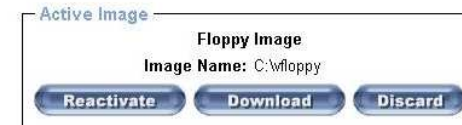When the image has been written you can upload it to the U8/16-IP.

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:

A virtual floppy drive will be installed on the host system and the image will be downloaded to the virtual floppy drive from the U8/16-IP. You can access the virtual floppy drive in the same way you would a regular drive.

You can download the image from the U8/16-IP to your remote system by clicking the **Download** button.

Clicking **Discard** removes the virtual floppy image from the U8/16-IP and from the hosts system.

Create a CD-ROM/ISO Image
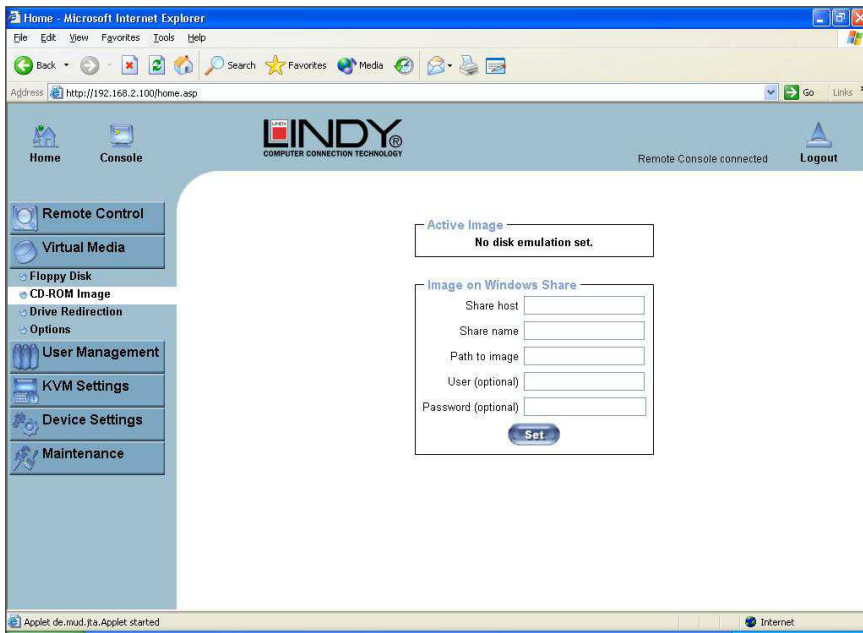
Follow the procedure below to create a CD-ROM image which can be accessed by the host system via the U8/16-IP. The image file must be an ISO file format!

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

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

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

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

For example, with 'Nero' 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 U8/16-IP 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**
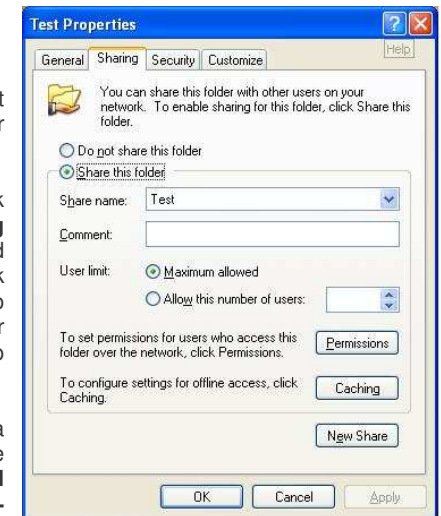
7. You will see the dialog below detailing the active image:

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.

Drive Redirection
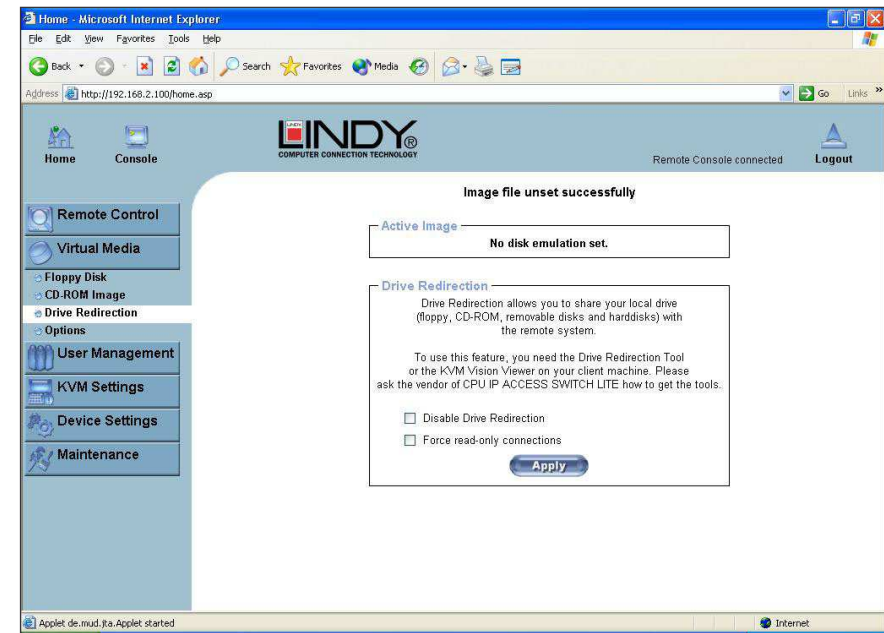
The Drive Redirection feature allows the host system to access the CD-Rom drives, hard drives, floppy drives etc. on your client PC.

To use this feature you need the Drive Redirection Tool which is part of the **KVM Vision Viewer** application included on the supplied CD.

1. To set up Drive Redirection, first install **KVM Vision Viewer**. After installation launch the application:
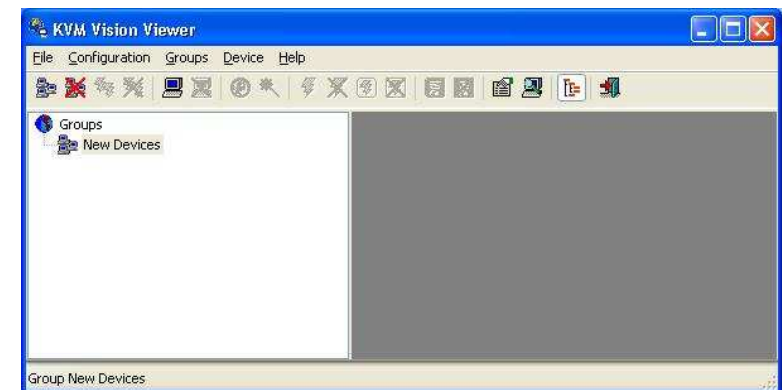
2. Click on the **Search for new devices** icon -   The U8/16-IP will be detected as an **Unconfigured device** and its MAC address will be displayed in the left panel. Double click on the MAC address to launch the **Device Configuration Wizard**.

3. Follow the on-screen instructions. You will be asked to input your user name (default is **super**) and password (default is **pass)**.

4. Continue with the Wizard until the device is correctly configured. Once the configuration is complete, select **Redirect Local Drive** from the **Device** menu:
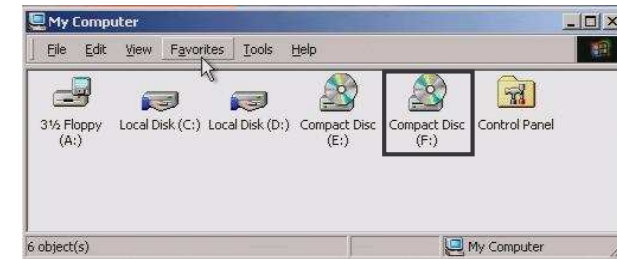
---
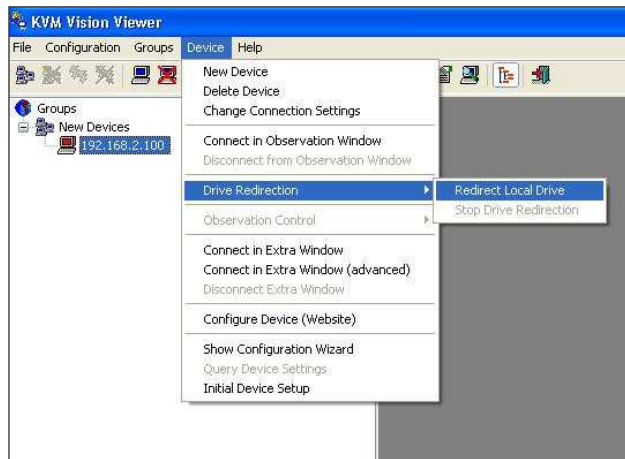
1. Choose the drive you wish to redirect from the drop-down list. Enter your user name and password and click **OK**.

> **Warning:** Please be aware that if **Allow Write Support** is selected, data on the shared media may be lost!

2. Access the host computer from the Remote Console window. You will see that the redirected drive will now be shown in Windows Explorer:

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.

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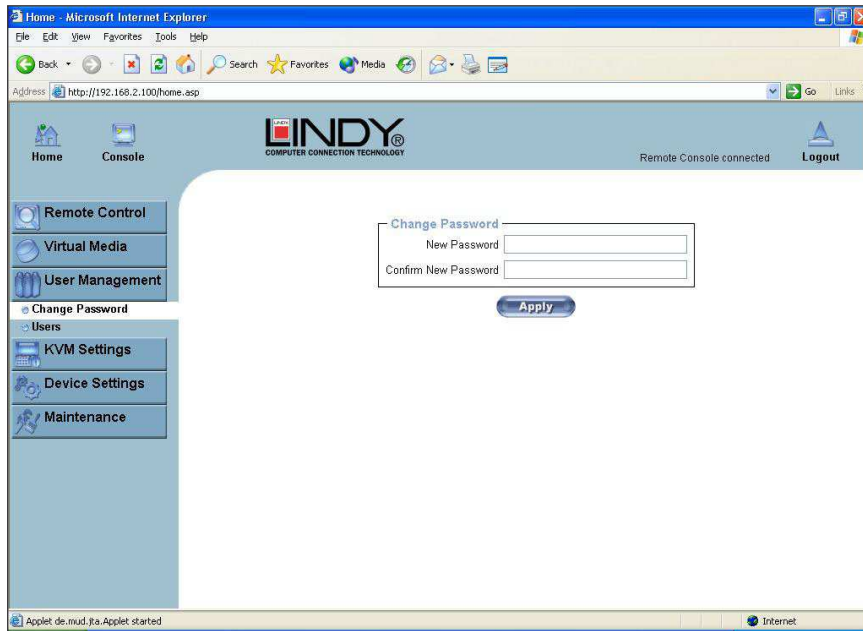
This option allows you to disable the mass storage emulation (and hide the virtual drive) if no image file is currently loaded. To set this option, press the button **Apply**.

5.7.3. User Management

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.

Users And Groups

The U8/16-IP 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 U8/16-IP 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.

5.7.4. KVM Settings

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.
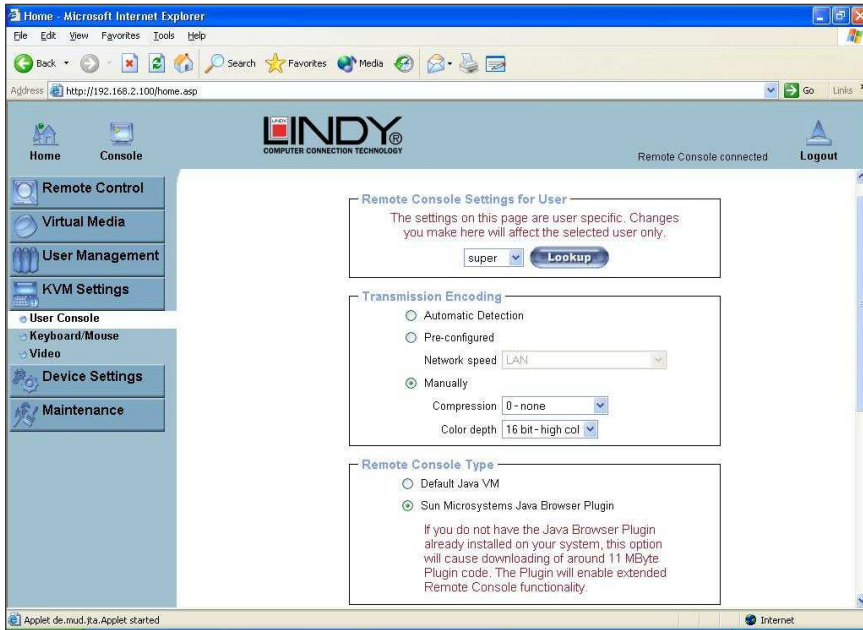
User select Unit
This box displays the user ID for which the values are shown and for which the changes will take effect. You may change the settings of other users if you have the necessary access rights.

Transmission Encoding
The Transmission Encoding setting allows changing the image-encoding algorithm that is used to transmit the video data to the Remote Console window. It is possible to optimize the speed of the remote screen 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 U8/16-IP 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 U8/16-IP 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 Microsoft JVM for Internet Explorer or the Sun JVM if it is configured this way. Use of the Sun JVM may also be forced (see below).
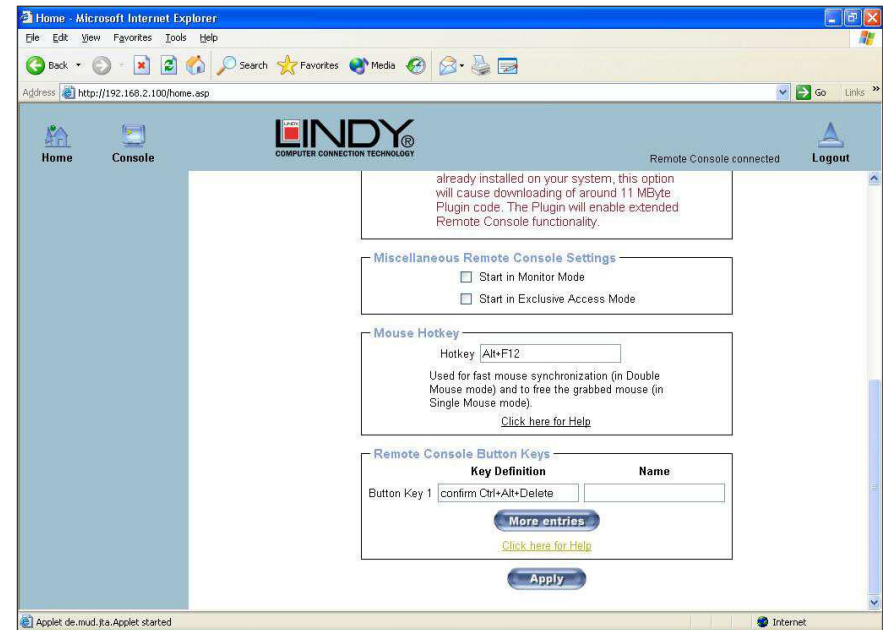
Sun Microsystems Java Browser Plug-in
Instructs the web browser of your administration system to use Sun's JVM. The JVM in the browser is used to run the code for the Remote Console window which is actually a Java Applet. If you check this box for the first time on your administration system and the appropriate Java plug-in is not already installed on your system, it will be downloaded and installed automatically. However, in order to make the installation possible, you still need to answer the appropriate dialogs with **yes**. The download size is around 11MB. The advantage of downloading 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.

Miscellaneous Remote Console Settings

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

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

Mouse hotkey
Allows 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.

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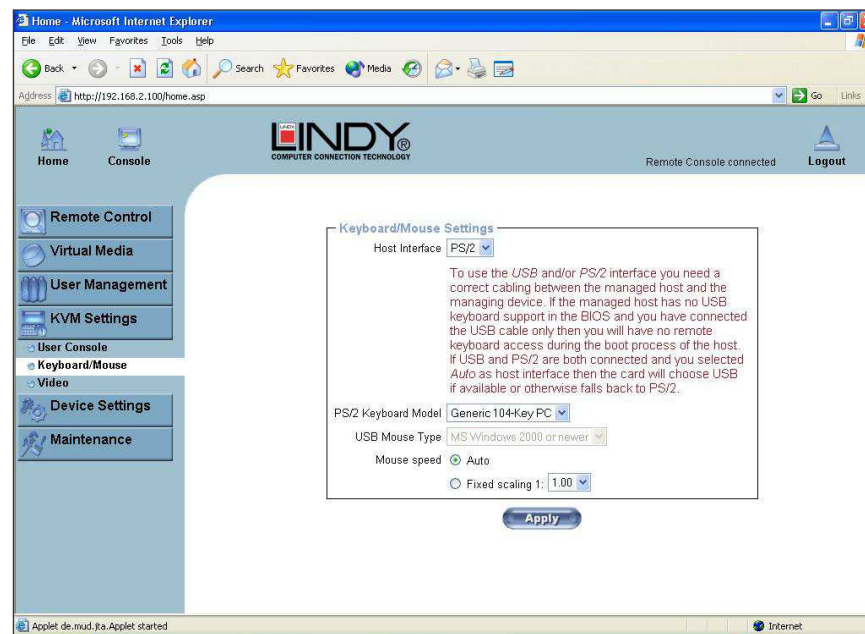
Host Interface
Enables the interface the mouse is connected to. You can choose between **Auto** for automatic detection, **USB** for a USB mouse, or **PS/2** for a PS/2 mouse.

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

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.

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.

Mouse Speed

- **Auto mouse speed** Use this option if the mouse settings on the host use an additional acceleration setting. The U8/16-IP 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.

Video
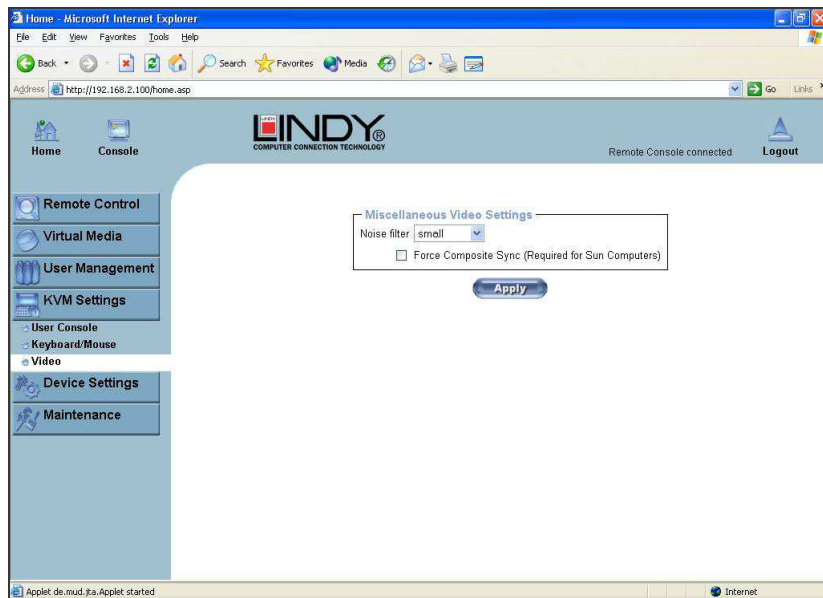
Miscellaneous Video Settings

Noise filter
This option defines how the U8/16-IP 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.

Force Composite Sync (Required for Sun Computers)
To support signal transmission from a Sun machine, enable this option. If not enabled the picture of the remote console will not be visible. To set the options, click **Apply**.

5.7.5. Device Settings

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.
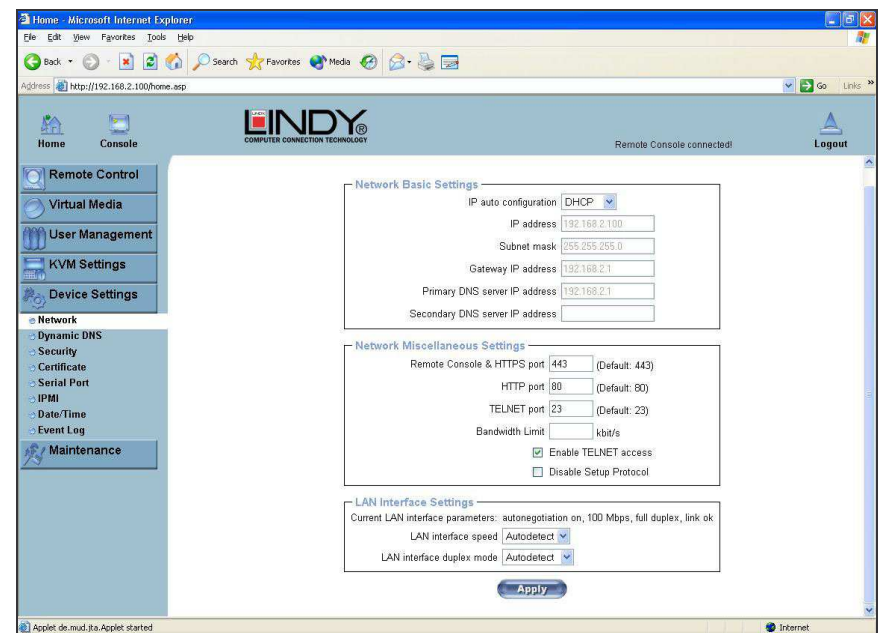
> **Note:** The initial IP configuration is usually done directly at the host system using the special procedure described on **Page 20.**
>
> Changing the network settings of the U8/16-IP might result in losing connection to it. In case you change the settings remotely make sure that all the values are correct and you still have an option to access the U8/16-IP.

IP auto configuration
With this option you can control if the U8/16-IP 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 U8/16-IP 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 U8/16-IP 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 U8/16-IP'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 U8/16-IP's HTTP server is listening. If left empty the default value will be used.

Telnet port
Port number at which the U8/16-IP's Telnet server is listening. If left empty the default value will be used.

Bandwidth limitation
The maximum network traffic generated through the U8/16-IP's Ethernet device. Value in Kbit/s.
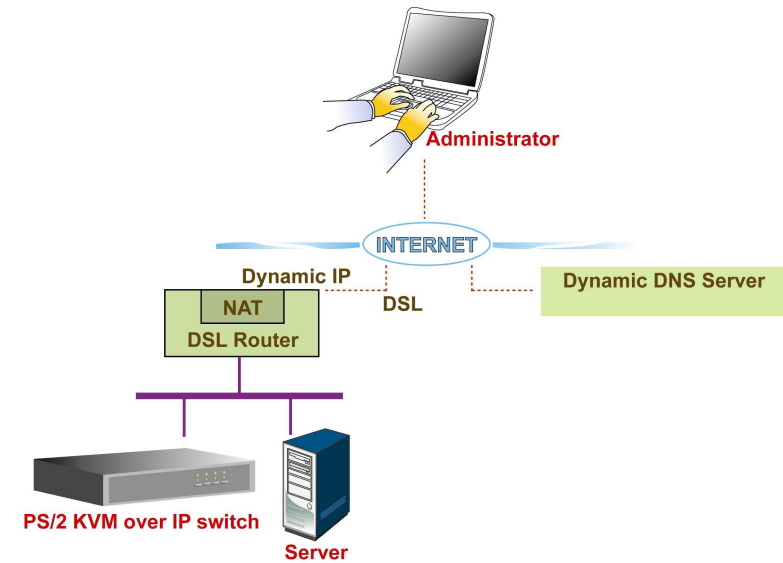
Enable Telnet access
Set this option to allow access to ARA express using the Telnet Gateway **(see the Section called Telnet Console on page 36.)**

Disable Setup Protocol
Enable this option to exclude the U8/16-IP from the setup protocol.

Dynamic DNS

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


The U8/16-IP 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 U8/16-IP 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 a U8/16-IP 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 U8/16-IP.

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

- Make sure that the LAN interface of the U8/16-IP 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).
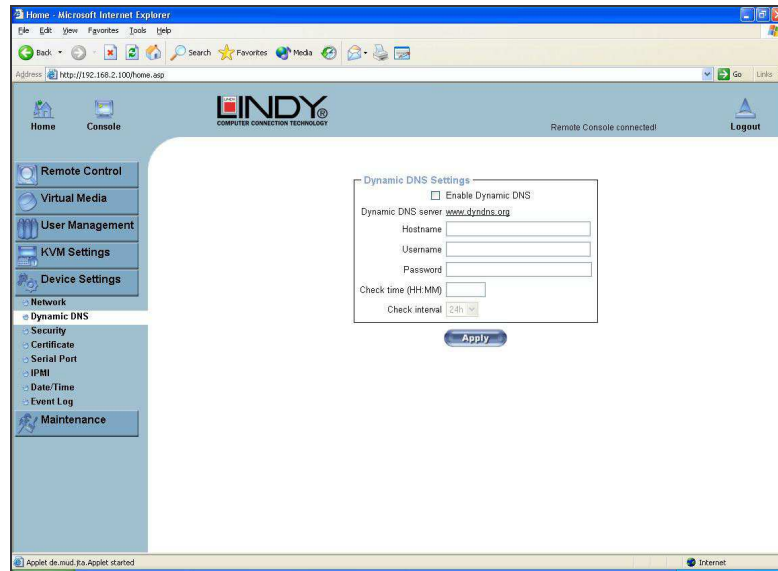
Enable Dynamic DNS
Enables the Dynamic DNS service. This requires a configured DNS server IP address.

Dynamic DNS server
This is the server name where the U8/16-IP 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 U8/16-IP 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 U8/16-IP 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 U8/16-IP.

> *Note:* The U8/16-IP has its own independent real time clock. Make sure the time setting of the U8/16-IP switch is correct. **(See the Section called Date and Time on page 63)**


Security

Force HTTPS
If this option is enabled, access to the web front-end is only possible using an HTTPS connection. The U8/16-IP 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 U8/16-IP **please refer to the section called Certificate on page 58.**

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 will attempt to establish 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.

Certificate
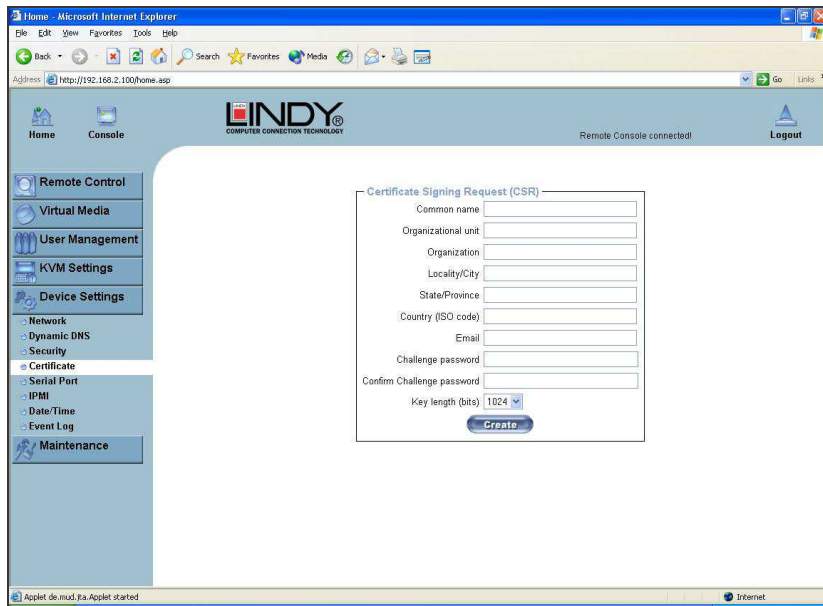
The U8/16-IP uses the Secure Socket Layer (SSL) protocol for any encrypted network traffic between itself and a connected client. During the connection establishment the U8/16-IP has to expose its identity to a client using a cryptographic certificate.

This certificate and the underlying secret key is the same for all U8/16-IP units and certainly will not match the network configuration that will be applied to the U8/16-IP 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 U8/16-IP. In order to do this, the U8/16-IP 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 U8/16-IP:

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 U8/16-IP switch using the **Upload** button.

After completing these three steps, the U8/16-IP has its own certificate that is used to identify it to its clients.

> **Note:** If you destroy the CSR on the U8/16-IP 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 U8/16-IP once it is installed in the user's network It is identical to the name that is used to access the U8/16-IP 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 U8/16-IP is accessed using HTTPS.

Organizational unit
This field is used for specifying to which department within an organization the U8/16-IP belongs.

Organization
The name of the organization to which the U8/16-IP 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 U8/16-IP 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 U8/16-IP during connection establishment.

Serial Port
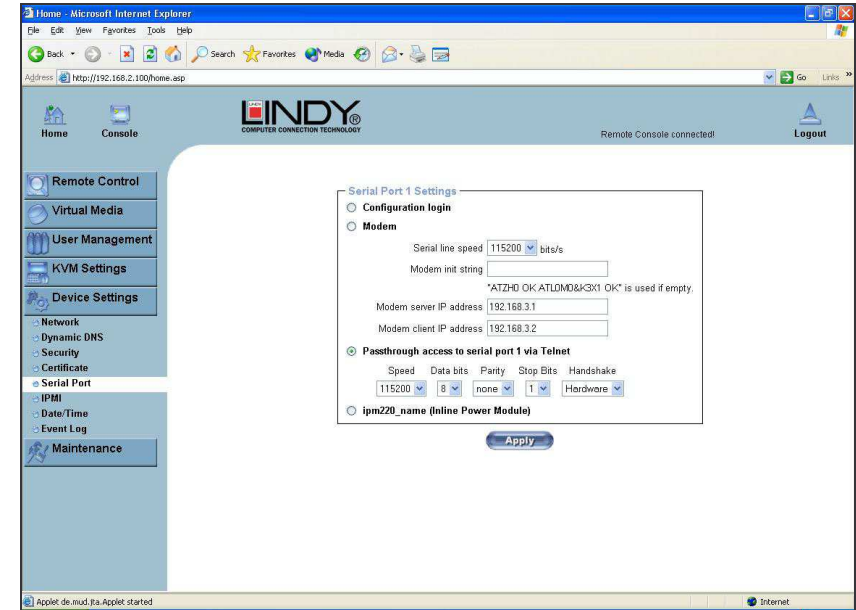
The U8/16-IP Serial Settings allow you to specify what device is connected to the serial port and how to use it.

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

Modem
The U8/16-IP 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 U8/16-IP.

Connecting to the U8/16-IP using a telephone line allows you to set up a dedicated point-to-point connection from your console computer to the U8/16-IP. In other words, the U8/16-IP 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 U8/16-IP, 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 U8/16-IP 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 U8/16-IP 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 U8/16-IP 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 U8/16-IP 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 U8/16-IP 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 U8/16-IP 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 U8/16-IP.

Date And Time
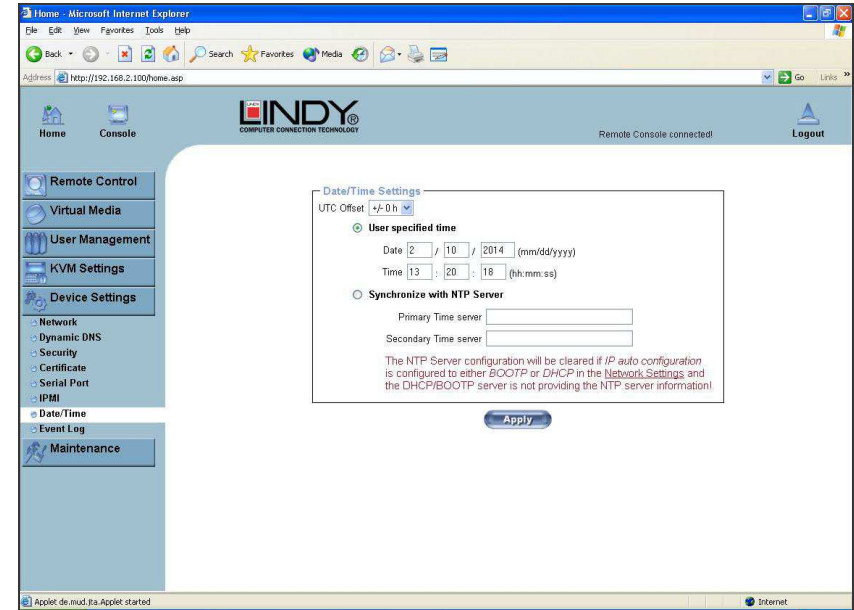
Here you can set the internal real-time clock of the U8/16-IP. You can adjust the clock manually or use an NTP timeserver. Without a timeserver your time setting will be lost if the U8/16-IP is powered down for more than a few minutes. To avoid this, you can use an NTP timeserver which sets up the internal 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 U8/16-IP 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.

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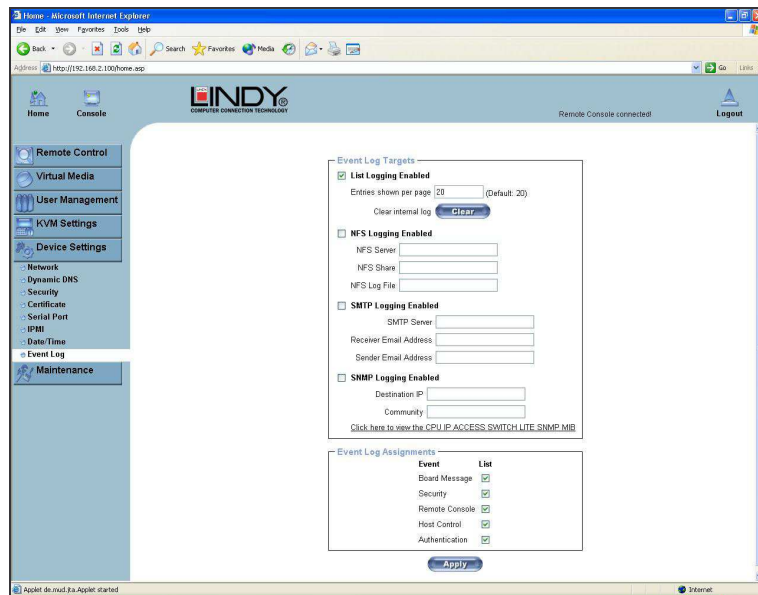
Important events like a login failure or a firmware update are logged to a selection of logging destinations. Each of those events belongs to an event group, which can be activated separately.

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 U8/16-IP. To show the log list, click on **Event Log** on the **Maintenance** page.

Since the U8/16-IP'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 U8/16-IP all logging information is saved permanently and is available after the U8/16-IP has been started. If the U8/16-IP 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 U8/16-IP 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 U8/16-IP 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 U8/16-IP and that needs no authentication at all (<serverip>:<port>).

SNMP Logging enabled
If this is activated, the U8/16-IP 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 U8/16-IP, 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.

5.7.6. Maintenance

Device Information

This section contains a summary showing various information about the U8/16-IP and its current firmware. It also allows you to reset the unit.
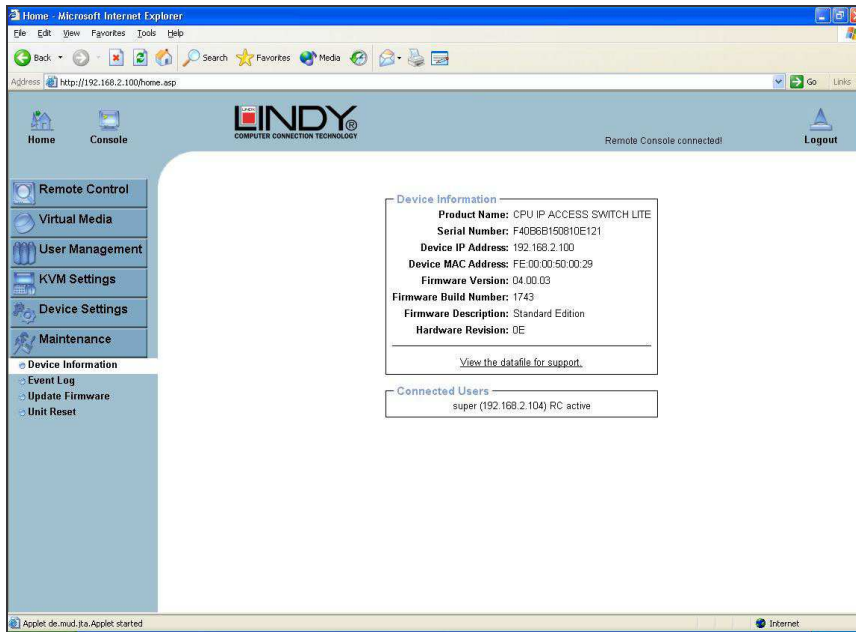
View the data file for support
Allows you to download the U8/16-IP data file with specific support information. This is an XML file with certain customized support information like the serial number etc. You can send this information if you contact LINDY technical support. It may help us solve any problems.

Connected Users
The example below displays the U8/16-IP 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 30.**
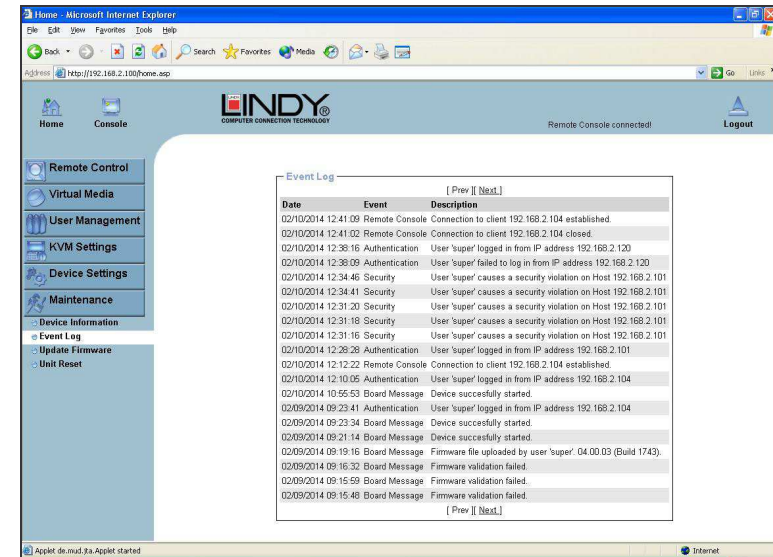
To display the user activity, the last column contains either the term **active** for an active user or **20 min idle** for a user who is inactive for a certain amount of time.
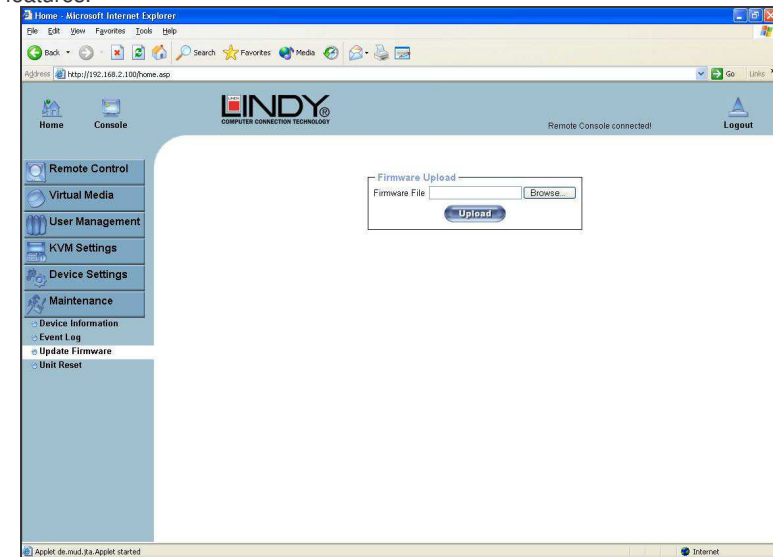
Event Log

Displays the log list including the events that are logged by the U8/16-IP.

Update Firmware

The U8/16-IP is a complete standalone computer. The software it runs is called the firmware. The firmware of the U8/16-IP 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 or which you can download from our website **www.lindy.com**.

Updating the firmware is a four stage process:

1. The new firmware file is uploaded to the U8/16-IP. 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.

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.

3. After the firmware has been stored, the U8/16-IP will automatically reset itself. Half a minute after the reset the U8/16-IP will run with the new firmware version and should be accessible. However, you will be required to login once again.

4. Once you have logged in we recommend you delete the **Temporary Internet Files** from your browser to ensure that the appearance of the web interface is correct. To do this in Internet Explorer, select:

Tools > Internet Options > General > Delete Files

Tick the check box: **Delete all offline content**, and click **OK**

Note: The firmware update process and consistency check means that making a mistake when updating the firmware is very unlikely. However, we recommend only experienced users or administrators should perform the firmware update. This process is not reversible and may take some minutes. Make sure the U8/16-IP's power supply will not be interrupted during the update process!

Tip: Should your keyboard fail to operate correctly, in the remote console, after a firmware update please use the **Reset Keyboard/Mouse** option in the **Maintenance** section as described on **page 69** .

Unit Reset

This section allows you to reset specific parts of the device. This involves the keyboard and mouse, the video engine and the U8/16-IP 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 U8/16-IP functionality, click on the Reset button.

Note: Only the super user is allowed to reset the U8/16-IP.

Troubleshooting

If none of the LED displays on the KVM Switch are illuminated, please check that the power adapter is connected and switched on at the mains.

Before you check any further please make sure that all cables are well connected!

KVM Switch Troubleshooting

If the KVM Switch reacts to keyboard input from the SCROLL LOCK key with a beep signal but you get no monitor picture displayed please check if the currently selected computer is in sleep mode or powered down. You can try to wake up this computer by pressing the ESCAPE key several times until the KVM Switch no longer beeps, and then pressing spacebar or RETURN key to wake up the computer. The U8/16-IP supports VGA power save modes and suspends the monitor signal if the currently selected computer has switched off the VGA signal.

Please check if your problems can be solved by resetting the KVM switch, via the push buttons on the front panel. For cascaded systems please follow the procedures mentioned in the CASCADING section.

1. **The Monitor picture is not sharp or shows shadows**
    - The maximum recommended VGA cable distance is 5 metres without ghosting and degradation.
    - Make sure you have used high quality video cables with coaxial cores. If the diameter of the cable is less then 6mm then the cable may not be high enough quality.

2. The maximum recommended PS/2 cable distance is 5 metres. Normally, the cable length is based on the electronic driver capacity of your motherboards PS/2 ports. If you need longer PS/2 distances it may be necessary to use a PS/2 extender.

3. Don't press any keys on the keyboard while the selected computer is booting up. Otherwise it may cause a keyboard error, or the keyboard may not be detected at the PC side.

4. **The computer boots up fine, but the keyboard doesn't work**
    Make sure the keyboard works when directly plugged into the computer. Try a different keyboard, but use standard PS/2 keyboards (some keyboards with extra multimedia keys may not be supported).

5. **The Mouse is not detected during PC boot up**
    - Make sure the mouse works when directly plugged into the computer. You have to install the appropriate mouse driver on all connected computers!
    - Make sure the mouse is a true PS/2 mouse. A combo mouse will work just as long as it is set for PS/2 mode with the correct adapter. Try a different mouse.
    - Some advanced mice like radio frequency mice, 5 button mice and scroll wheel mice use very uncommon proprietary signals. Although LINDY has carefully checked for the highest compatibility, we cannot guarantee that the U8/16-IP will work with all known mice, especially those developed and produced after the U8/16-IP's introduction.
    - Avoid moving the mouse or pressing the mouse buttons when switching ports.
    - Avoid switching ports during the PC shut down process.

6. If you have forgotten the OSD "**password**" please contact LINDY.

IP Access Troubleshooting

1. **The remote mouse doesn't work or is not synchronized**
    Make sure the mouse settings in U8/16-IP match the mouse model. Use the **Intelligent Sync** option from the **Mouse Handling** sub menu of the Remote Console **Options** menu.

2. **The remote mouse does not work correctly**
    Try using the **Reset Keyboard/Mouse** option in the **Maintenance** section as described on **page 69**.

3. **The video quality is bad or the picture is grainy**
    Try to correct the brightness and contrast settings **(see Page 33)** until they are out of a range where the picture looks grainy. Use the auto adjustment feature to correct a flickering video.

4. **Login on U8/16-IP switch fails.**
    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.

5. **The Remote Console window can't connect to the U8/16-IP.**
    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,

6. **No connection can be established to the U8/16-IP.**
    Check whether the network connection is working in general (ping the IP address of U8/16-IP). If not, check the network hardware. Is the U8/16-IP powered on? Check whether the IP address of U8/16-IP switch and all other IP related settings are correct! Also verify that all the IP infrastructure of your LAN, including routers etc., is correctly configured.

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

8. **In the browser the U8/16-IP switch pages are inconsistent.**
    Clear **Temporary Internet Files** from your browser. To do this in Internet Explorer, select:

    Tools > Internet Options > General > Delete Files

    Tick the check box: **Delete all offline content**, and click **OK**

9. **Windows XP doesn't awake from standby mode**
    This could be a Windows XP problem. Try not to move the mouse while XP goes into standby mode.

10. **Every time I open a dialog box with some buttons, the mouse pointers are not synchronous anymore**
    Please check if you have an option like '**Automatically move mouse pointer to the default button of dialog Unites**' enabled in the mouse settings of the operating system. This option needs to be disabled.

Key Codes

This table shows the key codes used to defines 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.

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

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).

Video Modes

The table below lists the video modes that the U8/16-IP remote console supports. Please do not use any other custom video settings; the U8/16-IP 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

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

United Kingdom
In 2006 the European Union introduced regulations (WEEE) for the collection and recycling of all waste electrical and electronic equipment. It is no longer allowed to simply throw away electrical and electronic equipment. Instead, these products must enter the recycling process.

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.

More details can be obtained from your national WEEE recycling agency.

Germany / Deutschland
Die Europäische Union hat mit der WEEE Direktive umfassende Regelungen für die Verschrottung und das Recycling von Elektro- und Elektronikprodukten geschaffen. Diese wurden von der Bundesregierung im Elektro- und Elektronikgerätegesetz – ElektroG in deutsches Recht umgesetzt.
Dieses Gesetz verbietet vom 24.März 2006 an das Entsorgen von entsprechenden, auch alten, Elektro- und Elektronikgeräten über die Hausmülltonne! B2C-Geräte müssen den lokalen Sammelsystemen bzw. örtlichen Sammelstellen zugeführt werden! Dort werden sie kostenlos entgegen genommen. Die Kosten für den weiteren Recyclingprozess übernimmt die Gesamtheit der Gerätehersteller. B2B Geräte wie dies KVM Switches nimmt LINDY kostenlos zurück und führt sie einem geordneten Recycling zu. Bitte nehmen Sie hierzu Kontakt mit LINDY auf, die Adressen finden Sie auf der LINDY Website www.lindy.com

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 WEEE 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.

CE Statement

This device complies with the European Regulations for Electromagnetic Compatibility (EMC) of the European Union and it is equipped with the CE mark. This unit has to be used with high quality shielded connection cables. Only if these high quality shielded cables are used can it be sure that the EMC compatibility is not adversely influenced.

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.

FCC Warning
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.

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

Free Manuals Download Website

http://myh66.com

http://usermanuals.us

http://www.somanuals.com

http://www.4manuals.cc

http://www.manual-lib.com

http://www.404manual.com

http://www.luxmanual.com

http://aubethermostatmanual.com

Golf course search by state

http://golfingnear.com

Email search by domain

http://emailbydomain.com

Auto manuals search

http://auto.somanuals.com

TV manuals search

http://tv.somanuals.com