CPI KVM IP Console
User Manual

Version 1.0
November 2011

CHATSWORTH
PRODUCTS, INC.

800-834-4969
techsupport@chatsworth.com
www.chatsworth.com

Table of Contents

Chatsworth Products, Inc.
9353 Winnetka Avenue
Chatsworth, CA 91311
800-834-4969

KVM IP Console User Manual

Legal Information

The information contained in this guide is subject to change without notice.
Chatsworth Products, Inc. shall not be liable for technical or editorial errors or omissions contained herein; nor is it liable for any injury, loss, or incidental or consequential damages resulting from the furnishing, performance, or use of this material and equipment.

Warranty

Chatsworth Products, Inc. (CPI) guarantees manufactured products and each part or component thereof against all defects in material and/or workmanship. Chatsworth Products, Inc. agrees to remedy any manufacturing defect either through replacement or repair at no charge provided that the defective unit is returned, transportation prepaid, to the Chatsworth Products, Inc. factory.

The warranty extends for a period of one year from the date of installation or initial use, provided that this period shall not exceed 18 months from the original date of shipment from the factory.

Any product that has been repaired or replaced shall be similarly warranted on its repair or replacement for the remaining product warranty period or 90 days from the date of repair or replacement, whichever expires last.

This warranty does not extend to products that have been subjected to neglect, accident or improper use, nor to units that have been altered by non-Chatsworth Products, Inc. personnel.

No warranties other than those set forth in this section are given or implied with respect to the products furnished. Chatsworth Products, Inc. shall, in no event, be liable for consequential damages, for loss, damage or expense directly or indirectly arising from the use of the products, for any inability to use materials or from any other cause.

Introduction

This document is the User's Manual for the IP console on IP KVM Switches from Chatsworth Products, Inc. (CPI). It provides detailed setup instructions for the KVM IP console on the following IP KVM Switches.

CPI Part Number				IP KVM Switch Description
LCD KVM Drawer and Switch Combination			Standalone IP KVM Switch	
Single Rail	US	37209-261	37212-260	16 port DB15 Switch, 1 IP, no remote
		37205-361	37207-360	16 port Cat5/6 Switch, 1 IP, 1 remote
		37205-421	37207-420	32 port Cat5/6 Switch, 2 IP, 1 remote
	UK	37209-262	37212-260	16 port DB15 Switch, 1 IP, no remote
		37205-362	37207-360	16 port Cat5/6 Switch, 1 IP, 1 remote
		37205-422	37207-420	32 port Cat5/6 Switch, 2 IP, 1 remote
Dual Rail	US	37206-361	37207-360	16 port Cat5/6 Switch, 1 IP, 1 remote
		37206-421	37207-420	32 port Cat5/6 Switch, 2 IP, 1 remote
	UK	37206-362	37207-360	16 port Cat5/6 Switch, 1 IP, 1 remote
		37206-422	37207-420	32 port Cat5/6 Switch, 2 IP, 1 remote

Product Features

Each KVM IP console on IP KVM Switches provides:

- Remote access to the 16 or 32 device ports on the KVM Switch and to device ports on expansion switches attached to the primary switch with Cascade Cables. Access up to 128 or 256 computers through a single IP connection.
- Remote management capability for one user over a 10/100 TCP/IP network and secure encrypted access via HTTPs connection. Users access equipment through a Java-compatible web browser using a password protected logon and switch between computers using an intuitive on-screen menu.
- User management that allows users to be assigned individual accounts with user preferences and user or administrator access.
- A log that automatically records access attempts and system changes.
- A separate serial connection that can be used to connect an arbitrary device that can be accessed using a standard Telnet client if the device supports terminal mode connection.
- Drive redirection that allows a local drive or USB stick to be shared with a connected computer.

Configuration

1.1 Initial IP Configuration

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

IP address 1: 192.168.1.22 (Single IP Console)

IP Address 2: 192.168.1.23 (Second IP Console)

Subnet mask: 255.255.255.0

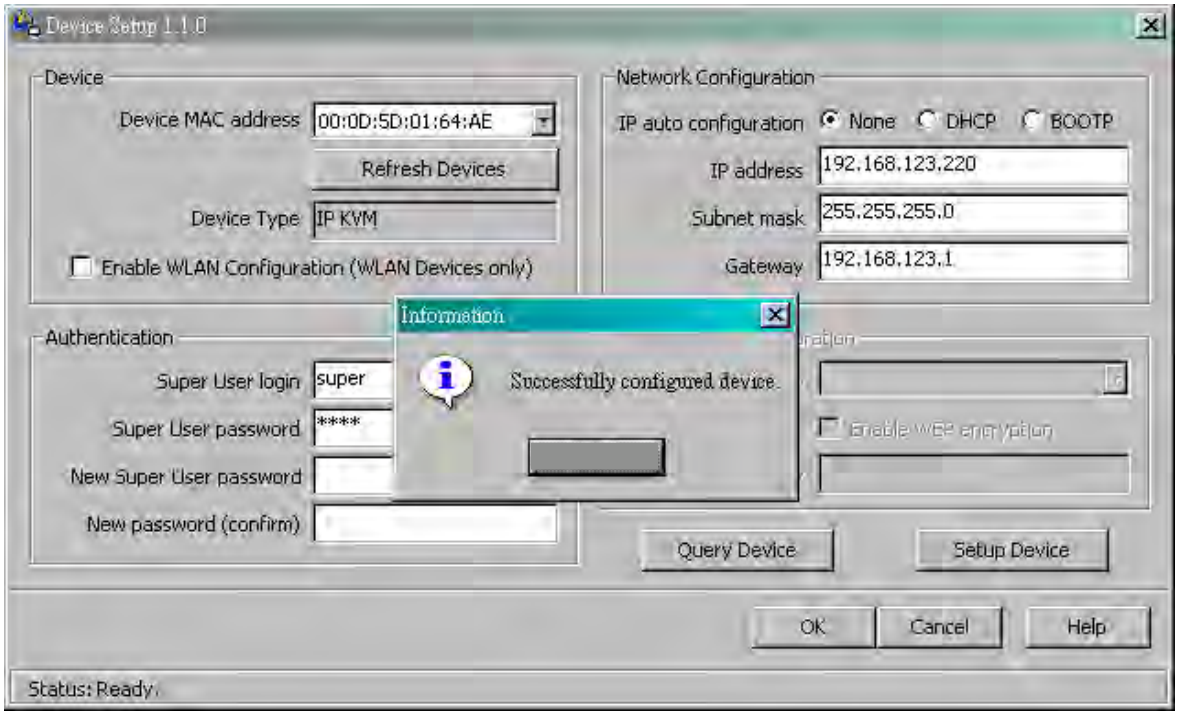
Gateway: None

1.2 Using The IP Configuration Setup Tool

If this initial configuration does not meet your local requirements, use the KVM IP Console Setup Software to change the configurations to your needs. Download: http://www.chatsworth.com/uploadedFiles/Files/37209_KVM_IP_CONSOLE_USER_MANUAL.pdf from the CPI Website: http://www.chatsworth.com/Support-and-Downloads/Downloads/Software/.

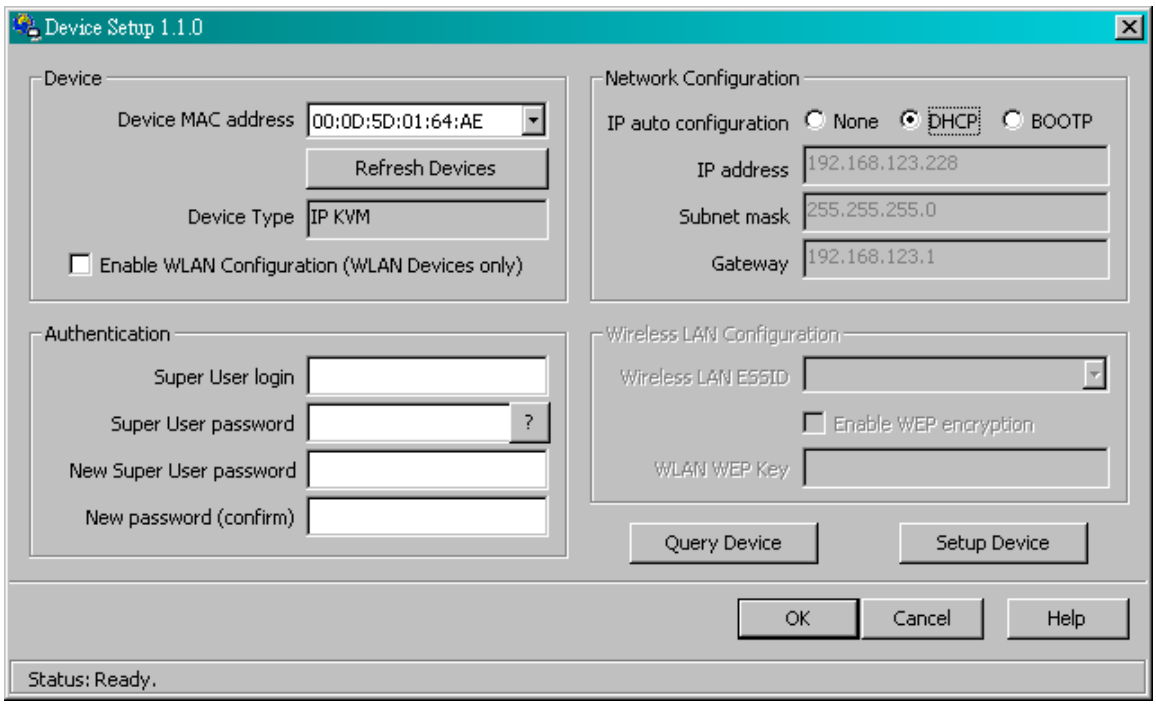
1.2.1 To Set A Fixed IP Address

1. Run KVMIPsetup.exe from the zip file. The screen below will display.
2. Under **Network Configuration**, select **None** for **IP auto configuration**
3. Set the IP address and Subnet mask
4. Enter Super user login and password for Authentication (default : super/pass)
5. Click **Setup Device**. If super login was authenticated, it will show Successfully configured device; otherwise it will show Permission Denied



1.2.2 To Use DHCP or BOOTP

1. Run KVMIPsetup.exe. The screen below will display.
2. Under **Network Configuration**, select **DHCP** or **BOOTP** for **IP auto configuration**
3. Enter Super user login and password for Authentication (default : super/pass)
4. Click **Setup Device**. If super login was authenticated, it will show Successfully configured device; otherwise it will show Permission Denied.



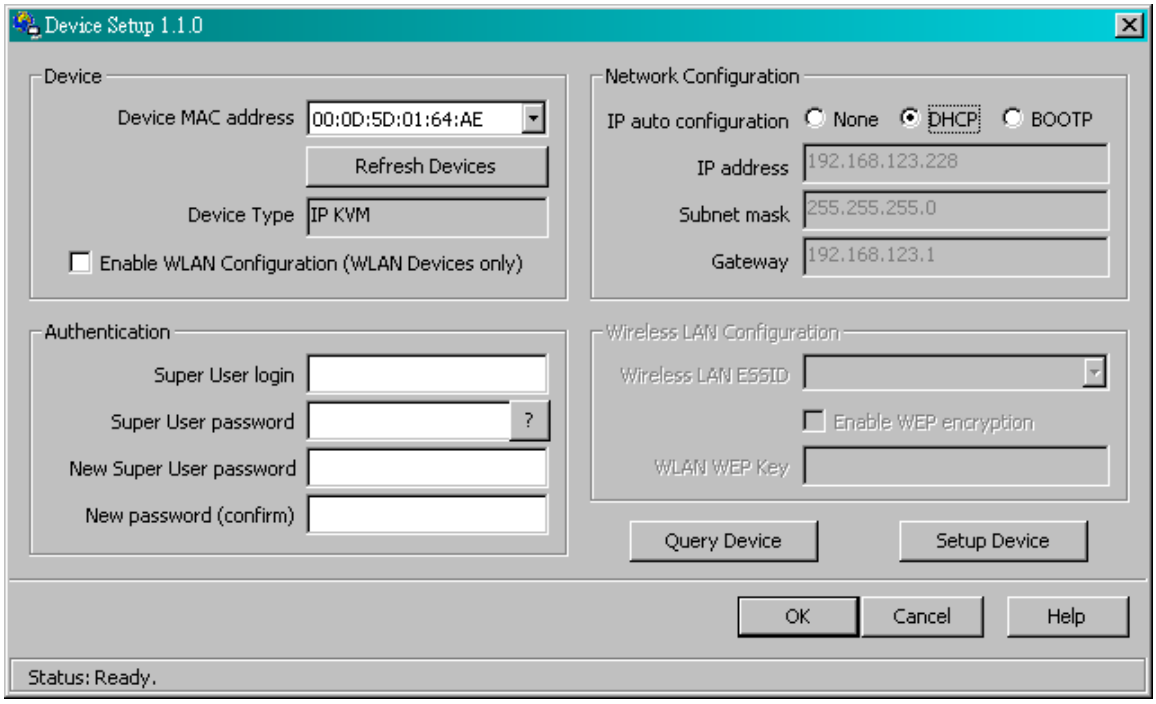
When DHCP mode is enabled (IP auto configuration = DHCP), the IP console will try to contact a DHCP server in the subnet to which it is physically connected. If a DHCP server is found, it may provide a valid IP address, gateway address and net mask. Before you connect the device to your local subnet,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

If you have installed the IP console on a network that enables DHCP, you can use the **KVMIPsetup.exe** to locate the IP console's IP address.

1. Plug the Ethernet cable into the IP KVM Switch. The IP console will get an IP address via DHCP.
2. Run **KVMIPsetup.exe**. The screen shown above will display. Under **Device**, select the MAC address which is printed on the label on the bottom of the IP KVM Switch from the **Device MAC address** list and click **Query Device**

1.2.3 To Change 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 characters are in lower case.

Super user password
Enter the current password for the super user. This initial value is “pass”. All characters are in 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 for confirmation.

To close the window and accept the changes, press the “OK” button; otherwise press the “Cancel” button.

1.3 Keyboard, Mouse and Video configuration

Between the IP console 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.

1.3.1 IP Console Keyboard Settings

The IP console settings for the host's keyboard type have to be corrected in order to make the remote keyboard work properly. Check the settings in the IP console Web front-end. See section 3.5.2 for details.

1.3.2 Remote Mouse Settings

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

- **Auto mouse speed**: the automatic mouse speed mode tries to detect the speed and acceleration settings of the host system automatically. See section 1.3.3 for a more detailed explanation.
- **Fixed mouse speed**: this mode just translates the mouse movements from the Remote Console (see Section 2.3) in a way that one pixel move will result in n-pixel moves on the remote system. This parameter n is adjustable with the scaling. Please note that this works only when mouse acceleration is turned off on the remote system.

1.3.3 Automatic mouse speed and mouse synchronization

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

- **Fast Sync:** the fast synchronization is used to correct a temporary, but fixed skew. Choose the option using the Remote Console options menu (see section 2.4.1) or press the mouse synchronization hotkey sequence in case you defined one.
- **Intelligent Sync:** If the fast sync does not work or the mouse settings have been changed on the host system, use the intelligent resynchronization. This method takes more time than the fast one and can be accessed with the appropriate item in the Remote Console option menu (see section 2.4.1). The intelligent synchronization requires a correctly adjusted picture. Use the auto adjustment function to setup the picture, and make sure that there are no windows at the top left corner of the remote desktop that are able to change the mouse cursor shape from the normal state. The Sync mouse button on top of the Remote Console can behave differently, depending on the current state of mouse synchronization. Usually pressing this button leads to a fast sync, except in situations where the KVM port or the video mode changed recently.

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

1.3.4 Host system mouse settings

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

Warning!
The following limitations do not apply in case of USB and Mouse Type "Windows >= 2000, MacOSX."

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

- **Special Mouse Driver:** There are mouse drivers that influence the synchronization process and lead to desynchronized mouse pointers. If this happens, make sure you do not use a special vendor-specific mouse driver on your host system.
- **Windows XP Mouse Settings:** Windows XP knows a setting named "improve mouse acceleration," which has to be deactivated.
- **Active Desktop:** If the Active Desktop feature of Microsoft Windows is enabled do not use a plain background. Instead, use some kind of wallpaper. As an alternative, you could also disable the Active Desktop completely.

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

1.3.5 Single and Double Mouse Mode

The information above applies to the Double Mouse Mode, where remote and local mouse pointers are visible and need to be synchronized. The IP console also features another mode, the Single Mouse Mode, where only the remote mouse pointer is visible. Activate this mode in the open Remote Console and click into the window area. The local mouse pointer will be hidden and the remote one can be controlled directly. To leave this mode, it is necessary to define a Mouse Hotkey in the Remote Console settings panel, see Section 3.5.1. Press this key to free the captured local mouse pointer.

1.3.6 Recommended Mouse Settings

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

- **MS Windows 2000/2003 (Professional and Server) and XP (all versions):** In general, we recommend the usage of a mouse via USB. Choose USB without Mouse Sync. For a PS/2 mouse choose Auto Mouse Speed. For XP disable the option "enhance pointer precision" in the Control Panel.
- **SUN Solaris:** Adjust the mouse settings either via xset m 1 or use the CDE Control Panel to set the mouse to "1:1, no acceleration." As an alternative you may also use the Single Mouse Mode.
- **MAC OS X:** We recommend using the Single Mouse Mode.

1.3.7 Video Modes

The IP console 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 IP console may not be able to detect them. We recommend using any of the standard VESA video modes, instead.

The table below lists the video modes IP console supports. Please don't use other custom video settings besides these. If you do so, IP console may not be able to detect them.

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

2.1 Prerequisites

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

The following interfaces are supported:

- **HTTP/HTTPS:** Full access is provided by the embedded web server. The IP console environment can be entirely managed using a standard web browser. You can access the IP console using the insecure HTTP protocol, or using the encrypted HTTPS protocol. Whenever possible, use HTTPS.
- **Telnet :** A standard Telnet client can be used to access an arbitrary device connected to the IP consoles multi port via a terminal mode.

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

In order to use the Remote Console (see section 2.3) window of your managed host system, the browser has to come with a Java Runtime Environment version 1.4.2 or above. If the browser has no Java support (such as on a small handheld device), you are still able to maintain your IP console using the administration forms displayed by the browser itself.

Important: We recommend installing a Sun JVM 1.5.0.4.

For an unsecure (HTTP) connection to the IP console, we can recommend the following browsers:

- **Microsoft Internet Explorer:** version 6.0 or higher on Windows 2000 and Windows XP
- **Netscape Navigator 7.0 or Mozilla 1.6:** on Windows 2000, Windows XP, Unix, Linux and UNIX-like Operating Systems

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

Using Internet Explorer, open the menu entry “?” and “Info” to read about the key length that is currently activated. The dialog box contains a link that leads you to information on how to upgrade your browser to a state of the art encryption scheme. The figure below shows the dialog box presented by the Internet Explorer 6.0. Note the Cipher Strength is 128-bit.

Newer web browsers generally support strong encryption on default.

2.2 Accessing The IP KVM Switch

2.2.1 Login Into The IP Console

Launch your web browser. Direct it to the address of your IP console, which you configured during the installation process. The address used might be an IP address or a domain name, in the case where you have given your IP console a symbolic name in the DNS.

For instance, type the following in the URL field of your browser when establishing an unsecured connection:
http://<IP address of IP console>

When using a secure connection, type in:
https://<IP address of IP console>

This will lead you to the IP console login page as shown in the figure below.

2.2.1.1 Default Password

The IP console has a built-in super user account that has all permissions to administrate your IP console. The default logon for the super user account is:

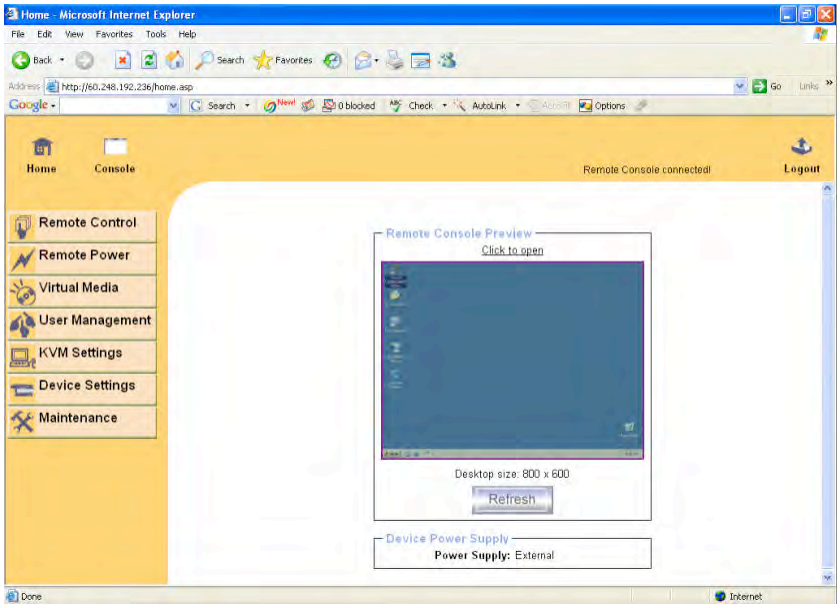
Username	super (factory default)
Password	pass (factory default)

Warning!
Please make sure to change the super user password immediately after you have installed and accessed your IP console for the first time. If you do not change the super user password, there is a severe security risk that may result in unauthorized access to the IP console and to the host system including all possible consequences!

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

2.2.1.2 Navigation

Having logged into the IP console successfully, the main page of the IP console appears, see the figure below. This page consists of three parts; each of them contains specific information. The buttons on the upper side allow you to navigate within the front end, see the table below for details. Within the right frame, task-specific information is displayed that depends on the section you have chosen before.



Return to the main page of the IP console.

Open the IP console remote console (see section 2.3).

Exit from the IP console front end.

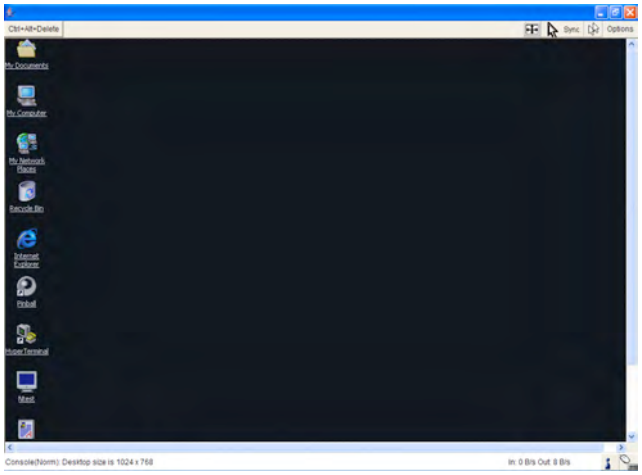
Warning!
If there is no activity for 30 minutes, the IP console will automatically log you out. A click on one of the links will bring you back to the login screen.

2.2.2 Logout From The IP Console

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

2.3 The Remote Console

The Remote Console is the redirected screen, keyboard and mouse of the remote host system that IP console controls. See the figure below.



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

In case the IP console 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 the desired connection. This is because today's web proxies are not capable of relaying the RFB protocol.

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

2.4 Main Window

Starting the Remote Console (see section 2.3) opens an additional window. It displays the screen content of your host system. The Remote Console will behave exactly in the same way as if you were sitting locally in front of the screen of your remote system. That means keyboard and mouse can be used in the usual way. However, be aware of the fact that the remote system will react to keyboard and mouse actions with a slight delay. The delay depends on the bandwidth of the link to which you use to connect to the IP console.

With respect to the keyboard, the very exact remote representation might lead to some confusion as your local keyboard changes its keyboard layout according to the remote host system. For instance, if you use a German administration system, and your host system uses a US English keyboard layout, 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.

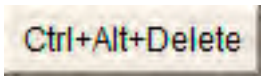
The Remote Console window (see Section 2.3) always tries to show the remote screen with its optimal size. That means it will adapt its size to the size of the remote screen initially and after the screen resolution of the remote screen has been changed. However, you can always resize the Remote Console window in your local window system as usual.

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

2.4.1 Remote Console Control Bar

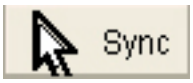
The upper part of the Remote Console window contains a control bar. Using its elements you can see the state of the Remote Console and adjust the local Remote Console settings. A description for each control follows.

Remote Console Control Bar



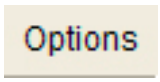
Ctrl+Alt+Delete – Special button key to send the “Control Alt Delete” key combination to the remote system (see also section 3.5.1 for defining new button keys).

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



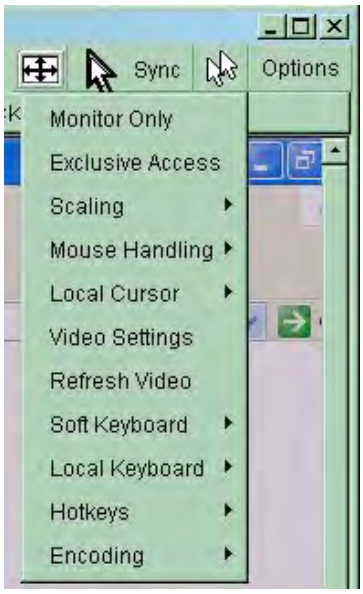
Sync mouse button - Activates the mouse synchronization process. Choose this option in order to synchronize the local with the remote mouse cursor. This is especially necessary when using accelerated mouse settings on the host system. In general, there is no need to change mouse settings on the host.

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



Options – To open the Options menu, click on the button “Options.”

Remote Console Options Menu



A short description of the options follows.

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

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

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

  Remote Console Exclusive Mode 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.

Remote Console Options Menu: Scaling

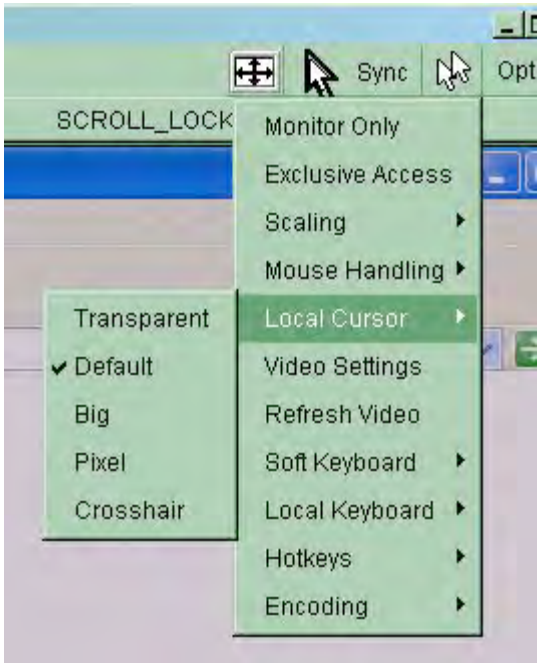
When you designate 25%, 50%, or 100% scaling, the size of Remote Console window is calculated according to the remote host video setting with scaling algorithm execution. When you designate “Scale to fit,” the remote video displaying is scaled to fit the size of Remote Console window.

- **Mouse Handling:** The submenu for mouse handling offers two options for synchronizing the local and the remote mouse cursors.
  - **Fast Sync:** The fast synchronization is used to correct a temporary, but fixed skew.
  - **Intelligent Sync:** Use this option if the fast sync does not work or the mouse settings have been changed on the host system.

	**Warning!** The Mouse Handling Intelligent Sync method takes more time than the Fast Sync and requires a correctly adjusted picture. Use the auto adjustment function 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 1.4.2 or above offers the full list.

Remote Console Options Menu: Cursor



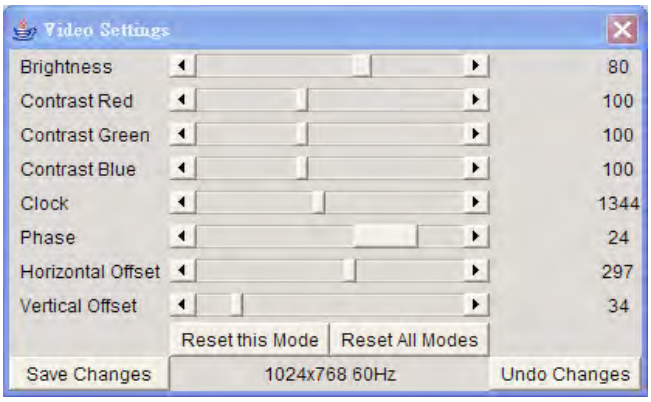
- **Video Settings:** Opens a panel for changing the IP console video settings. IP console features two different dialogs, which are for adjusting the video settings.

  - **Video Settings through the HTML-Frontend:** To enable local video port, select this option. This option decides if the local video output of IP console is active and passing through the incoming signal from the host system.

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

- **Video Settings through the remote console:** allows you to make adjustments manually. The panel is shown in the figure below and explanations follow.

Video Settings Panel



- **Brightness:** Controls the brightness of the picture
- **Contrast:** Controls the contrast of the picture
- **Clock:** Defines the horizontal frequency for a video line and depends on the video mode. Different video card types may require different values here. The default settings in conjuction with the auto adjustment procedure should be adequate for all common configurations. If the picture quality is still bad after auto adjustment you may try to change this setting together with the sampling phase to achieve a better quality.
- **Phase:** Defines the phase for video sampling, used to control the display quality together with the setting for sampling clock.
- **Horizontal Position:** Use the left and right buttons to move the picture in horizontal direction while this option is selected.
- **Vertical Position:** Use the left and right buttons to move the picture in vertical direction while this option is selected.
- **Reset this Mode:** Reset mode specific settings (Clock , Phase and Position) to the factory-made defaults.
- **Reset all Modes:** Reset all settings to the factory-made defaults.
- **Save Changes:** Save changes permanently
- **Undo Changes:** Restore last settings

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

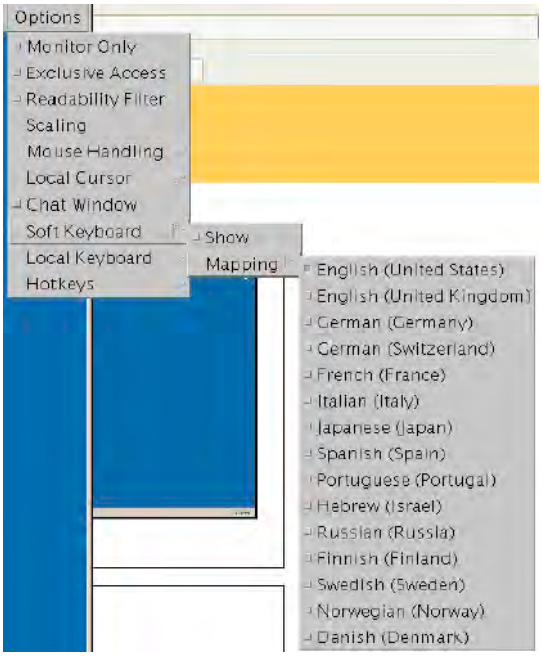
- **Soft Keyboard:** Opens up the Menu for the Soft Keyboard.

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

    Soft Keyboard

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

    Soft Keyboard Mapping Options

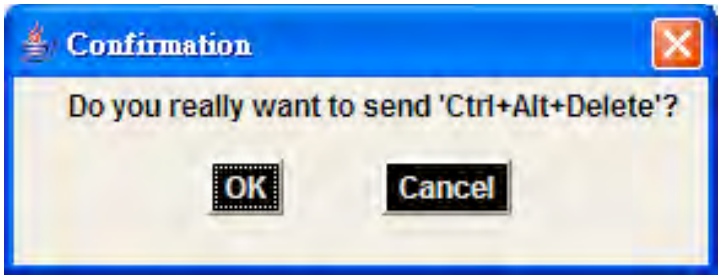


- **Local Keyboard:** Used to change the language mapping of your browser machine running the Remote Console Applet. Normally, the applet determines the correct value automatically. However, depending on your particular JVM and your browser settings this is not always possible. A typical example is a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

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

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

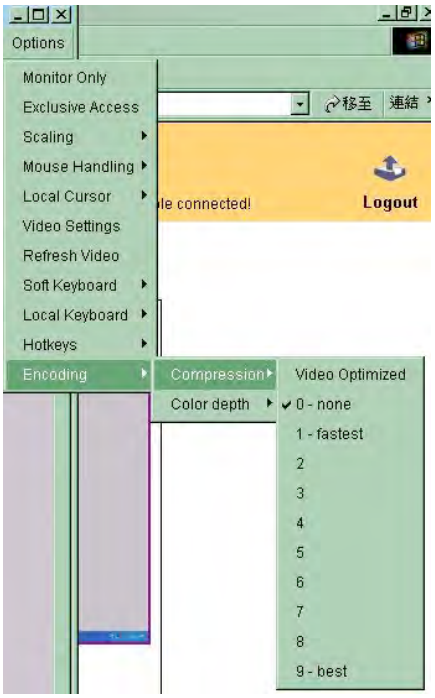
  Remote Console Configuration Dialog



- **Encoding:** These options are used to adjust the encoding level in terms of compression and color depth. They are only available unless "Transmission Encoding" is determined automatically (see Transmission Encoding in section 3.5.1).

  - **Compression Level:** you may select a value between 1 and 9 for the desired compression level with level 1 enabling the fastest compression and level 9 the best compression.

    Encoding Compression Menu



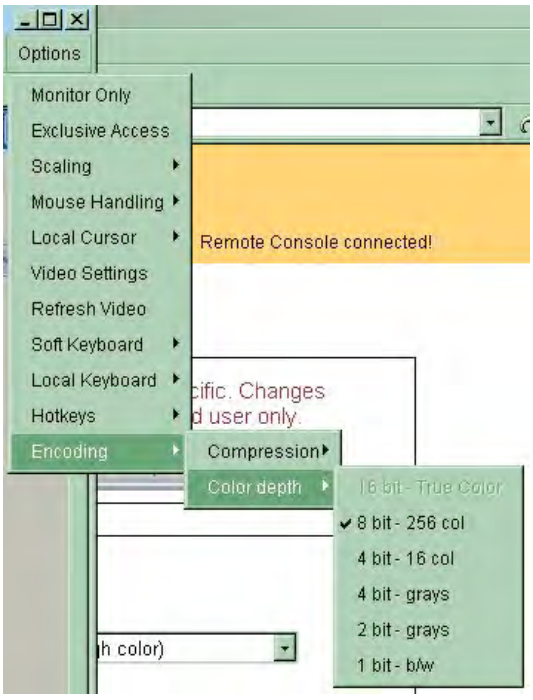
The most suitable compression level should always be seen as a compromise between the network bandwidth that is available, on your video picture to be transferred, and on the number of changes between two single video pictures. We recommend using a higher compression level if the network bandwidth is low. The higher the compression level the more time is needed to pack and unpack the video data on either side of the connection. The compression quality depends on the video picture itself, e.g. the number of the colors or the diversity of pixels. The lower the compression quality, the more data have to be sent and the longer it may take to transfer the whole video picture.

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

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

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

Options - Encoding – Color Depth Menu

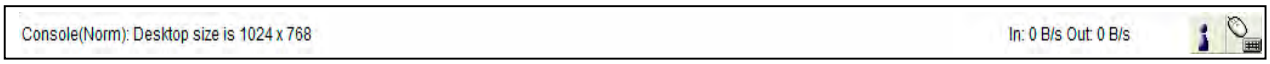


Note: *If displaying motion pictures on a connection with low speed you may achieve an improvement regarding the video transfer rate by lowering the color depth and disabling the option "Video Optimized." As a general result, the data rate is reduced (less bits per color). Furthermore, the OPMA module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

2.4.2 Remote Console Status Line

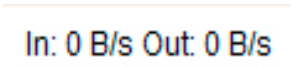
The Remote Console status line, displayed at the bottom of the Remote Console screen (see section 2.3), shows both console and the connection state. The size of the remote screen is displayed. The figure below was taken from a Remote Console with a resolution of 800x600 pixels. The value in brackets describes the connection to the Remote Console. “Norm” means a standard connection without encryption, “SSL” means a secure connection.

Status line



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

Status line transfer rate



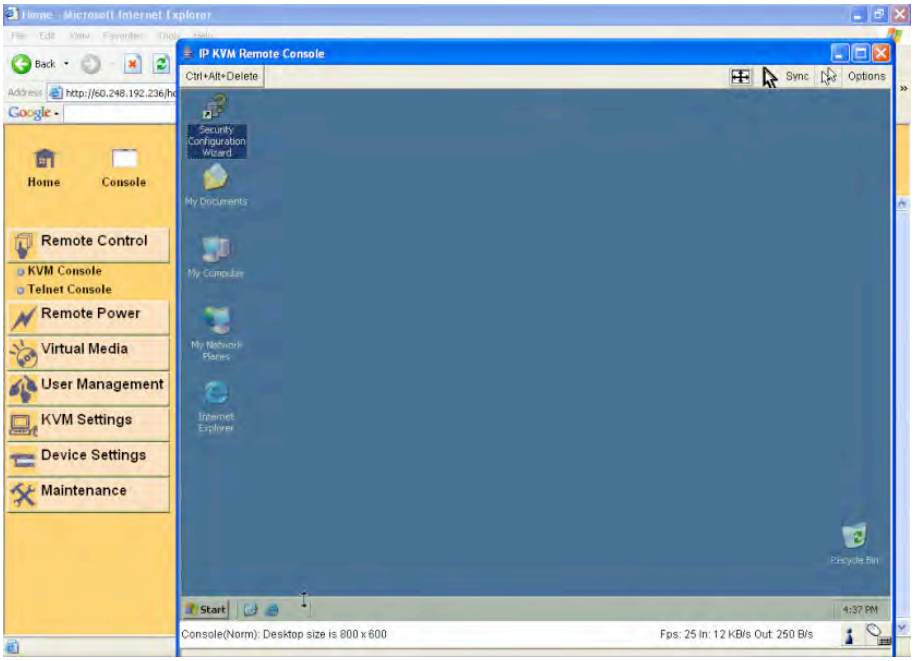
3.1 Remote Control

The Remote Control menu provides access to attached servers through the KVM Console and to an optional serial connection through the Telnet Console.

3.1.1 KVM Console

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

KVM Console



3.1.2 Telnet Console

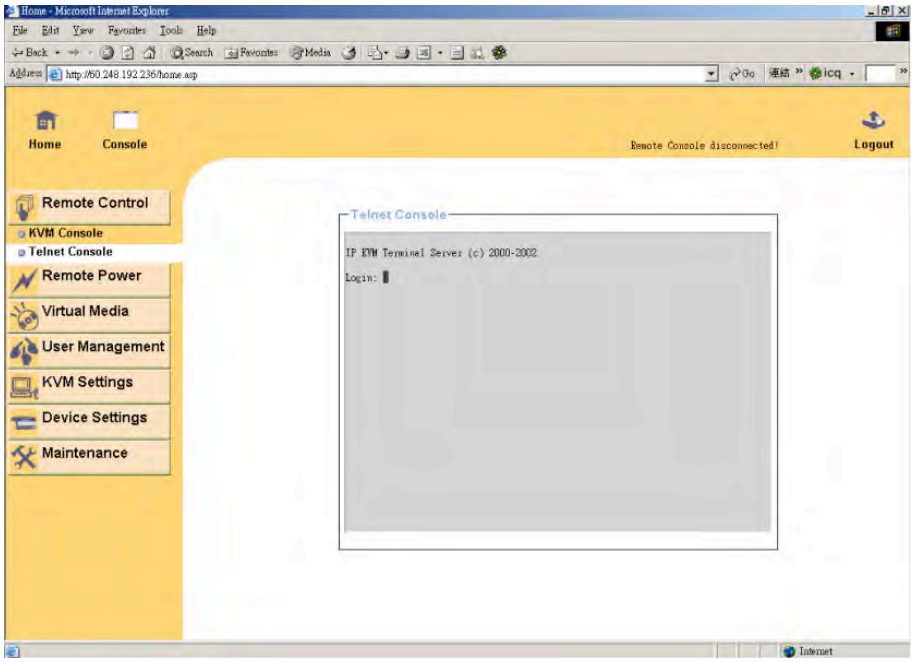
The IP module firmware features a Telnet server that enables a user to connect via a standard Telnet client. In case the Telnet program is using a VT 100, VT 102 or VT 220 terminal or an according emulation, it is even possible to perform a console redirection as long as the IP console host machine is using a text mode screen resolution.

Connecting to the IP console 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 IP console. This will prompt for username and password in order to log into the device. The credentials that need to be entered for authentication are identical to those of the web interface. That means, the user management of the Telnet interface is entirely controlled with the according functions of the web interface.

Telnet Console



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

In general, the Telnet interface supports two operation modes: the command line mode and the terminal mode. The command line mode is used to control or display some parameters. In terminal mode the pass-through access to serial port 1 is activated (if the serial settings were configured accordingly, see section 3.6.5). All inputs are redirected to the device on serial port 1 and its answers are displayed on the Telnet interface.

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

- help – Displays the list of possible commands
- cls – Clears the screen
- quit – Exists the current session and disconnects from the client
- version – Displays the release information
- terminal – Starts the terminal passthrough mode for serial port 1. The key sequence *esc exit* switches back to the command mode.

3.2 Remote Power Control

CPI PDUs are not compatible with the Remote Power Control function which requires a serial connection between the KVM and a PDU. CPI PDUs have their own IP console, connect directly to the network and are accessed directly using a web browser.

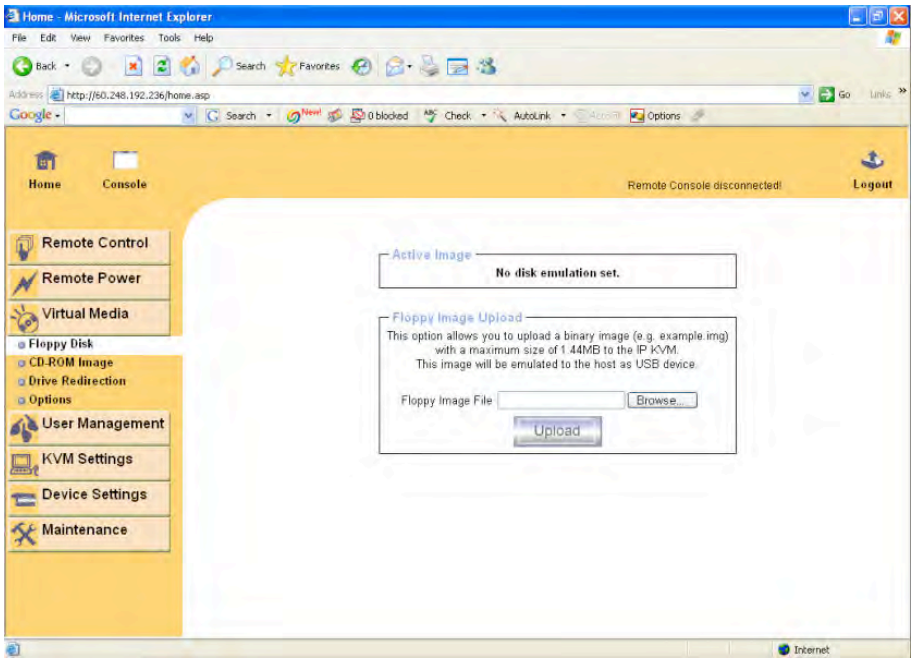
3.3 Virtual Media

The Virtual Media menu provides several ways to share data with the servers attached to the IP KVM Switch from the remote system that is accessing the servers using the IP console.

3.3.1 Floppy Disk – Upload a Floppy Image

Click the Virtual Media button and then the Floppy Disk button to upload a floppy image.

Virtual Media Floppy Disk Screen



A certain (floppy) image can be built up in two steps.

- Click “Browse” button and select the image file.

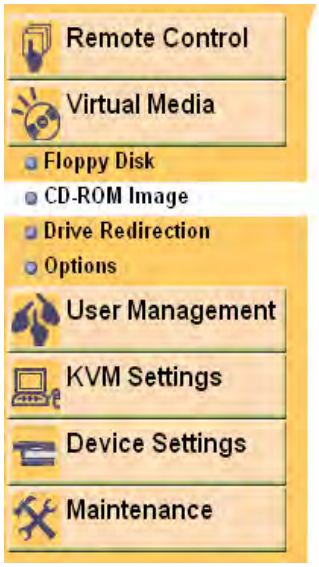
- Click “Upload” button to upload the chosen image file into the IP console’s onboard memory. This image file is kept in the onboard memory of the IP console until the end of the current session, as you logged out, or initiated a reboot of the IP console.

The maximum image size is limited to 1.44MB. For a larger image please see CD-ROM Image section below.

3.3.2 CD–ROM Image

- **Use An Image on Windows Share (SAMBA):**
  To include an image from a Windows share, select “CD-ROM” from the Virtual Media submenu.

Selecting CD ROM



Under Image on Windows Share, the following information has to be given to mount the image properly:

- **Share host:** The server name or its IP address.
- **Share folder name:** The name of the share folder to be used.
- **Image file name:** The name of the image file on the share folder.
- **User name:** If necessary, specify the user name for the share named in advance. If unspecified, and a guest account is activated, this guest account information will be used as your login.
- **Password:** If necessary, specify the password for the given user name.

Select A Windows Share

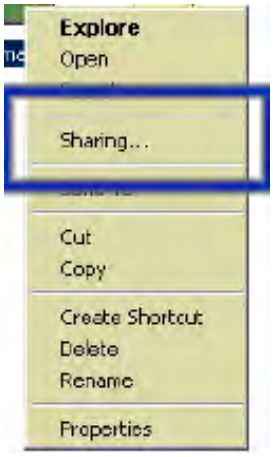
To register the specified file image and its location click on the button “Set.”

The specified image file should be accessible from the IP console. The information above has to be given from the point of view of the IP console. It is important to specify correct IP addresses, and device names. Otherwise, IP console may not be able to access the referenced image file.

Furthermore, the specified share has to be configured correctly. Therefore, administrative permissions are required. As a regular user you may not have these permissions. You should either login as a system administrator (or as “root” on UNIX systems), or ask your system administrator for help to complete this task.

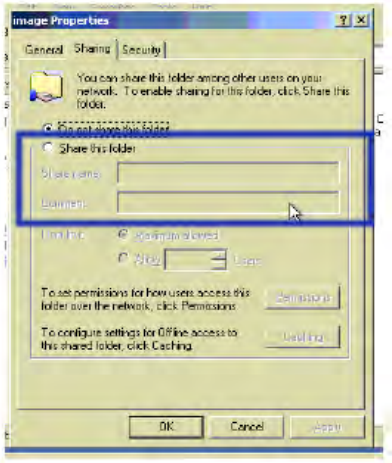
- **For Windows 2000/XP:**
  Open Windows Explorer, navigate to the directory (or share), and press the right mouse button to open the context menu.

  Explorer Context Menu



  Select “Sharing” to open the configuration dialog.

  Share Configuration Dialog Box



  Adjust the settings for the selected directory.
  - Activate the selected directory as a share. Select “Sharing this folder.”
  - Choose an appropriate name for the share. You may also add a short description for this folder (input field “Comment”).
  - If necessary, adjust the permissions (button “permissions”).
  - Click “OK” to set the options for this share.

- **For UNIX and UNIX-like OS (Sun Solaris, and Linux)**
  If you like to access the share via SAMBA, SAMBA has to be set up properly. You may either edit the SAMBA configuration file /etc/samba/smb.conf, or use the Samba Web Administration Tool (SWAT) or WebMin to set the correct parameters.

- **Creating a Floppy Image:**

  - **Floppy Images for *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.)

  - **Floppy Images for *MS Windows:*** Use an imaging tool like “Raw Write for Windows.”

- **Creating a CD ROM/ISO Image**

  - **CD-ROM/ISO Images For *UNIX and UNIX-like OS*:** To create an image file, make use of “dd.” This is one of the original UNIX utilities and is included in every UNIX-like OS (UNIX, Sun Solaris, and Linux).

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

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

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

  - **CD-ROM/ISO Images For MS Windows:** To create the image file, use your favorite CD imaging tool. Copy the whole contents of the disc into one single image file on your hard disk.

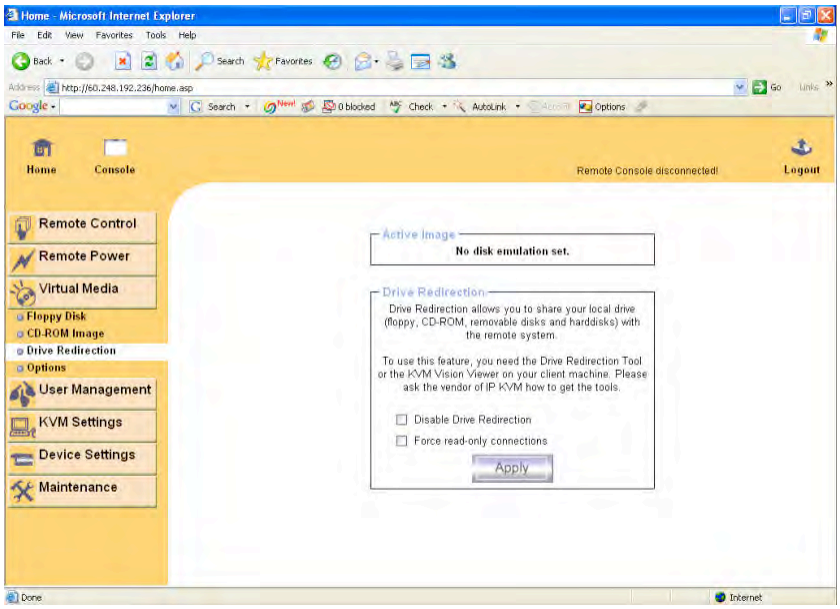
    For example, with “Nero” you choose “Copy and Backup.” Then, navigate to the “Copy Disc” section. Select the CD ROM or DVD drive you would like to create an image from. Specify the filename of the image, and save the CD ROM content in that file.

    Nero selection dialog

3.3.3. Drive Redirection

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

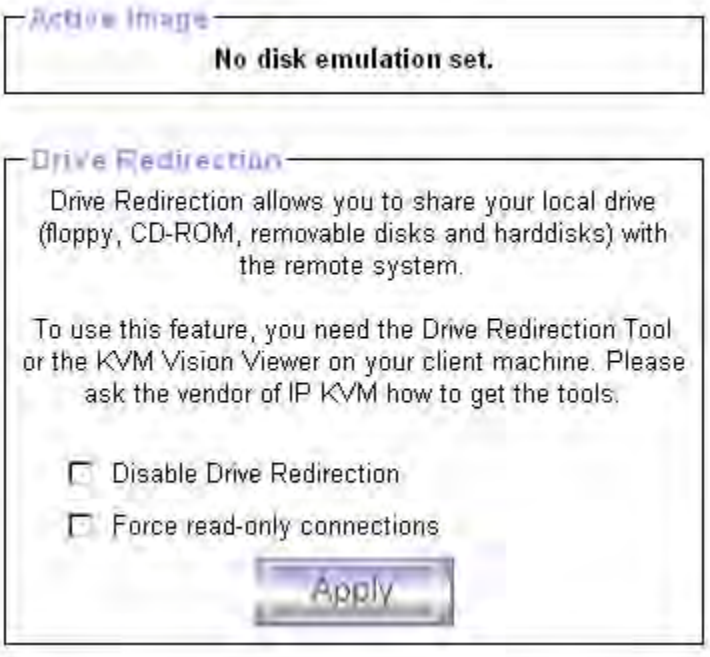
Drive Redirection Menu



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

Under the Drive Redirection menu, there are two setup options:

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

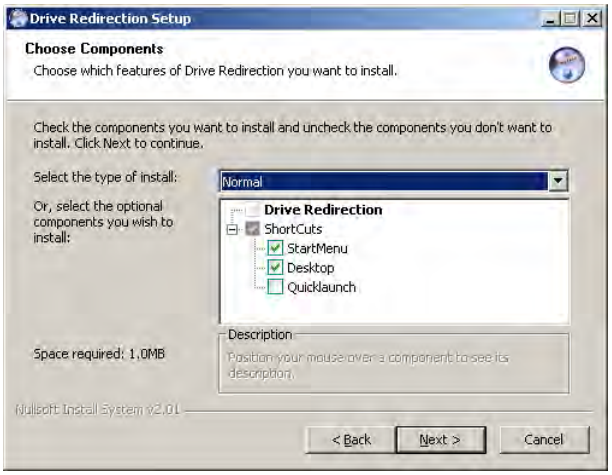


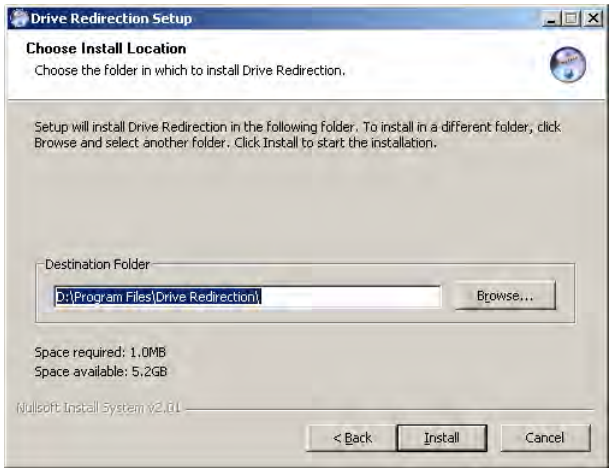
Select the desired options and click “Apply” to submit your changes.
The Drive Redirection Setup Wizard will open so you can install drivers.

3.3.3.1 Installing The Drive Redirection Drivers

On first use, you will need to install drivers for the drive redirection software. Please follow the Drive Redirection Setup Wizard step by step to install the driver from the included CD ROM.

Drive Redirection Setup

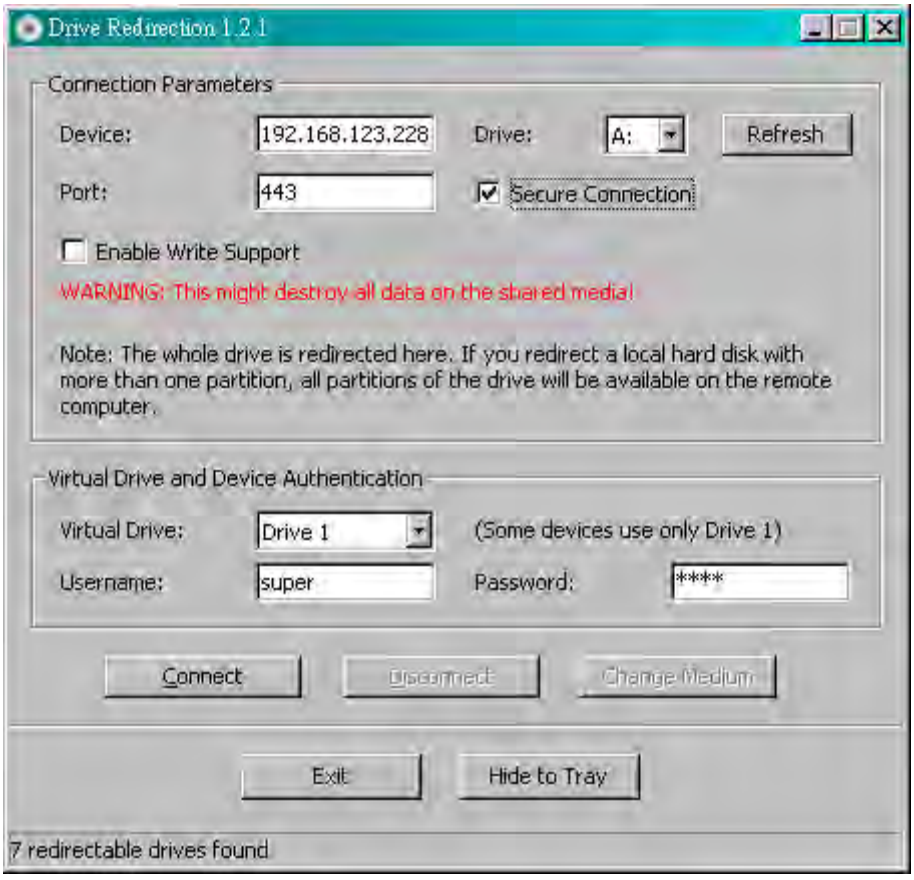




3.3.3.2 Setup Drive Redirection

Start Drive Redirection to display the Drive Redirection dialog.

Drive Redirection Dialog



Under Connections Parameters, designate the drive to redirect.

- **Device –** This is the address (either the DNS name or the IP address) of the IP console you would like to connect to.

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

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

- **Port –** This is the network port. By default, IP console uses the remote console port (#443) here. You may change this value if you have changed the remote console port in your IP consoles network settings. (see section 3.6.1)

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

- **Enable Write Support –** Enable write support means that the remote computer is allowed to write on your local drive. As you can imagine, this is very dangerous. If both the remote and the local system try to write data on the same device, this will certainly destroy the file system on the drive. Please use this only when you exactly know what you are doing.

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

- **Virtual Drive and Device Authentication –** Enter the administrator's username and password for the IP console. The factory default Username is "super" and the default Password is "pass."

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

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

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

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

- **Exit/Hide** – If the "Exit" button is pressed, the Drive Redirection software is closed. If a Drive Redirection connection is active, the connection will be closed before the application terminates.

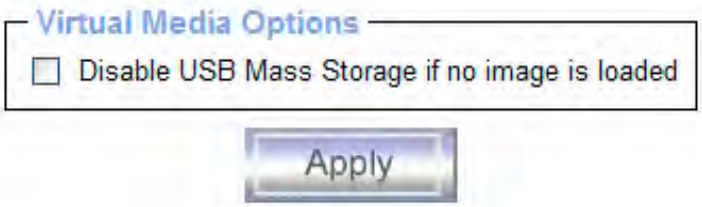
Using the Hide to Tray button the application is hidden, but not terminated completely. That means that an active connection will be kept active until it is closed explicitly. You can access the software by its tray icon. The tray icon also shows whether a connection is established or not. A double click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

Tray Icon and Menu for Drive Redirection

3.3.4 Options

- **Disable USB Mass Storage if no image is loaded** - Set this option to disable the mass storage emulation (and hide the virtual drive) if no image file is currently loaded.

USB Mass Storage Option



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

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

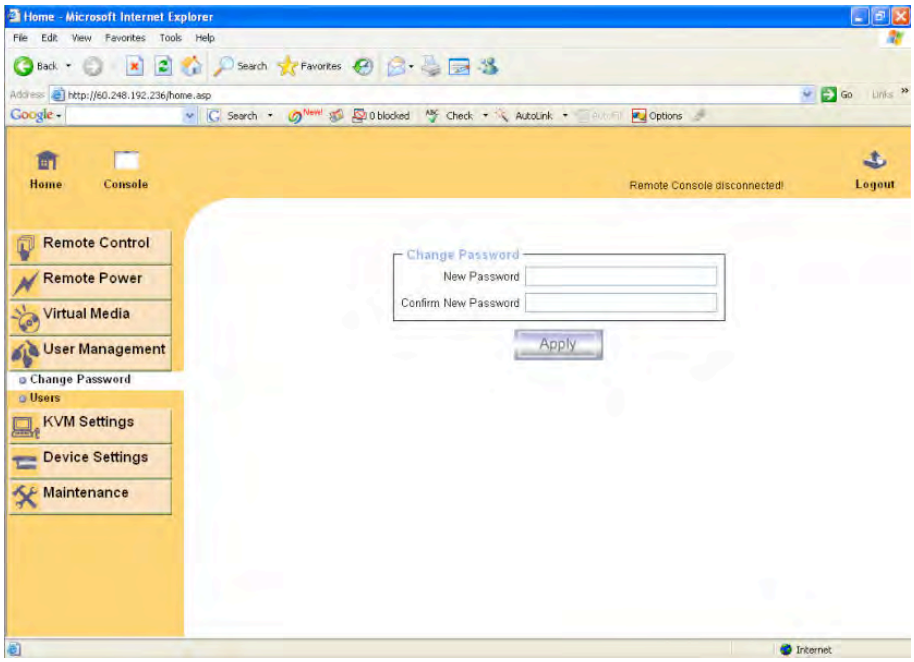
3.4 User Management

The User Management button allows you to change passwords and create/edit individual user accounts.

3.4.1 Change Password

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

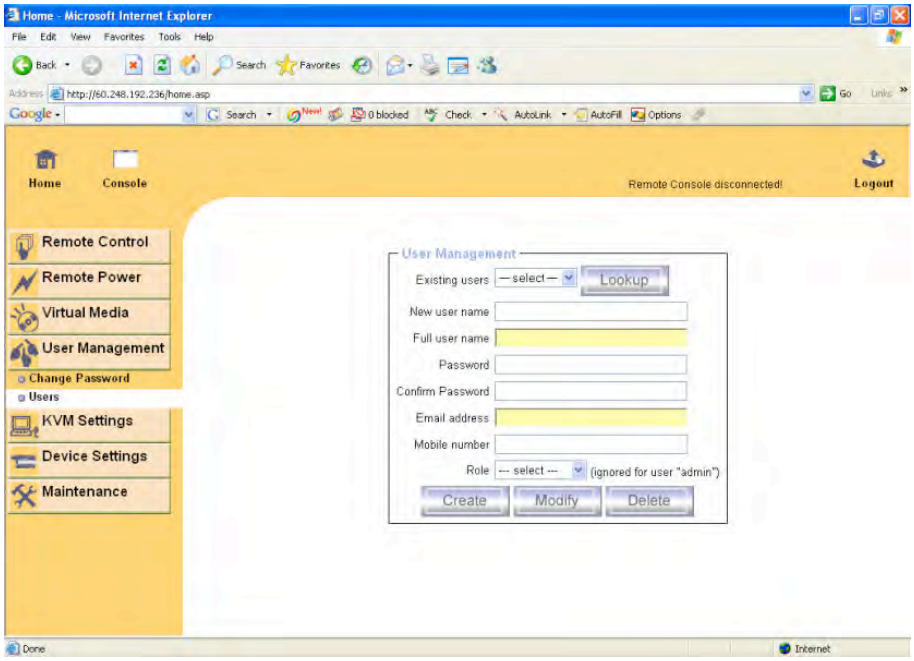
Set Password dialog



3.4.2 Users and Groups

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

Set User Dialog



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

Select the Users menu to set up a new user or change an existing user account:

- **Existing users:** Select an existing user for modification. Once a user has been selected, click the lookup button to see the user information.
- **New User name:** The new user name for the selected account.
- **Password:** The password for the login name. It must be at least three characters long.
- **Confirm password:** Confirmation of the password above.
- **Email address:** This information is optional.
- **Mobile number:** This information is optional.
- **Role:** Each user can be a member of a group (named a “role”) - either an administrator, or a regular user. Choose the desired role from the selection box.

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

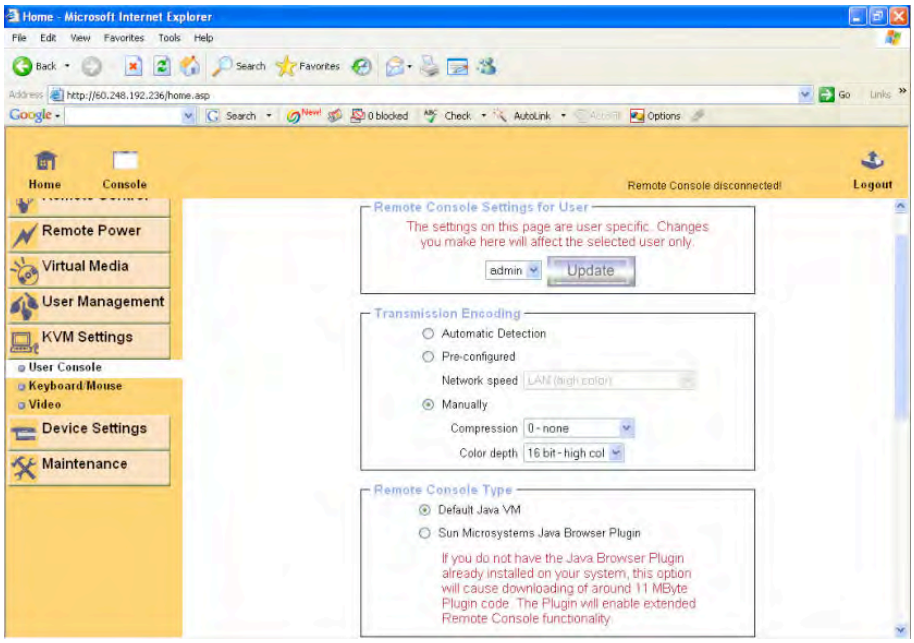
Note:The IP console is equipped with a host-independent processor and memory unit which both have a limitation in terms of the processing instructions and memory space. To guarantee an acceptable response time we recommend not exceeding 50 user profiles.

3.5 KVM Settings

3.5.1 User Console

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

User Console Settings



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

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

    - **Automatic detection:** The encoding and the compression level is determined automatically from the available bandwidth and the current content of the video image.
    - **Pre-configured:** The pre-configured settings deliver the best result because of optimized adjustment of compression and color depth for the indicated network speed.
    - **Manually:** Allows to adjustment of both compression rate and the color depth individually. Depending on the selected compression rate the data stream between the IP console and the Remote Console will be compressed in order to save bandwidth. Since high compression rates consume more computing power of IP console, they should not be used while several users are accessing the IP console simultaneously.

Note: The standard color depth is 16 Bit (65536 colors). The other color depths are intended for slower network connections in order to allow a faster transmission of data. Therefore compression level 0 (no compression) uses only 16 Bit color depth. At lower bandwidths only 4 Bit (16 colors) and 2 Bit (4 gray scales) are recommended for typical desktop interfaces. Photo-like pictures have best results with 4 Bit (16 gray scales). 1 Bit color depth (black/white) should only be used for extremely slow network connections.

- **Remote Console Type** : Specifies which Remote Console Viewer to use.
  - **Default Java VM:** Uses the default Java Virtual Machine of your Browser. This may be the Microsoft JVM for the Internet Explorer, or the Sun JVM if it is configured this way. Use of the Sun JVM may also be forced (see below).
  - **Sun Microsystems Java Browser Plugin:** Instructs the web browser of your administration system to use the JVM of Sun Microsystems. The JVM in the browser is used to run the code for the Remote Console window, which is actually a Java Applet. If you check this box for the first time on your administration system and the appropriate Java plug-in is not already installed on your system, it will be downloaded and installed automatically. However, in order to make the installation possible, you still need to answer the according dialogs with “yes.” The download volume is around 11 Mbytes. The advantage of downloading Sun's JVM provides a stable and identical Java Virtual Machine across different platforms. The Remote Console software is optimized for this JVM version and offers a wider range of functionality when run in SUN's JVM. Please make sure that you are installing Sun JVM 1.4.2 or above to your client system.

Additional User Console Settings

- **Miscellaneous Remote Console Settings:** Logon preferences.
  - **Start in Monitor Mode:** Sets the initial value for the monitor mode. By default the monitor mode is off. If 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:** Specifies a hotkey combination which starts either the mouse synchronization process if pressed in the Remote Console, or is used to leave the single mouse mode.

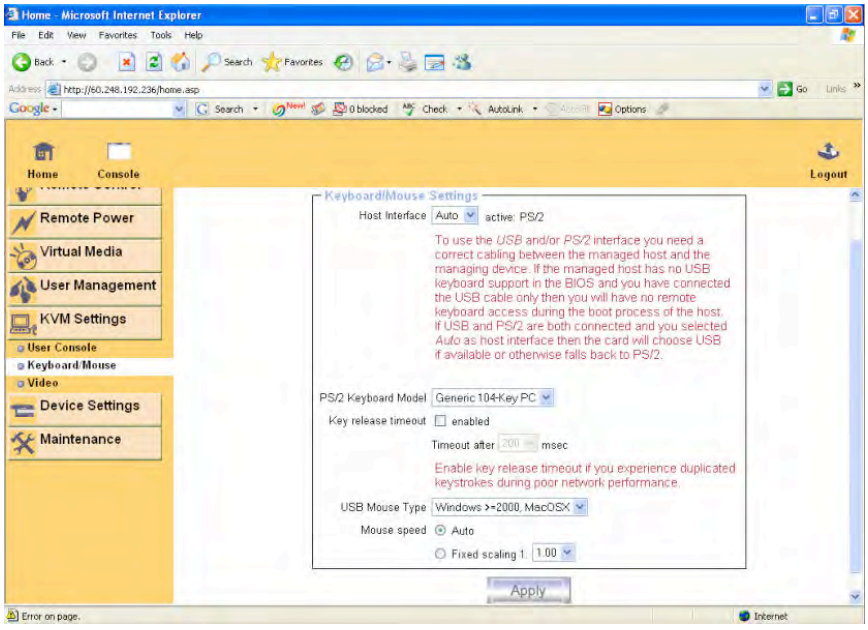
- **Remote Console Button Keys:** Button Keys allow simulating keystrokes on the remote system that cannot be generated locally. The reason for this might be a missing key or the fact, that the local operating system of the Remote Console is unconditionally catching this keystroke already. Typical examples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

  The syntax to define a new Button Key is as follows:
  [confirm] <keycode>[+|-[*]<keycode>]*
  - “confirm” requests confirmation by a dialog box before the key strokes will be sent to the remote host.
  - “keycode” is the key to be sent.
  - Multiple key codes can be concatenated with a plus, or a minus sign. The plus sign builds key combinations, all keys will be pressed until a minus sign or the end of the combination is encountered. In this case all pressed keys should be released in reversed sequence. The minus sign builds single, separate key presses and releases.
  - The star inserts a pause with duration of 100 milliseconds.

3.5.2 Keyboard/Mouse

Under KVM Settings, select Keyboard/Mouse to modify keyboard and mouse settings.

Keyboard and Mouse Settings



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

Warning!
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 the card will select “USB” if available or otherwise falls back to “PS/2.”

To get 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 extendend by three additional windows keys, “Generic 106-Key PC” for a Japanese keyboard, and “Apple Macintosh” for the Apple Macintosh.

- **Keyboard release timeout** - Recommend “enable” for keyboard timeout when host is UNIX or UNIX-like OS.

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

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

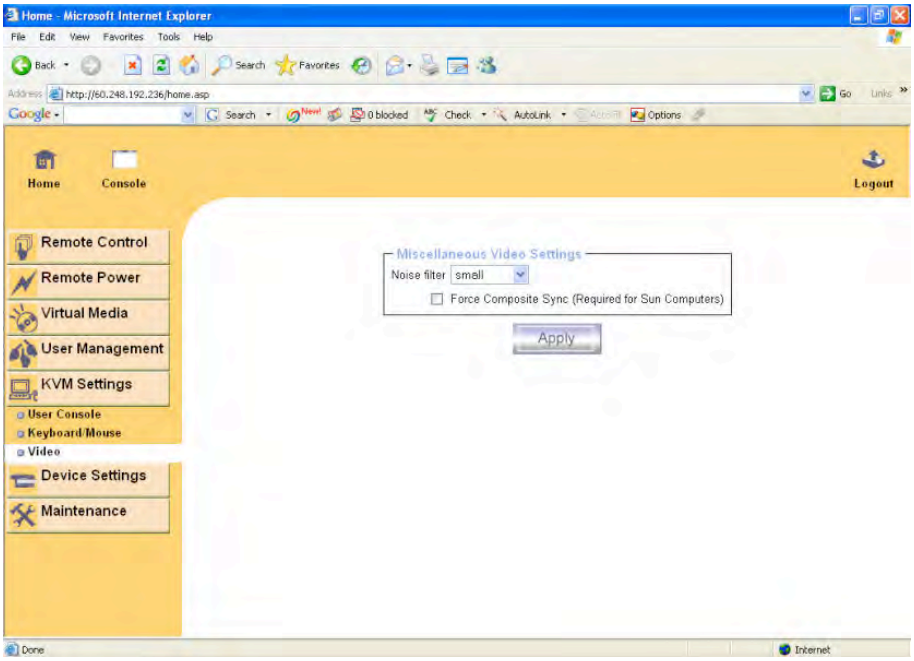
  You may also set a fixed scaling which determines the pixel-amount of the remote mouse pointer movement when the local mouse pointer is moved by one pixel. This option is used to manually control the remote mouse speed and only works when the mouse settings on the host are linear. This means mouse acceleration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

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

3.5.3 Video

Under KVM Settings, select Video to change the video settings.

Video Settings



- **Miscellaneous Video Settings**

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

  - **Force Composite Sync (Required for Sun Computers):** When connecting the device directly to legacy Sun computer (with composite sync as the video output), it may be possible that the IP console does not recognize the composite sync automatically. To support signal transmission from a Sun machine, enable this option. If not enabled the picture of the remote console will not be visible.

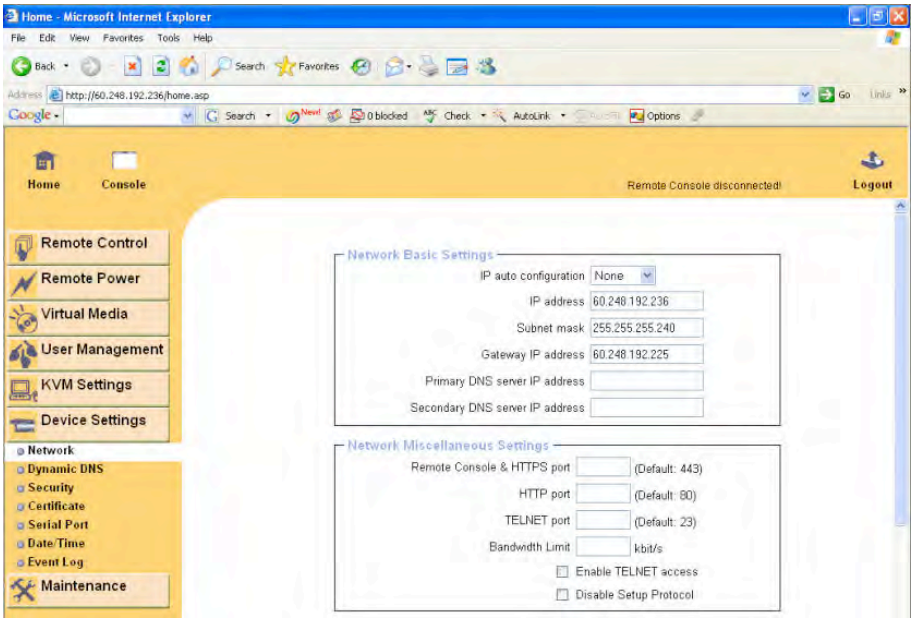
To set the options, click on the button “Apply.”

3.6 Device Settings

3.6.1 Network

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

Network Settings



	**Warning!** The initial IP configuration is usually done directly at the host system using the special procedure described in Section 1.2 Using The IP Configuration Setup Tool. Changing the network settings of the IP console might result in losing connection to it. In case you change the settings remotely make sure that all the values are correct and you still have an option to access the IP console.

- **Network Basic Settings**
  - **IP auto configuration:** With this option you can control if the IP console should fetch its network settings from a DHCP or BOOTP server. For DHCP, select “dhcp,” and for BOOTP select “bootp” accordingly. If you choose “none” then IP auto configuration is disabled.
  - **IP address:** IP address in the usual dot notation.
  - **Subnet Mask:** The net mask of the local network.
  - **Gateway IP address:** In case the IP console should be accessible from networks other than the local one, this IP address must be set to the local network router's IP address.

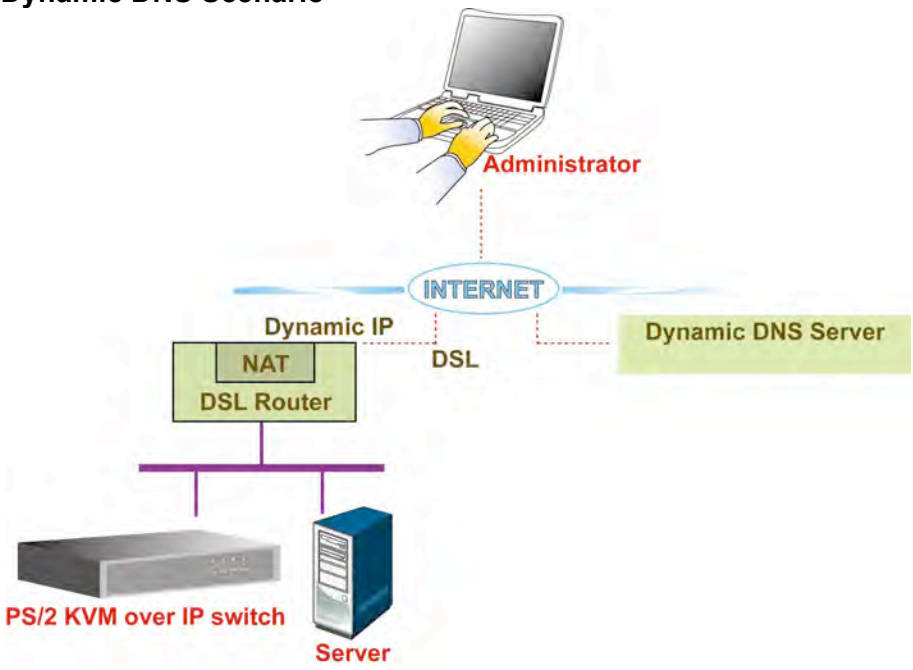
- **Primary DNS Server IP Address:** IP address of the primary Domain Name Server in dot notation. This option may be left empty, however the IP console will not be able to perform name resolution.
- **Secondary DNS Server IP Address:** IP address of the secondary Domain Name Server in dot notation. It will be used in case the Primary DNS Server cannot be contacted.

- **Network Miscellaneous Settings**
  - **Remote Console and HTTPS port:** Port number at which the IP console'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 IP console's HTTP server is listening. If left empty the default value will be used.
  - **Telnet port:** Port number at which the IP console's Telnet server is listening. If left empty the default value will be used.
  - **Bandwidth limitation:** The maximum network traffic generated through the IP consoles Ethernet device. Value in Kbit/s.
  - **Enable Telnet access:** Set this option to allow accessing the IP console using the Telnet Gateway, see section 3.1.2, Telnet Console.
  - **Disable Setup Protocol:** Enable this option to exclude the IP console from the setup protocol. Setup protocol is a proprietary layer-2 MAC-based protocol to allow some configuration software to detect IP consoles in the network, even without IP address, and then config network related settings to IP console.
  - **LAN Interface Settings:** The “Autodetect” will set the Ethernet speed to the fastest possible value supported by both endpoints of the link. For example, if you use a 10M/half duplex HUB, this speed will be auto-selected. If this option does not work with some network device (HUB, switches, and routers), you can set the Ethernet interface speed of IP console manually to the values as supported by the network device.

3.6.2 Dynamic DNS

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

Dynamic DNS Scenario



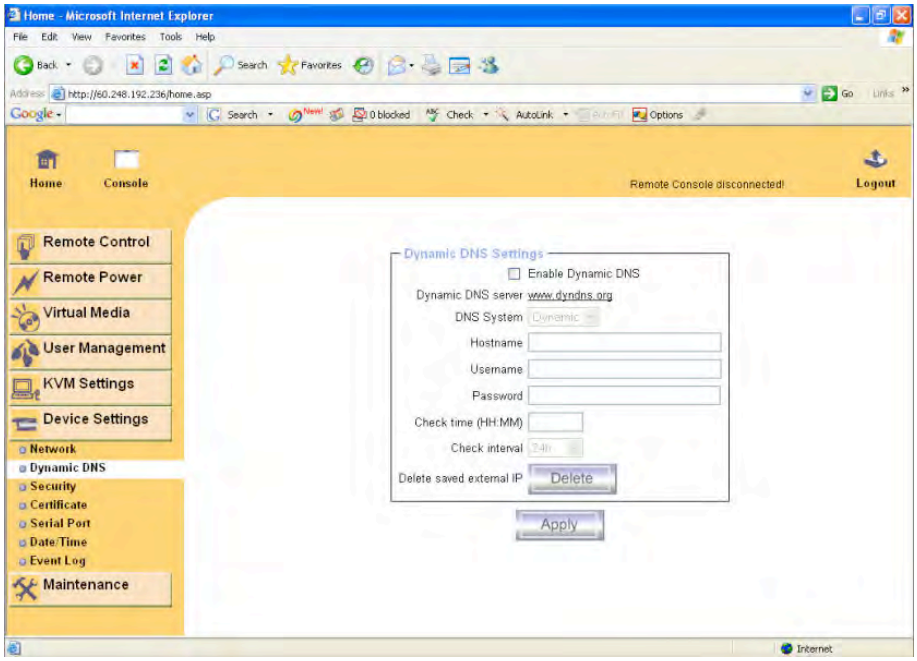
A freely available Dynamic DNS service (www.dyn.com/dns/dyndns-free) can be used in the above scenario.

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

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

- Make sure that the LAN interface of the IP console is properly configured.
- Enter the Dynamic DNS Settings configuration dialog as shown in the figure below.

Dynamic DNS Dialog



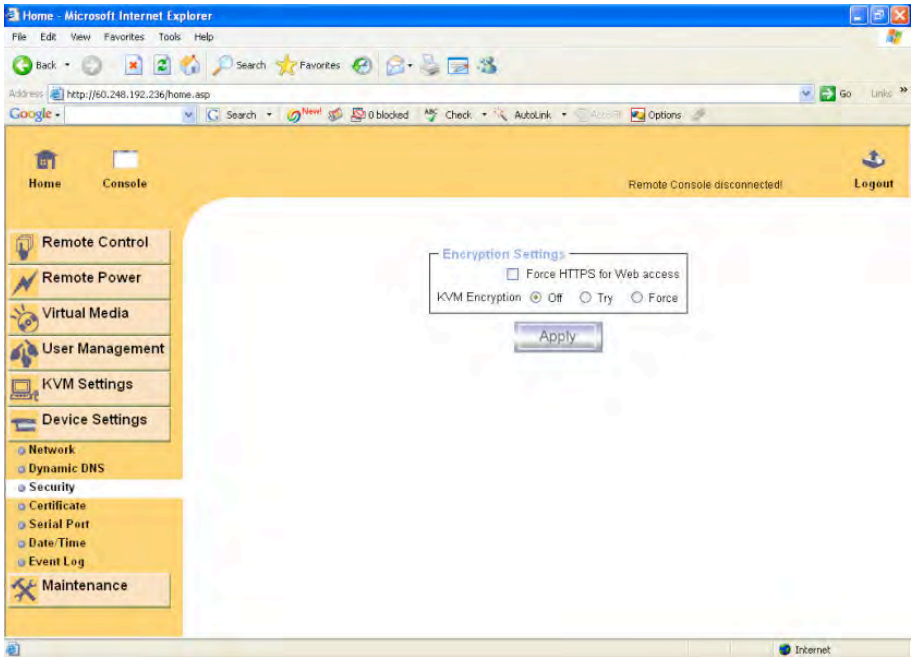
- **Enable Dynamic DNS** and change the settings according to your needs (see below).
  - **Enable Dynamic DNS:** This enables the Dynamic DNS service. This requires a configured DNS server IP address.
  - **Dynamic DNS server:** This is the server name where IP console registers itself in regular intervals. Currently, this is a fixed setting since only dyndns.org is supported for now.
  - **DNS System:** Choose Dynamic for free DNS service. Custom for your own domain.
  - **Hostname:** This is the hostname of the IP console that is provided by the Dynamic DNS Server. (Use the whole name including the domain, e.g. testserver.dyndns.org , not just the actual hostname).
  - **Username:** You have registered this username during your manual registration with the Dynamic DNS Server. Spaces are not allowed in the Nickname.
  - **Password:** You have used this password during your manual registration with the Dynamic DNS Server
  - **Check time:** The IP console registers itself for initiating the IP address of IP console stored in the Dynamic DNS server at this time.
  - **Check interval:** This is the interval for reporting again to the Dynamic DNS server for updating the IP address associated with the Domain Name of the IP console.
  - **Apply:** saves and activates changes.

	**Warning!** The IP console has its own independent real time clock. Make sure the time setting of the IP console is correct. (see section 3.6.6 Date And Time)

3.6.3 Security

Under Device Settings, select Security to change the security settings.

Device Security Dialog



- **Encryption Settings:**
  - **Force HTTPS:** If this option is enabled access to the web front-end is only possible using an HTTPS connection. The IP console will not listen on the HTTP port for incoming connections.

    In case you want to create your own SSL certificate that is used to identify the IP console refer to section 3.6.4 Certificate.

  - **KVM encryption:** This option controls the encryption of the RFB protocol. RFB is used by the Remote Console to transmit both the screen data to the administrator machine and keyboard and mouse data back to the host.

    If set to “Off” no encryption will be used.

    If set to ”Try” the applet tries to make an encrypted connection. In case connection establishment fails for any reason an unencrypted connection will be used.

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

3.6.4 Certificate

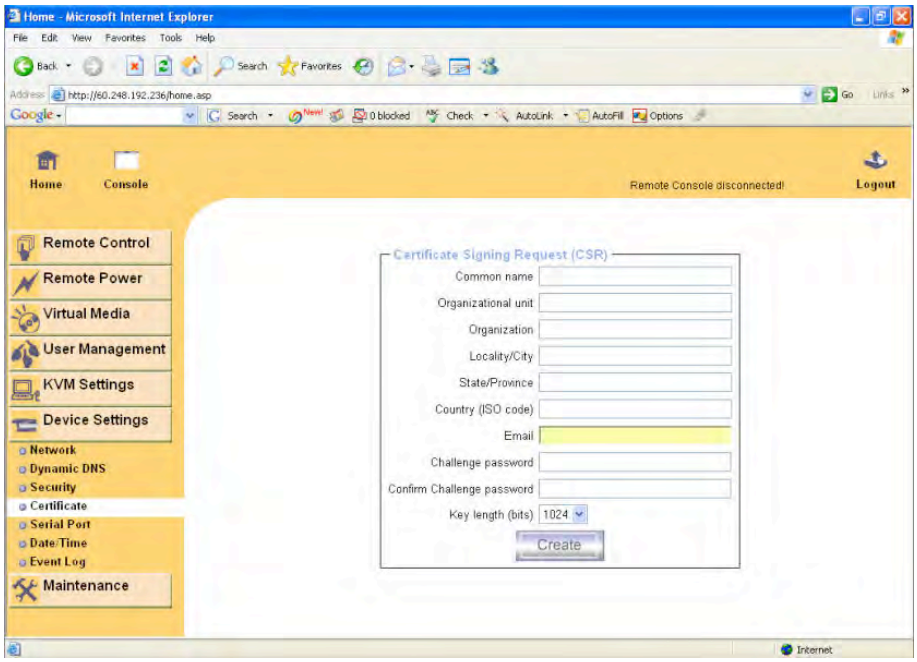
The IP console uses the Secure Socket Layer (SSL) protocol for any encrypted network traffic between itself and a connected client. During the connection establishment the IP console has to expose its identity to a client using a cryptographic certificate. The default certificate that comes with the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

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

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

1. Create a SSL Certificate Signing Request using the panel shown in the figure below. You need to fill out a number of fields that are explained below. Once this is done, click on the button “Create” which will initiate the Certificate Signing Request generation.

Certificate Settings Dialog

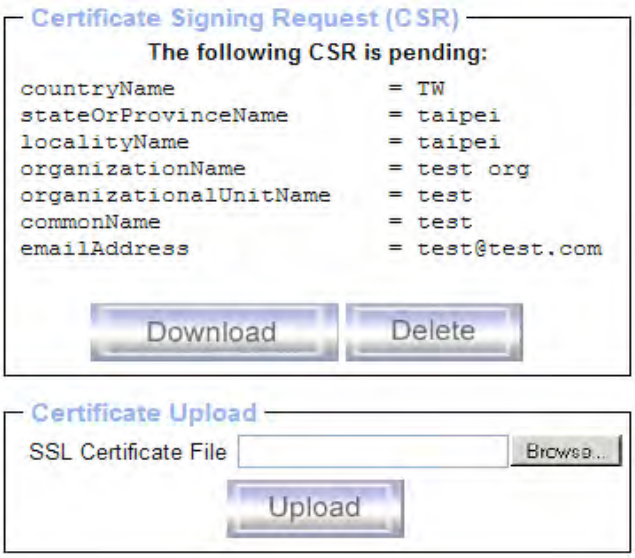


- **Common name:** This is the network name of the IP console once it is installed in the user's network (usually the fully qualified domain name). It is identical to the name that is used to access the IP console with a web browser (without the “http://” prefix). In case the name given here and the actual network name differ, the browser will pop up a security warning when the IP console is accessed using HTTPS.
- **Organizational unit:** This field is used for specifying to which department within an organization the IP KVM Switch belongs.
- **Organization:** The name of the organization to which the IP KVM Switch belongs.

- **Locality/City:** The city where the organization is located.
- **State/Province:** The state or province where the organization is located.
- **Country (ISO code):** The country where the organization is located. This is the two-letter ISO code, e.g. DE for Germany, or US for the USA. (Note: the country code has to be entered in CAPITAL LETTERS.)
- **Challenge Password:** Some certification authorities require a challenge password to authorize later changes on the certificate (e.g. revocation of the certificate). The minimal length of this password is four characters.
- **Confirm Challenge Password:** Confirmation of the Challenge Password.
- **Email:** The email address of a contact person that is responsible for the IP console and its security.
- **Key length:** This is the length of the generated key in bits. 1024 Bits are supposed to be sufficient for most cases. Longer keys may result in slower response time of the IP console during connection establishment.

2. Next, download the CSR to your administration machine with the “Download CSR” button.

SSL Certificate Download and Upload



3. Send the saved CSR string to a CA for certification. You will get the new certificate from the CA after a traditional authentication process (depending on the CA selected.)

Example CSR String

4. Upload the certificate to the IP console using the “Upload” button as shown in the figure below.

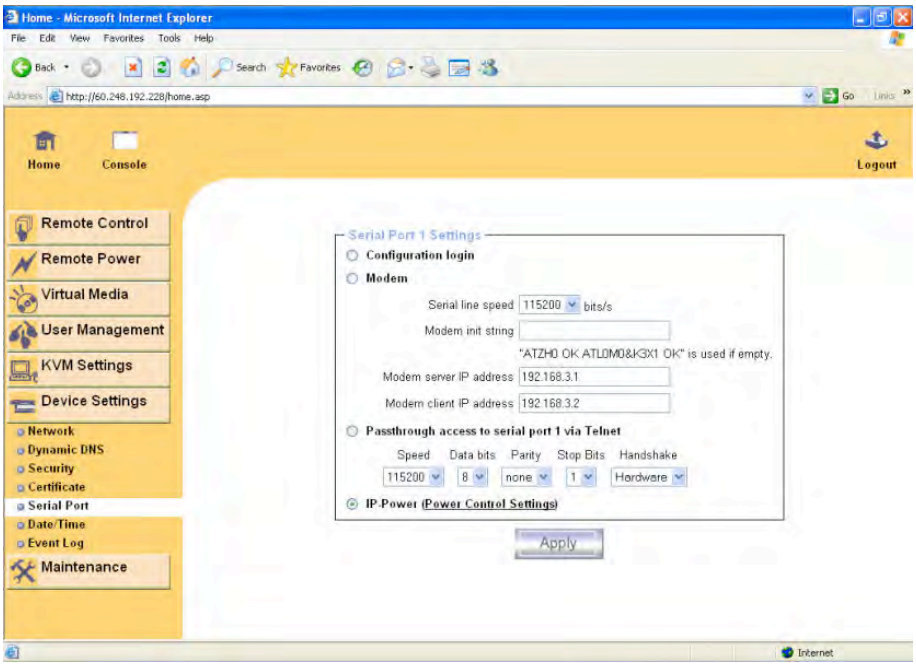
After completing these four steps, the IP console has its own certificate that is used for identifying the card to its clients.

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

3.6.5 Serial Port

The IP console's Device Settings for the Serial Port allows you to specify what device is connected to the serial port and how to use it.

Device Settings for the Serial Port



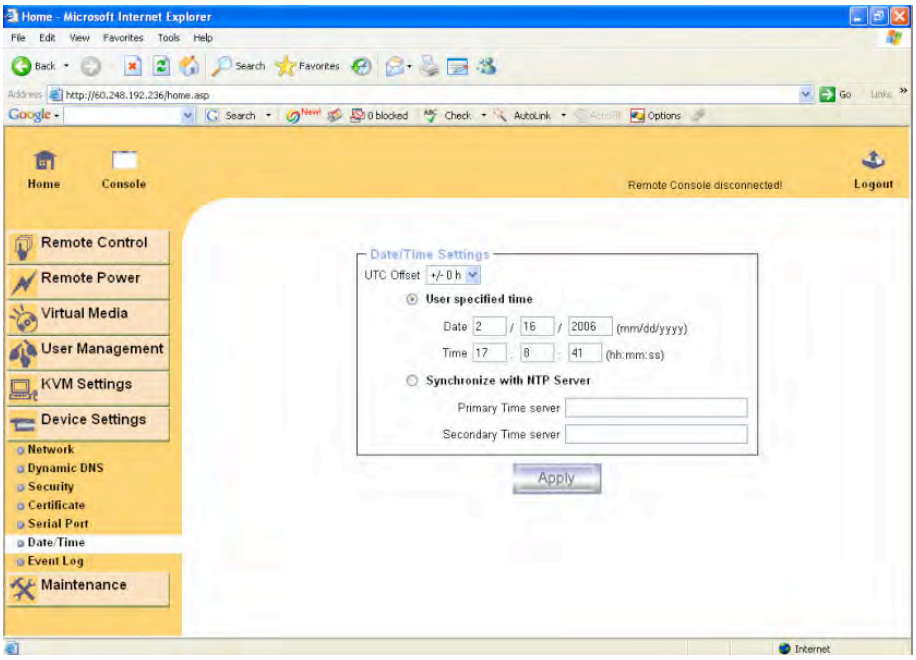
- **Serial Port Settings:**
  - **Configuration or console login:** Select this option if you will not be using the serial port for Passthrough access via Telnet.
  - **Modem:** This feature is not available on the CPI IP KVM Switch.
  - **Passthrough access to serial port via Telnet:** Using this option, it is possible to connect an arbitrary device to the serial port and access it (assuming it provides terminal support) via Telnet. Select the appropriate options for the serial port and use the Telnet Console, or a standard Telnet client to connect to the IP console, see section 3.1.2.
  - **IP Power:** This feature is not available on the CPI IP KVM Switch.

Click the "Apply" button to set the options.

3.6.6 Date And Time

This link refers to a page, where the internal real-time clock of the IP console can be set up (see the figure below).

Device Settings for Date and Time



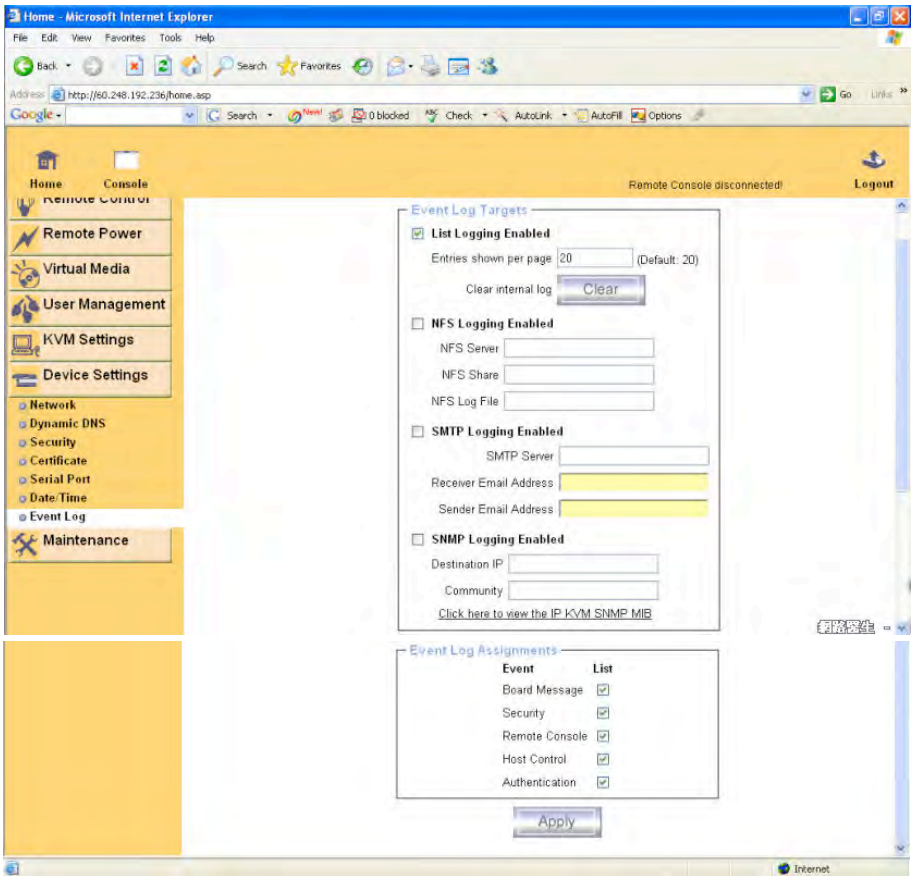
You have the possibility to adjust the clock manually, or to use a NTP timeserver. Without a timeserver, your time setting will not be persistent, so you have to adjust it again, after IP console loses power for more than a few minutes. To avoid this, you can use a NTP timeserver, which sets up the internal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

	**Warning!** There is currently no way to adjust the daylight saving time automatically. So you have to set up the UTC offset twice a year properly to the local rules of your country.

3.6.7 Event Log

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

Device Settings for Event Log



The common way to log events is to use the internal log list of the IP console. To show the log list, click on “Event Log” on the “Maintenance” page. In the Event Log Settings you can choose how many log entries are shown on each page. Furthermore, you can clear the log file here.

- **List Logging Enabled:** The common way to log events is to use the internal log list of the IP console . To show the log list, click on “Event Log” on the “Maintenance” page, see section 3.7.2. Since the IP console's system memory is used to save all the information, the maximum number of possible log list entries is restricted to 1,000 events. Every entry that exceeds this limit overrides the oldest one, automatically.

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

- **NFS Logging enabled:** Define a NFS server, where a directory or a static link have to be exported, to write all logging data to a file that is located there. To write logging data from more than one IP console device to only one NFS share, you have to define a file name that is unique for each device. When you change the NFS settings and press the button “Apply,” the NFS share will be mounted immediately. That means, the NFS share and the NFS server must be filled with valid sources or you will get an error message.

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

- **SMTP Logging enabled:** With this option, the IP console is able to send Emails to an address given by the Email address text field in the Event Log Settings. These emails contain the same description strings as the internal log file and the mail subject is filled with the event group of the occurred log event. In order to use this log destination you have to specify a SMTP server, that has to be reachable from the IP console and that needs no authentication at all (<serverip>:<port>).
- **SNMP Logging enabled:** If this is activated, the IP console sends a SNMP trap to a specified destination IP address, every time a log event occurs. If the receiver requires a community string, you can set it in the appropriate text field. Most of the event traps only contain one descriptive string with all information about the log event. Only authentication and host power events have an own trap class that consists of several fields with detailed information about the occurred event. To receive these SNMP traps, any SNMP trap listener may be used.

Here is an example of all gerenated events and event group.

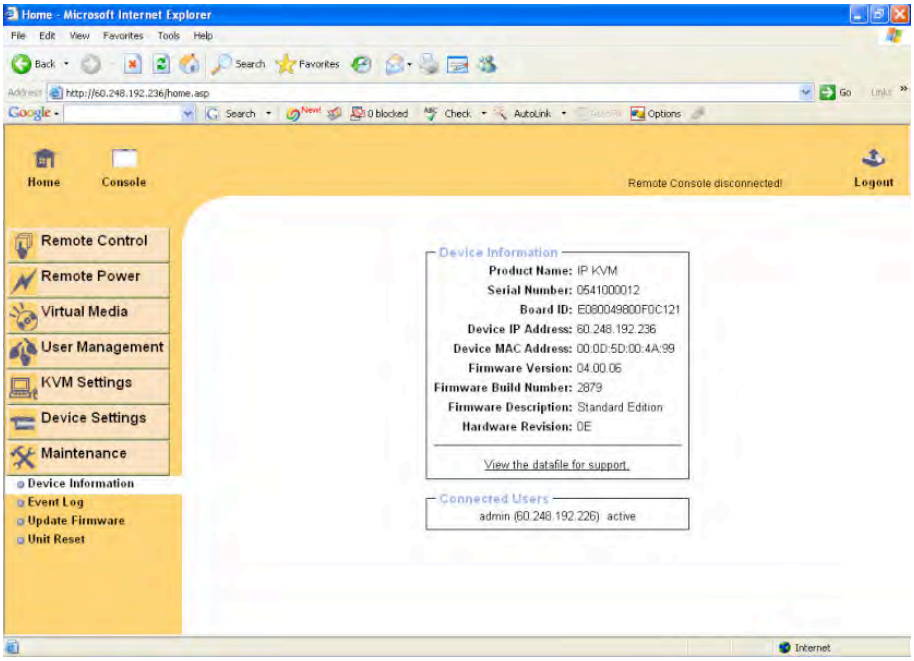
Device succesfully started	device
Board Reset performed by user...	device
Firmware upload failed	device
No firmware file uploaded	device
Uploaded firmware file discarded	device
Firmware validation failed	device
Firmware file uploaded by user	device
Firmware updated by user	device
Internal log file cleared by user	device
Security Violation	security
Host Power host	host
Host Reset host	host
Connection to Remote Console failed: reason	console (several)
Connection to client ... established	console
Connection to client ... closed	console
Login failed. auth	auth
Login succeed	auth

3.7 Maintenance

3.7.1 Device Information

This section contains a summary with various information about this IP console and its current firmware and allows you to reset the card.

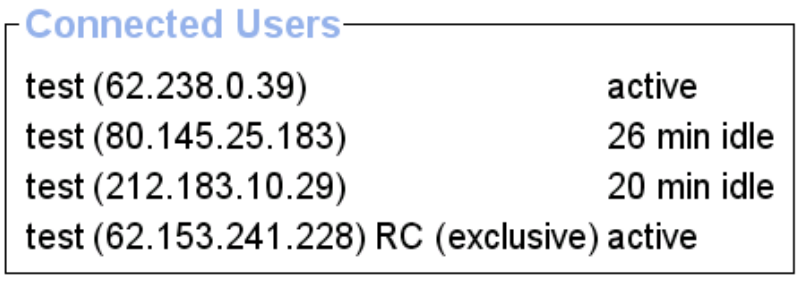
Device Information



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

Connected Users displays the IP console's activity. From left to right the connected user(s), its IP address (from which host the user comes from) and its activity status is displayed. RC means that the Remote Console is open. If the Remote Console is opened in exclusive mode the term (exclusive mode) is added. The last column contains either the term active for an active user or 30 min idle for an user who is inactive for a certain amount of time.

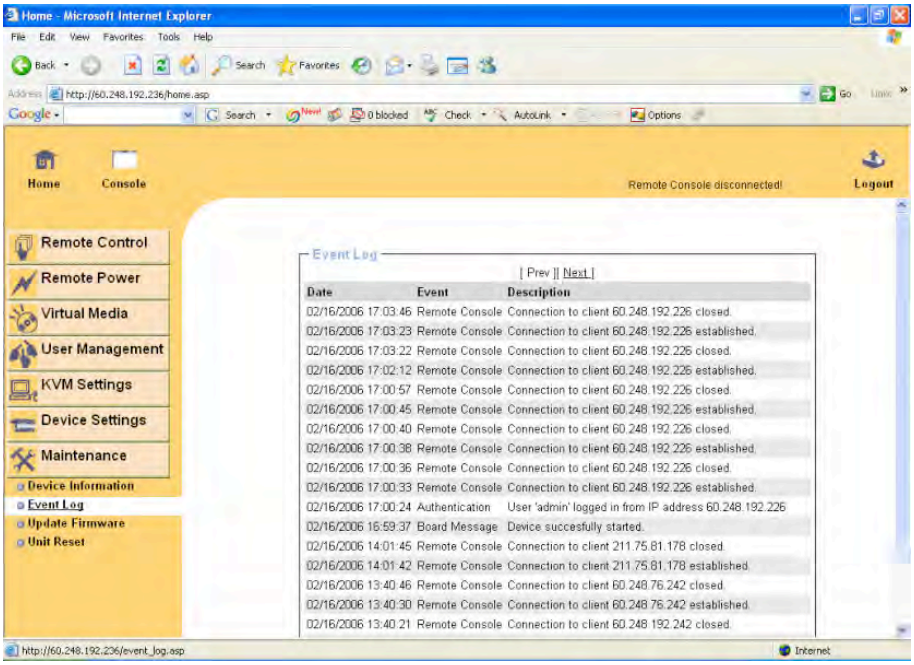
Connected Users



3.7.2 Event log

The Maintenance Event Log displays the list of events that are logged by the IP console.

Event Log List



3.7.3 Update Firmware

The IP console is a complete standalone computer. The software it runs is called firmware. The firmware of the IP console can be updated remotely in order to install new functionality or special features.

A new firmware update is a binary file which you can download from the CPI website:

http://www.chatsworth.com/Support-and-Downloads/Downloads/Software/.

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

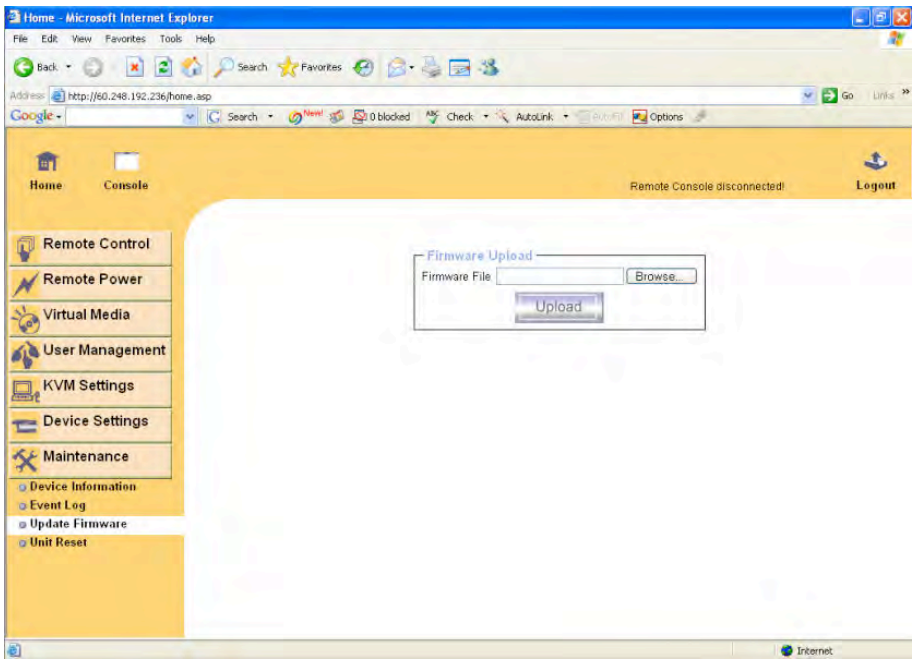
Before you can start updating the firmware of your IP console the new uncompressed firmware file has to be accessible on the system that you use for connecting to the IP console.

Updating the firmware is a three-stage process:

	**Warning!** Only experienced staff members or administrators should perform the firmware update.

1. The new firmware file is uploaded onto the IP console. In order to do that you need to select the file on your local system using the button “Browse” of the Upload Firmware panel. Once the firmware file has been uploaded, it is checked whether it is a valid firmware file and whether there were any transmission errors. In case of any error the Upload Firmware function will be aborted.

Update Firmware



2. If everything went well, you see the Update Firmware panel. The panel shows you the version number of the currently running firmware and the version number of the uploaded firmware. Pressing the button “Update” will store the new version and substitute the old one completely.

	**Warning!** This process is not reversible and might take some minutes. Make sure the IP console's power supply will not be interrupted during the update process, because this may cause an unusable card.

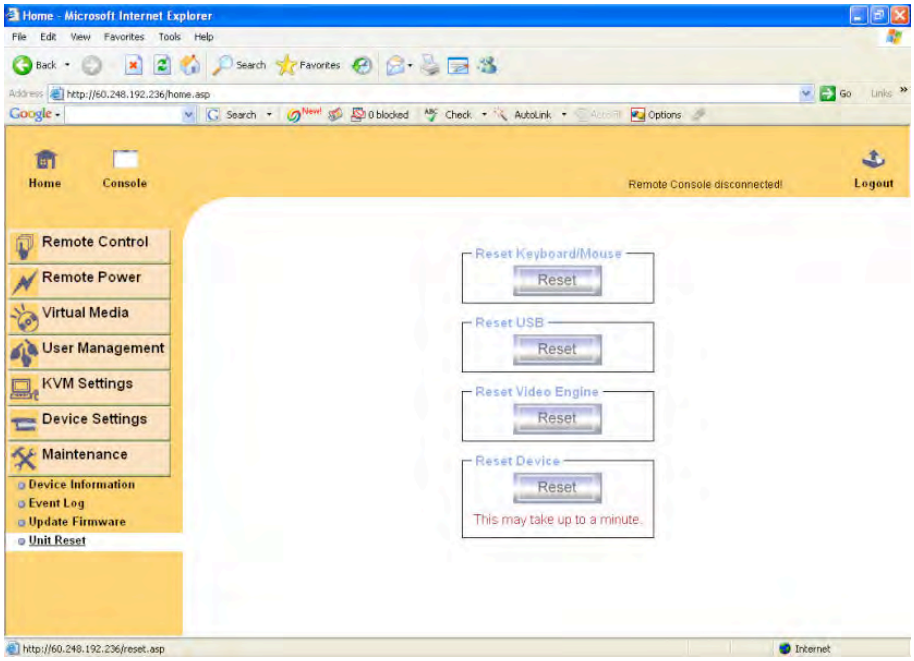
3. After the firmware has been stored, the panel will request you to reset the IP console manually, see section 3.7.4. Half a minute after the reset, the IP console will run with the new firmware version and should be accessible. However, you are requested to login once again.

3.7.4 Unit Reset

This section allows you to reset specific parts of the device. This involves the keyboard and mouse, the video engine and the IP console.

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

Unit Reset



Resetting the switch (Reset Device) 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 (Keyboard & Mouse, USB, Video Engine) will take some seconds only and does not result in closing connections.

Note: Only the super user is allowed to reset the IP console.

Troubleshooting guide

1. The remote mouse doesn't work or is not synchronous.

    - Make sure the mouse settings in IP console match the mouse model.
    - There are some circumstances where the mouse synchronization process could behave incorrectly, refer to section 3.5.2 Keyboard/Mouse under KVM Settings and section 2.4.1 Remote Console Control Bar under Usage for further explanation.

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

    - Try to correct the brightness and contrast settings until they are out of a range where the picture looks grainy. See section 3.5.3 Video under KVM Settings and section 2.4.1 Remote Console Control Bar under Usage for further explanation.
    - Use the auto adjustment feature to correct a flickering video.

3. Login on IP console fails.

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

4. The Remote Console window can't connect to IP console.

    - Possibly a firewall prevents access to the Remote Console. Make sure the TCP port numbers 443 or 80 are open for incoming TCP connection establishments.

5. No connection can be established to IP console.

    - Check whether the network connection is working in general (ping the IP address of IP console).
    - If not, check network hardware. Is IP console powered on? Check whether the IP address of IP console and all other IP related settings are correct.
    - Also verify that all the IP infrastructure of your LAN, like routers etc., is correctly configured. Without a ping functioning, IP console can't work either.

6. 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." Refer to Remote Console Button Keys under Section 3.5.1 User Console in KVM Settings.

7. In the browser the IP console pages are inconsistent or chaotic.

    - Make sure your browser cache settings are feasible. Especially make sure the cache settings are not set to something like ”never check for newer pages.” Otherwise IP console pages may be loaded from your browser cache and not from the card.

8. Windows XP doesn’t awake from standby mode.

    - This is possibly a Windows XP problem. Try not to move the mouse while XP goes in standby mode.

9. Can’t upload the signed certificate in MacOS X.

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

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

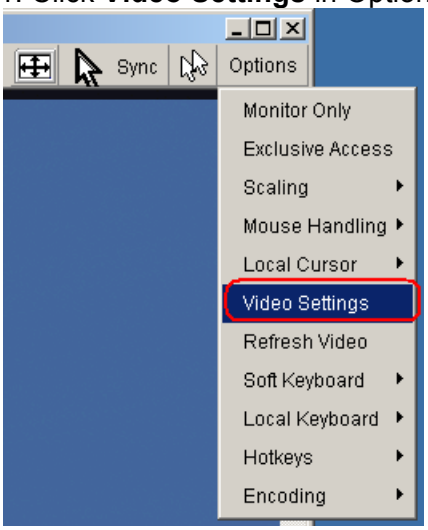
    - Please check if you have an option like ”Automatically move mouse pointer to the default button of dialog boxes” enabled in the mouse settings of the operating system. This option needs to be disabled.

FAQ

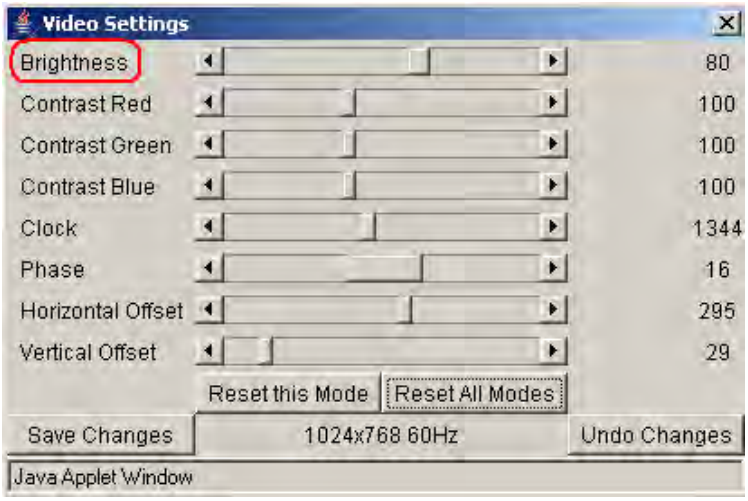
Q. The color of remote console displaying a pinkish tint.

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

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



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



Q. Is any software required on servers which connect to the IP KVM Switch through the IP console?

A. No, the IP console is a 100% hardware solution. No extra software required on servers.

Q. What operating systems does IP console support?

A. The IP console supports Windows 98, Windows ME, Windows 2000, Windows XP, Unix, Unix-like Operating System (Sun Solaris, Linux) and Mac OSX.

Q. Which browsers does the IP console support?

A. The IP console supports Microsoft Internet Explorer version 6.0 or higher, Netscape 7.0 and Mozilla 1.6.

Q. How many letters can the username and password be on the IP console?

A. The IP console accepts 32 letters of username and password.

Q. How many bits of connection encryption does IP console provide?

A. The IP console provides AES 256 bits connection encrypted.

Q. Local mouse and remote mouse didn't sync after doing mouse Intelligent Sync.

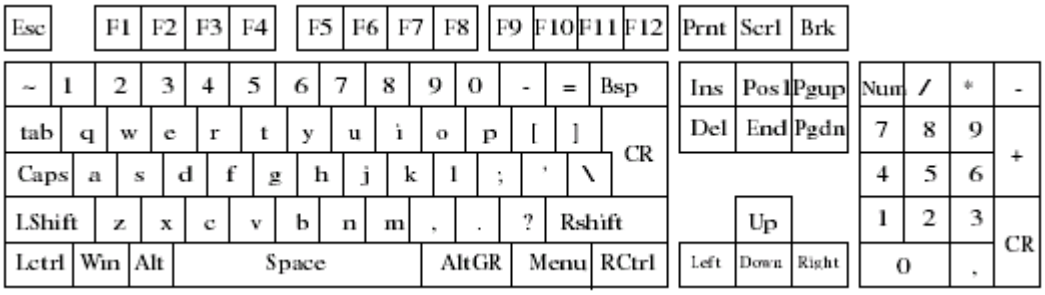
A. Make sure no windows are on the left-up corner of the remote console. Intelligent Sync has to re-calculate the coordinate of mouse from left-up corner on remote console.

Appendices

A. Key Codes

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

English (US) Keyboard Layout, used for key codes in table below.



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

B. User Role Permissions

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

Function	User	Administrator	Superuser
Remote Control: KVM	x	x	x
Remote Control: Telnet Console	x	x	x
Virtual Media	x	x	x
User Management: Change Password	x	x	x
User Management: Create Users	-	-	x
KVM Settings: User Console	x (w/o Misc.Settings)	x	x
KVM Settings: Keyboard/Mouse	-	x	x
KVM Settings: Video	-	x	x
Device Settings	-	-	x
Maintenance: Device Information	x	x	x
Maintenance: Event Log	-	-	x
Maintenance: Update Firmware	-	-	x
Maintenance: Unit Reset: Kb/Mse	x	x	x
Maintenance: Unit Reset, Video	x	x	x
Maintenance: Unit Reset, Device	-	-	x

C. IP Console Port Table

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

D. Bandwidth Consumption

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

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

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