



***freedom***

TM

# **freeView IP 100**

**Single Port KVM over IP SWITCH**

## **USER'S MANUAL**

Rev 1.4  
P/N: KVM-011A

## **Copyright and Trademark Information**

This document contains proprietary information that is protected by copyright. All rights reserved. No part of this document may be photocopied, reproduced, or translated into another language without express prior to written consent of freedom9 inc.

© Copyright 2005, freeView IP and the freedom9 company logo are trademarks or registered trademarks of freedom9 inc. All rights reserved. Sun and Java are trademarks or registered trademarks of Sun Microsystems, Inc. Internet Explorer, Windows Explorer, Windows, and HyperTerminal are trademarks or registered trademarks of Microsoft Corporation. Netscape and Netscape Navigator are trademarks or registered trademarks of Netscape Communication Corporation. Other trademarks or registered trademarks are the property of their respective holders.

## TABLE OF CONTENTS

|          |  |           |
|----------|--|-----------|
| <b>1</b> | <b>QUICK INSTALLATION GUIDE.....</b>                           | <b>3</b>  |
| 1.1      | INTRODUCTION.....  | 3         |
| 1.2      | HARDWARE INSTALLATION.....                                     | 3         |
| 1.3      | VIDEO MODES .....  | 3         |
| 1.4      | INITIAL IP CONFIGURATION.....                                  | 4         |
| 1.5      | WEB INTERFACE .....  | 5         |
| 1.6      | REMOTE CONSOLE.....  | 5         |
| <b>2</b> | <b>INTRODUCTION.....</b>                                       | <b>7</b>  |
| 2.1      | WHEN THE SERVER IS OPERATIONAL.....                            | 7         |
| 2.2      | WHEN THE SERVER IS NON-OPERATIONAL.....                        | 7         |
| 2.3      | FEATURES .....   | 8         |
| 2.4      | PACKAGE CONTENTS.....  | 8         |
| 2.5      | TECHNICAL SPECIFICATIONS .....                                 | 9         |
| 2.6      | SYSTEM REQUIREMENTS .....                                      | 9         |
| 2.7      | CABLE DIAGRAMS .....   | 10        |
| <b>3</b> | <b>HARDWARE INSTALLATION .....</b>                             | <b>11</b> |
| 3.1      | OPERATION OVERVIEW.....  | 11        |
| 3.2      | CONNECTING THE FREEVIEW IP 100 TO THE HOST SYSTEM.....         | 11        |
| 3.3      | ETHERNET CONNECTION .....                                      | 14        |
| 3.4      | CONNECTING THE FREEVIEW IP 100 TO A MULTI-PORT KVM SWITCH..... | 15        |
| 3.5      | CONNECTING THE EXTERNAL RESET/POWER OPTION.....                | 15        |
| <b>4</b> | <b>CONFIGURATION .....</b>                                     | <b>16</b> |
| 4.1      | INITIAL CONFIGURATION.....                                     | 16        |
| 4.2      | INITIAL CONFIGURATION VIA DHCP SERVER.....                     | 16        |
| 4.3      | FREEVIEW IP 100 SETUP PROGRAM .....                            | 16        |
| 4.4      | INITIAL CONFIGURATION VIA SERIAL CONSOLE .....                 | 17        |
| 4.5      | KEYBOARD, MOUSE AND VIDEO CONFIGURATION .....                  | 18        |
| <b>5</b> | <b>USAGE.....</b>  | <b>22</b> |
| 5.1      | PREREQUISITES .....  | 22        |
| 5.2      | HTTP/HTTPS.....  | 22        |
| 5.3      | LOGGING IN AND LOGGING OUT.....                                | 23        |
| 5.4      | THE REMOTE CONSOLE.....  | 25        |
| 5.5      | MAIN WINDOW .....  | 26        |

|           |   |           |
|-----------|---|-----------|
| <b>6</b>  | <b>MENU OPTIONS.....</b>                        | <b>35</b> |
| 6.1       | REMOTE CONTROL.....                             | 35        |
| 6.2       | VIRTUAL MEDIA.....                              | 37        |
| 6.3       | USER MANAGEMENT .....                           | 49        |
| 6.4       | KVM SETTINGS .....                              | 50        |
| 6.5       | DEVICE SETTINGS.....                            | 56        |
| 6.6       | MAINTENANCE .....                               | 68        |
| <b>7</b>  | <b>TROUBLESHOOTING.....</b>                     | <b>72</b> |
| 7.1       | CERTIFICATES.....                               | 73        |
| <b>A.</b> | <b>PIN ASSIGNMENTS .....</b>                    | <b>74</b> |
| <b>B.</b> | <b>KEY CODES .....</b>                          | <b>75</b> |
| <b>C.</b> | <b>VIDEO MODES .....</b>                        | <b>78</b> |
| <b>D.</b> | <b>RACK MOUNT KIT INSTALLATION DIAGRAM.....</b> | <b>78</b> |

## LIST OF FIGURES

|   |    |
|---|----|
| Figure 1-1: The Host and Console Connectors .....           | 5  |
| Figure 1-2: KVM Setup Program.....                          | 6  |
| Figure 1-3: Java Warning.....                               | 8  |
| Figure 1-4: Remote Console.....                             | 8  |
| Figure 3-1a: Single Server Usage Scenario .....             | 13 |
| Figure 3-1b: Multiple Server Usage Scenario.....            | 13 |
| Figure 4-1: Setup Utility.....                              | 19 |
| Figure 5-1: Encryption Key Length in Internet Explorer..... | 25 |
| Figure 5-2: Login Screen.....                               | 25 |
| Figure 5-3: Main Page.....                                  | 26 |
| Figure 5-4: Remote Console.....                             | 27 |
| Figure 5-5: Remote Console Control Bar.....                 | 28 |
| Figure 5-6: Remote Console Options Menu .....               | 29 |
| Figure 5-7: Remote Console Exclusive Mode.....              | 30 |
| Figure 5-8: Remote Console Options Menu – Scaling .....     | 30 |
| Figure 5-9: Remote Console Options Menu – Local Cursor..... | 31 |
| Figure 5-10: Video Settings Panel .....                     | 32 |
| Figure 5-11: Soft Keyboard .....                            | 33 |
| Figure 5-12: Soft Keyboard Mapping.....                     | 34 |
| Figure 5-13: Remote Console Confirmation Dialog.....        | 35 |
| Figure 5-14: Encoding.....                                  | 35 |
| Figure 5-15: Status Line.....                               | 36 |
| Figure 5-16: Bandwidth Usage.....                           | 36 |
| Figure 6-1: KVM Console.....                                | 37 |
| Figure 6-2: Telnet Console .....                            | 38 |
| Figure 6-3: Virtual Floppy Disk Screen .....                | 39 |
| Figure 6-4: Select Image File.....                          | 40 |
| Figure 6-5: Virtual CD-ROM Image Screen .....               | 41 |
| Figure 6-6: Select Windows Share .....                      | 41 |
| Figure 6-7: Windows Explorer Context Menu .....             | 42 |
| Figure 6-8: Share Configuration Dialog .....                | 42 |
| Figure 6-9: RawWrite for Windows Selection Dialog.....      | 44 |

|   |    |
|---|----|
| Figure 6-10: Nero Selection Dialog .....          | 45 |
| Figure 6-11: Drive Redirection Menu .....         | 45 |
| Figure 6-13: Create a New Device.....             | 48 |
| Figure 6-14: Device Configuration Dialog .....    | 48 |
| Figure 6-15: New Device Added .....               | 49 |
| Figure 6-16: Drive Redirection Setting.....       | 49 |
| Figure 6-17: Drive Redirection Dialog.....        | 49 |
| Figure 6-18: Drive Redirection Completed.....     | 50 |
| Figure 6-19: USB Mass Storage Option.....         | 50 |
| Figure 6-20: Set Password.....                    | 51 |
| Figure 6-21: Set User .....                       | 52 |
| Figure 6-22: User Console Settings (Part 1).....  | 53 |
| Figure 6-22: User Console Settings (Part 2).....  | 54 |
| Figure 6-23: Keyboard and Mouse Settings .....    | 56 |
| Figure 6-24: Video Settings.....                  | 57 |
| Figure 6-25: Network Settings .....               | 59 |
| Figure 6-26: Dynamic DNS .....                    | 60 |
| Figure 6-27: Dynamic DNS Scenario.....            | 61 |
| Figure 6-28: Device Security.....                 | 62 |
| Figure 6-29: Certificate Settings .....           | 63 |
| Figure 6-30: SSL Certificate Upload .....         | 64 |
| Figure 6-31: Serial Port .....                    | 65 |
| Figure 6-32: Date and Time .....                  | 67 |
| Figure 6-33: Event Log.....                       | 68 |
| Figure 6-34: Device Information.....              | 70 |
| Figure 6-35: Connected Users.....                 | 70 |
| Figure 6-36: Event Log List.....                  | 71 |
| Figure 6-37: Update Firmware .....                | 71 |
| Figure 6-38: Unit Reset.....                      | 73 |
| Figure B-1: English (US) Keyboard Layout.....     | 78 |
| Figure D-1: Rack Mount Installation Diagram ..... | 79 |

# 1 QUICK INSTALLATION GUIDE

## 1.1 Introduction

The freeView IP 100 redirects local keyboard, mouse and video data to a remote administration console. All data is transmitted via internet protocol (IP). The unit can also be used in a multi administrator and multi server environment. In addition, the unit is a KVM switch, which can also be used with a local console (a local set of monitor, keyboard, and mouse).

## 1.2 Hardware Installation

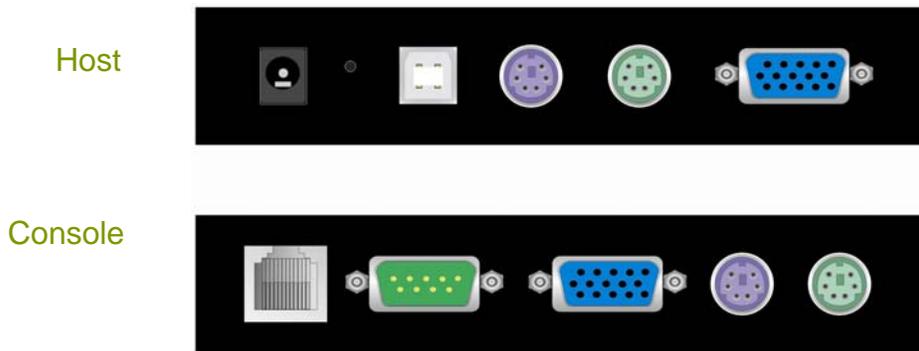


Figure 1-1: The Host and Console Connectors

1. Power off the server.
2. Remove the unit from the box.
3. Connect the included KVM cable from the server to the ports labeled Host on the unit. (Check that the keyboard and mouse connectors are connected to the proper ports and are not crossed.)
4. If a local console is being used, connect the local monitor, mouse, and keyboard to the ports labeled Console on the unit.
5. If a remote mass storage device is being used, connect the included USB cable from the server to the USB port on the unit.
6. Connect an Ethernet cable to the LAN port and/or modem to RS-232 serial port, depending on how the unit will be accessed.
7. Power on the unit.
8. Power on the server.

## 1.3 Video Modes

The freeView IP 100 supports many common video modes. Please refer to Appendix C for a list of all supported video modes.

## 1.4 Initial IP Configuration

By default, the freeView IP 100 uses the network parameters shown in Table 1-1.

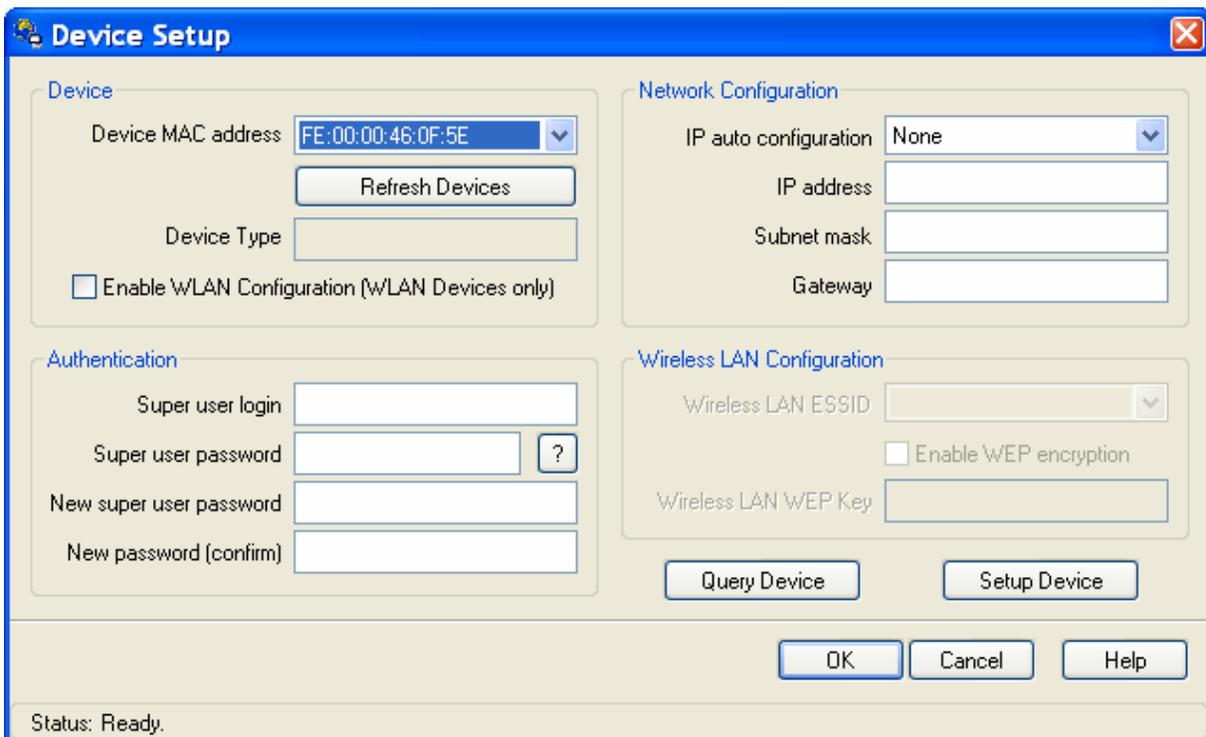
| Parameter             | Value         |
|-----------------------|---------------|
| IP auto configuration | Static        |
| IP-Address            | 192.168.1.22  |
| Net-mask              | 255.255.255.0 |
| Default-Gateway       | None          |

**Table 1-1: Default network configuration**

If these network parameters do not match the network configuration, the device's network settings can be configured using the program KVMSetup.exe located on the installation CD after the unit has been connected to the network and powered on.

To change the network settings of the device:

1. Open Windows Explorer and browse to the CD drive.
2. Double-click the file KVMSetup.exe.
3. A screen similar to Figure 1-2 will be displayed.



**Figure 1-2: KVM Setup Program**

4. Select the unit's MAC address from the drop-down list under "Device MAC address".
5. Enter the desired IP address for the device under "Network Configuration".

6. Enter the user name and password under "Authentication". The default user name is "super" and the default password is "pass".
7. Click "Setup Device".

## 1.5 Web Interface

Once the device has been configured to match the network setup, log in to the web interface using a Java enabled web browser. Once the web browser is running, enter "http://<device IP address>" in the browser window (e.g. if the device's IP address is 192.168.1.22, type "http://192.168.1.22" in the browser window).

The default user name and password to log into the device are shown below.

|           |       |
|-----------|-------|
| User name | super |
| Password  | pass  |

It is recommended that the default password be changed immediately to prevent unauthorized access to the device.

## 1.6 Remote Console

The Remote Console is the redirected screen, keyboard and mouse of the remote host system to which the freeView IP 100 is connected. The web browser which is used to access the unit has to have Java Runtime Environment version 1.1 or higher installed. However, it is strongly recommended that the Sun JVM 1.4 is installed.

To access the remote console of the host, click the Console icon on the top-left corner of the screen. There may be a slight delay as the Java virtual applet is being loaded. If the screen shown in Figure 1-3 appears, click "Yes".



**Figure 1-3: Java Warning**

Figure 1-4 shows the top of the Remote Console window.



**Figure 1-4: Remote Console**

Once connected, the following can be performed to improve the user experience:

**Auto Adjust button** 

If the video displayed is distorted, click this button and the device will automatically adjust its display to improve the quality.

**Sync Mouse button** 

Choose this option in order to synchronize the local with the remote mouse cursor. This is only required if using Double Mouse mode. It is recommended that mouse acceleration is turned off on the host device.

## 2 Introduction

Thank you for purchasing the freeView IP 100. The freeView IP 100 saves money, time, space, equipment and power. The freeView IP 100 defines a new class of remote KVM access devices, it combines digital remote KVM access via IP networks with comprehensive and integrated system management.

The device provides convenient, remote KVM access and control via LAN or Internet. It captures, digitizes, and compresses the video signal and transmits it with keyboard and mouse signals to and from a remote computer. The freeView IP 100 provides a non-intrusive solution for remote access and control. Remote access and control software runs on the embedded processor only and not on the mission-critical servers, so that there is no impact on server or network performance.

Furthermore, the freeView IP 100 offers additional remote power management when used with an optional IP Power device.

The device supports consoles consisting of a PS/2 keyboard and mouse and HDDDB 15 video output and will automatically detect the current video mode of the console. The freeView IP 100 will accept video streams up to 110 MHz. This results in a screen resolution of 1280x1024 pixels with a frame rate of 60 Hz.

### 2.1 When The Server Is Operational

The freeView IP 100 gives you full control over the remote server. The Management Console allows you to access the remote server's graphics, keyboard and mouse and the ability to send special commands to the server. You can also perform periodic maintenance on the server. Using the Remote Console, you can do the following:

- A. Reboot the system.
- B. Monitor the boot process.
- C. Boot to a different operating system on dual-boot machines.
- D. Boot up in Windows Safe Mode.
- E. Boot the system from a separate partition to load diagnostic environment.
- F. Run special diagnostic programs.

### 2.2 When The Server Is Non-Operational

Using the freeView IP 100, the system administrator can discover problems with the server, though fixing hardware problems is not possible through a remote management device. Nevertheless, the device gives the administrator valuable information about the type of hardware failure. Serious hardware failures can be categorized into five different categories, with the percentage chance of failure listed below:

- A. Hard disk failure 50%

- B. Power cable detached, power supply failure 28%
- C. CPU, Controller, main board failure 10%
- D. CPU fan failure 8%
- E. RAM failure 4%

Using the freeView IP 100, administrators can determine which kind of serious hardware failure has occurred (See table 2-1).

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

**Table 2-1 Host System Failures and Detection Methods**

## 2.3 Features

- Manage servers around the world from your desk
- KVM (keyboard, video, mouse) access over IP and analog telephone line (modem required)
- BIOS level access
- SSL encryption
- No impact on server or network performance
- High-performance mouse tracking and synchronization
- Port to connect a user console for direct analog access to KVM switch
- Local Mouse suppression (only when using Sun's Java Virtual Machine)
- Can be used with any standard KVM
- Remote mass storage control

## 2.4 Package Contents

|   |       |
|---|-------|
| freeView IP 100                                 | 1 PC  |
| Quick Install Guide                             | 1 PC  |
| Installation software and User Manual on CD-ROM | 1 PC  |
| AC to DC Power Adapter                          | 1 PC  |
| Rack mount Kit                                  | 1 SET |

|                         |      |
|-------------------------|------|
| Null modem cable        | 1 PC |
| USB A to B 6 feet cable | 1 PC |
| 3-in-1 3 feet KVM cable | 1 PC |

## 2.5 Technical Specifications

| Model No.                                    | freeView IP 100   |
|--|---|
| PC Port                                      | 1   |
| Console Port                                 | 1   |
| PC Port Connector<br>(All Female Types)      | PS/2 Keyboard Mini Din 6 pin<br>PS/2 Mouse Mini Din 6 pin<br>VGA HDDB 15 pin<br>USB Type B receptacle |
| Console Port Connector<br>(All Female Types) | PS/2 Keyboard Mini Din 6 pin<br>PS/2 Mouse Mini Din 6 pin<br>VGA HDDB 15pin                           |
| Remote Console Connector                     | RJ-45 8P8C  |
| Serial Port (DB9 pin Male)                   | 1   |
| LAN port (RJ-45 8P8C)                        | 1 x 10BASE-T Ethernet<br>1 x 100BASE-T Ethernet   |
| Reset button                                 | 1   |
| Keyboard Emulation                           | PS/2  |
| Mouse Emulation                              | PS/2  |
| VGA Resolution                               | Local: 1600X1200 Remote: 1280X1024  |
| Housing                                      | Metal   |
| Power Adapter                                | DC 5V, 2.5A   |
| Operation Temperature                        | 0 ~ 5°C   |
| Storage Temperature                          | -20 ~ 60°C  |
| Humidity                                     | 0 ~ 80%, Non-Condensing   |
| Size   | Desktop   |
| Weight (kg)                                  | 1700g   |
| Dimension (mm)                               | 156 X139 X 27   |

## 2.6 System Requirements

| Item                | Description  |
|---------------------|--|
| Local console side  | One PS/2 Keyboard, one PS/2 Mouse and one monitor          |
| Remote Console side | One PC or Multiple PCs are linked into the network         |
| Host side           | One PC or Server or the console port of another KVM switch |

## 2.7 Cable Diagrams

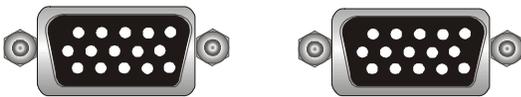
### PS/2 Cable:

Mini Din 6 pin Male to Male



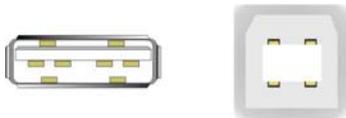
### VGA Cable:

HDB15 pin Male to Male



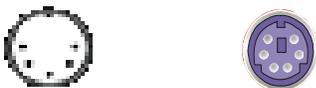
### USB 2.0 Cable:

USB A-B cable



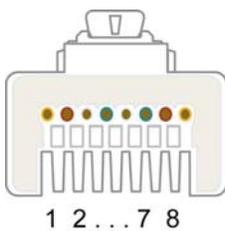
### AT to PS/2 keyboard adapter: (Optional)

Din 5 pins Male to Mini Din 6 pin Female



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

8P8C



### 3 Hardware Installation

#### 3.1 Operation Overview

Figure 3-1 shows some examples of how to connect the freeView IP 100 to the local area network.



Figure 3-1a: Single Server Usage Scenario

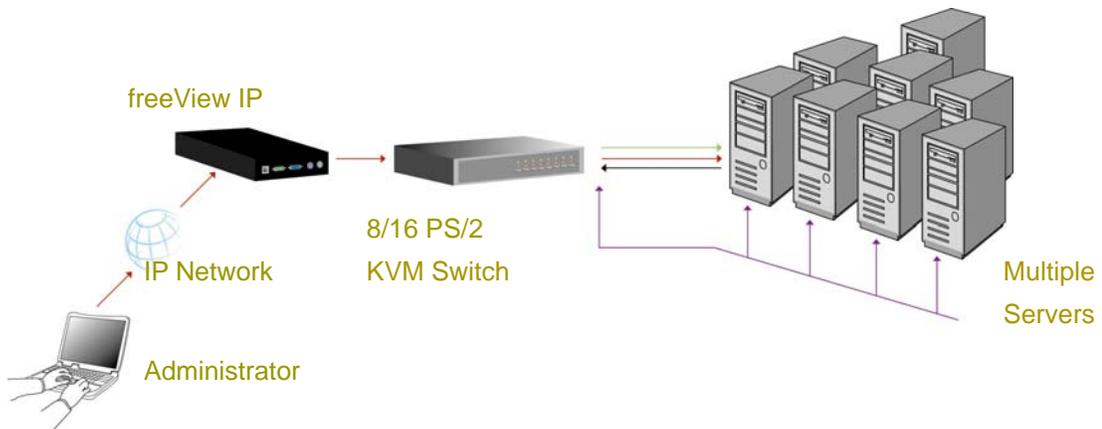


Figure 3-1b: Multiple Server Usage Scenario

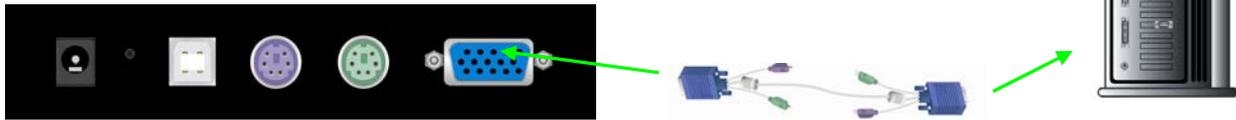
The freeView IP 100 can be used in a multi-administrator, multi-server environment. Attaching one or several units to a matrix KVM switch allows multiple users to access multiple servers using the remote console.

#### 3.2 Connecting The freeView IP 100 To The Host System

In order to connect the device to the host system, perform the following steps:

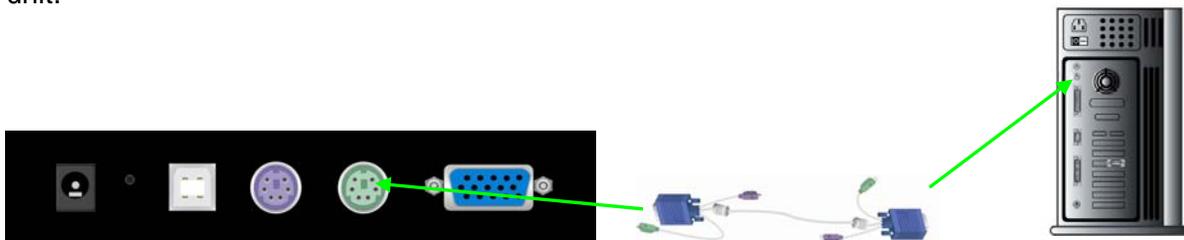
##### Step 1

Connect the VGA cable on one end a KVM cable to the monitor port on the host system and the VGA cable on the other end of the cable to the monitor port on the host side of the unit.



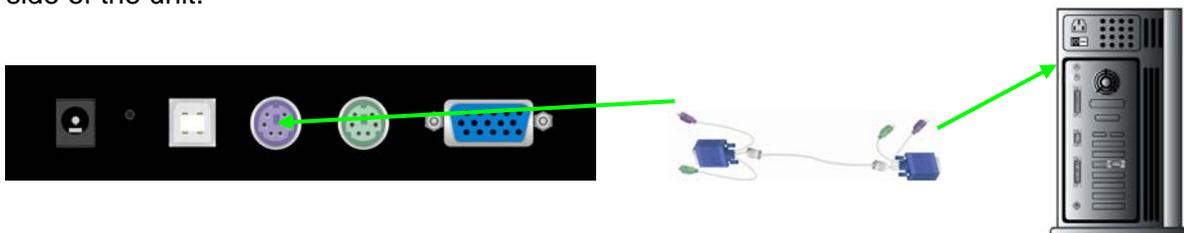
### Step 2

Connect the green PS/2 plug on one end of a KVM cable to the mouse port on the host system and the green PS/2 plug on the other end of the cable to the mouse port on the host side of the unit.



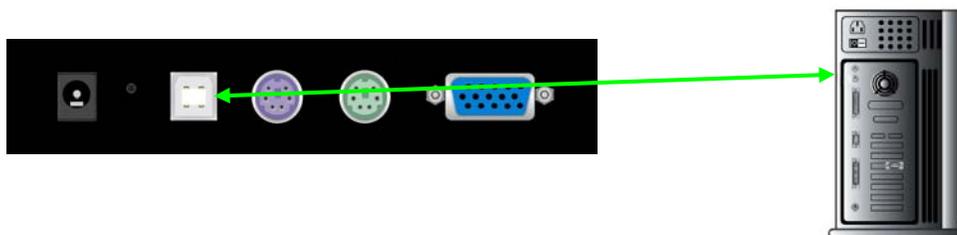
### Step 3

Connect the purple PS/2 plug on one end of a KVM cable to the keyboard port on the host system and the purple PS/2 plug on the other end of the cable to the keyboard port on the host side of the unit.



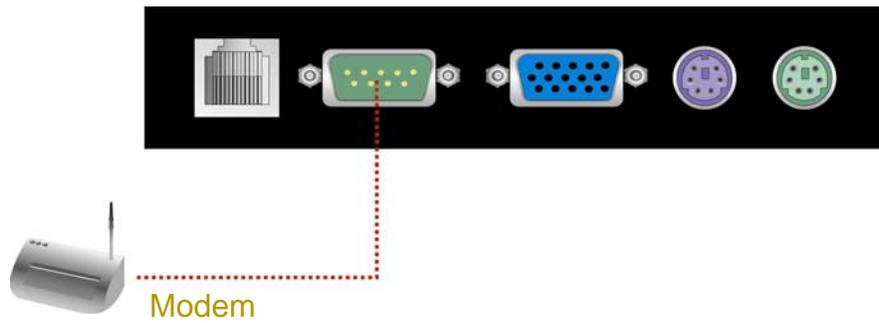
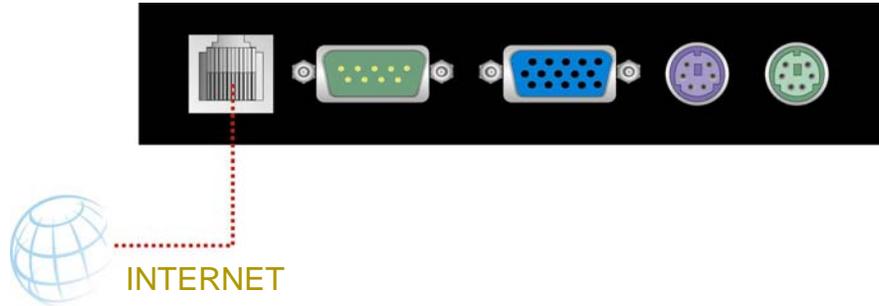
### Step 4 (Only required if using Virtual Media)

Connect the type A connector of a USB A-B cable to the USB port on the host system and the type B connector to the unit.



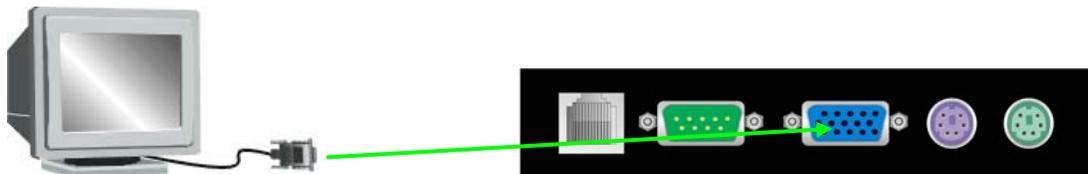
### Step 5

Connect an Ethernet cable to the Ethernet port on the unit and/or connect a modem to the DB-9 port on the unit, depending on how the KVM is accessed remotely.



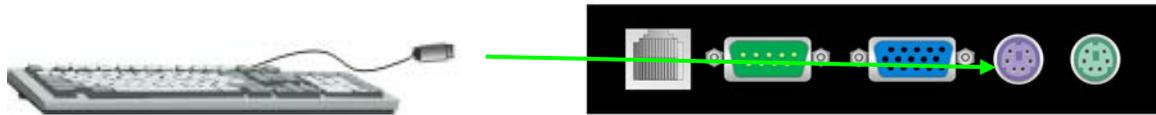
### Step 6 (Only required if using a local console)

Connect the monitor to the monitor port on the console side.



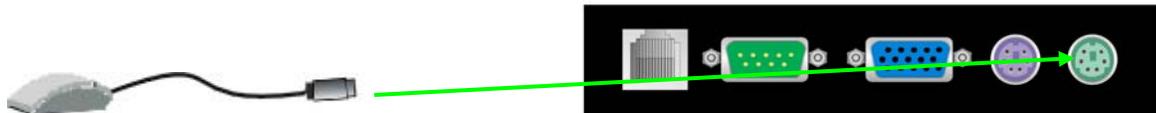
### Step 7 (Only required if using a local console)

Connect the keyboard to the PS/2 port marked as keyboard on the console side.



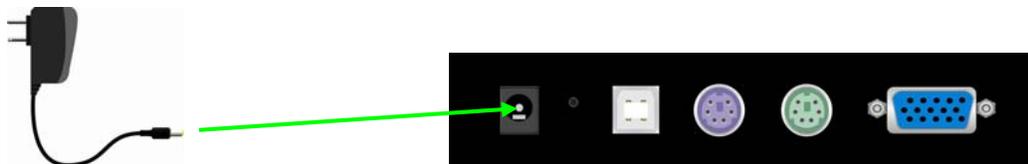
### Step 8 (Only required if using a local console)

Connect the mouse to the PS/2 port marked as mouse on the console side.



### Step 9

Connect the power supply on to the freeView IP 100.



## 3.3 Ethernet Connection

The rear side of the freeView IP 100 provides a RJ-45 connector for a 10/100 Mbps Ethernet connection.

### Using a 10 Mbps Connection

For 10BASE-T Ethernet networks, the Ethernet adapter uses Category 3, 4, 5 or 6 UTP cable. To establish a 10 Mbps connection, the cable must be connected to a 10BASE-T hub.

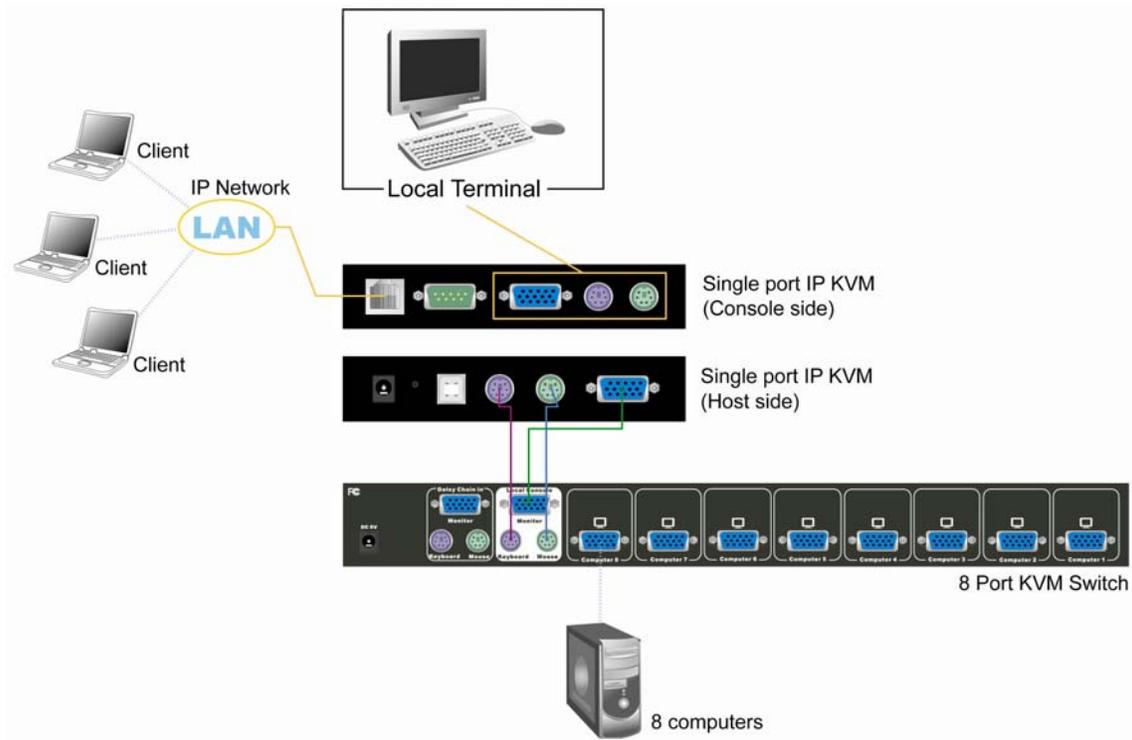
- Make sure that the cable is wired appropriately for a standard 10BASE-T adapter.
- Align the RJ-45 plug with the notch on the adapter's connector and insert it into the adapter's connector.

### Using a 100 Mbps Connection

For 100BASE-TX Fast Ethernet networks, the freeView IP 100 supports Category 5 or higher UTP cabling. To establish a 100 Mbps connection, the cable must be connected to a 100BASE-TX hub or switch.

- Make sure that the cable is wired appropriately for a standard 100BASE-TX adapter.
- Align the RJ-45 plug with the notch on the adapter's connector and insert it into the adapter's connector.

### 3.4 Connecting The freeView IP 100 To A Multi-Port KVM Switch



### 3.5 Connecting The External Reset/Power Option

Refer to the manual of the IP Power or Serial over IP device for instructions on connecting them to the serial interface on the rear of the freeView IP 100.

## 4 Configuration

### 4.1 Initial Configuration

The freeView IP 100 is shipped with the network configuration listed in Table 4-1.

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

**Table 4-1: Initial Network Configuration**

**Note:** If the freeView IP 100 cannot find a DHCP server on startup, it will not have an IP address.

The following describes the initial IP configuration that is necessary to access the unit for the first time. **Note:** Before installation, make a note of the MAC address of the unit before installing the device, it is located on the label on the bottom of the unit.

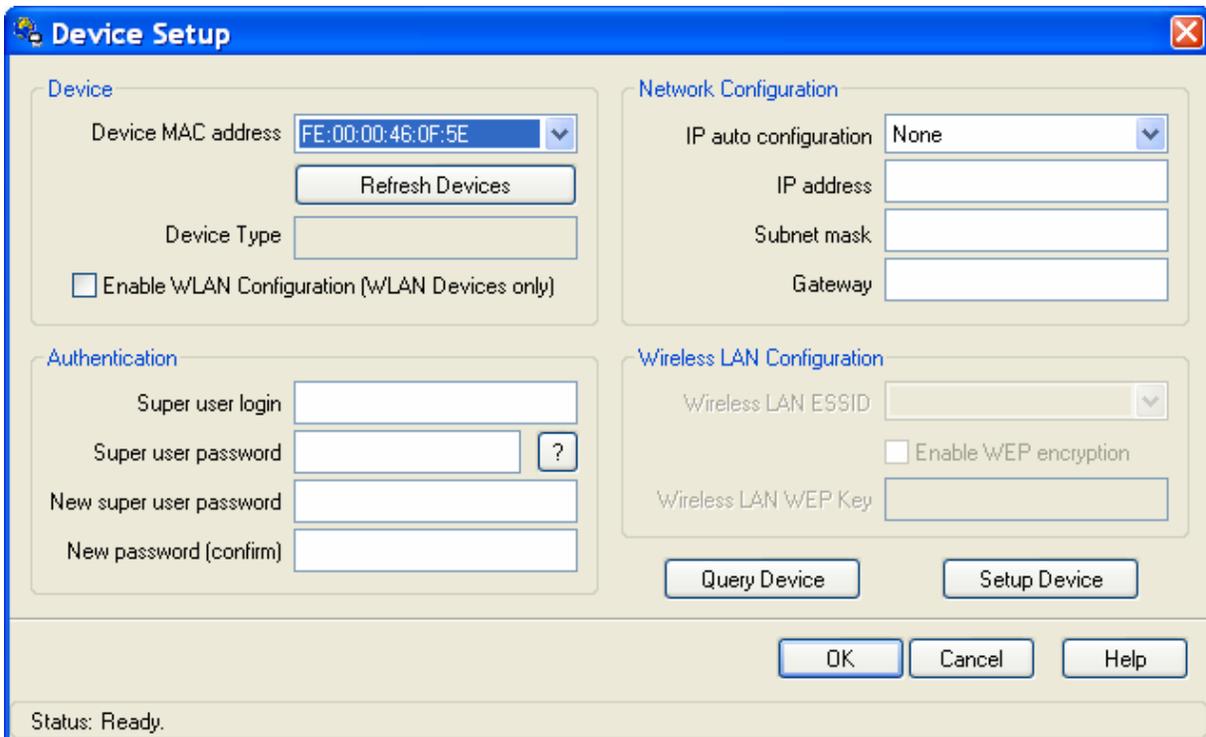
### 4.2 Initial Configuration Via DHCP Server

By default, the freeView IP 100 will attempt to obtain an IP address from a DHCP server on the network. To determine the IP address obtained via DHCP, either check the list of assigned IP addresses on the DHCP server and find the IP address assigned to the MAC address of the unit, or set the DHCP server to assign a fixed IP address to the MAC address of the device. Consult the manual for the DHCP server for detailed configuration instructions.

Alternatively, the setup tool KVMSSetup.exe found on the Installation Disk accompanying the product can also be used to set up the unit.

### 4.3 freeView IP 100 Setup Program

Connect the freeView IP 100 to a computer via local network or USB. Start the setup tool KVMSSetup.exe located on the Installation Disk on the computer. The program screen is shown in Figure 4-1.



**Figure 4-1: Setup Utility**

On the upper left corner, the MAC address(es) of all freeView IP 100 switches are displayed. To rescan for devices, click “Refresh Devices”.

1. Select the MAC address of the unit to be configured from the dropdown list.
2. Click “Query Device” to populate the current configuration of the device.
3. Enter the network configuration settings in the Network Configuration screen.
4. Enter the username and password of the device in the Authentication screen. The default username is “super” and the default password is “pass”.
5. If desired, enter a new password for the super user. **Note:** Write down the new password and keep it in a safe, secure location for later reference.
6. Click “Setup Device” to save the new settings.
7. Click “OK” to close the window.

#### 4.4 Initial Configuration Via Serial Console

Connect a null modem cable from a serial port on a computer to the RS-232 port on the console side of the freeView IP 100. Open up a terminal access program (e.g. HyperTerminal) to access the device. The unit uses the terminal parameters shown in Table 4-2.

| Parameter   | Value  |
|-------------|--------|
| Bits/second | 115200 |
| Data bits   | 8      |

|              |      |
|--------------|------|
| Parity       | No   |
| Stop bits    | 1    |
| Flow Control | None |

**Table 4-2: Serial line parameters**

1. Power off the unit.
2. Power on the unit and immediately press the <ESC> key.
3. After the boot up sequence is completed, a “=>” prompt will appear.
4. Type “config” and press the <Enter> key and wait for the configuration questions to appear.
5. For each question, type in the desired settings, or press <Enter> to accept the default value shown in square parenthesis [ ].
6. The parameters that can be set are as follows:

**IP auto configuration (none/dhcp/bootp) [dhcp]:**

With this option, the user can specify whether the freeView IP 100 gets its network settings from a DHCP or BOOTP server. For DHCP, enter “dhcp”, and for BOOTP enter “bootp”. If neither option is selected, the IP auto configuration is disabled and the network settings will need to be configured manually.

**IP [192.168.1.22]:**

The IP address of the unit. This option is only applied if IP auto configuration is set to none.

**Net mask [255.255.255.0]:**

The subnet mask of the unit. This option is only applied if IP auto configuration is set to none.

**Gateway (0.0.0.0 for none) [0.0.0.0]:**

The IP address of the default gateway of the device. If a default gateway is not available, enter 0.0.0.0. This option is only applied if IP auto configuration is set to none.

**4.5 Keyboard, Mouse And Video Configuration**

The freeView IP 100 can be connected to the host machine’s peripheral ports via PS/2 or USB. The correct operation of the remote mouse depends on several settings which will be discussed in the following subsections.

**4.5.1 freeView IP 100 Keyboard Settings**

The freeView IP 100’s settings for the host keyboard type have to be correct in order for the remote keyboard to work properly. See Section 6.4.2 for details.

## 4.5.2 Remote Mouse Settings

A common problem with KVM devices is the synchronization between the local and remote mouse cursors. The freeView IP 100 addresses this problem with an intelligent synchronization algorithm. There are two mouse modes available on the freeView IP 100:

### Auto mouse speed

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

### Fixed mouse speed

This mode translates the mouse movements from the Remote Console in a way that one pixel move will lead to a fixed number of pixel moves on the remote system. The number of pixels can be adjusted using the scaling feature. It should be noted that this will only work when mouse acceleration is turned off on the remote system.

## 4.5.3 Auto Mouse Speed And Mouse Synchronization

The automatic mouse mode performs the speed detection during mouse synchronization. If the local mouse loses synchronization with the remote mouse, there are two methods for re-synchronizing local and remote mouse:

### Fast Sync

Fast synchronization is used to correct a temporary, but fixed skew. Choose this option using the Remote Console options menu or press the mouse synchronization hotkey sequence if it has been defined.

### Intelligent Sync

If fast synchronization does not work or the mouse settings have been changed on the host system, use intelligent resynchronization. This method takes more time than the fast synchronization and can be accessed in the Remote Console option menu. Intelligent synchronization requires the picture be adjusted correctly. Use the auto adjustment function or the manual correction in the Video Settings panel to configure the picture. The Sync Mouse button at the top of the Remote Console behaves differently, depending on the current state of mouse synchronization. Pressing this button will perform a fast sync, except when the KVM port or the video mode have been changed, in which case an intelligent sync will be performed.

**Note:** When using the console for the first time, press the Auto Adjust Button if the local mouse pointer is not synchronized with the remote mouse pointer.

#### **4.5.4 Host System Mouse Settings**

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

Note that the following limitations do not apply if the Mouse Type is set to USB and "MS Windows 2000 and newer".

While the freeView IP 100 works with accelerated mice and is able to synchronize the local with the remote mouse pointer, there are limitations which may prevent this synchronization from working properly:

##### **Special Mouse Driver**

There are mouse drivers which influence the synchronization process and lead to desynchronized mouse pointers. If this occurs, disable the vendor-specific mouse driver on the host system.

##### **Windows XP Mouse Settings**

Windows XP has a setting called "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, use a wallpaper instead. Alternatively, Active Desktop can be disabled altogether.

Move the mouse pointer to the upper left corner of the applet screen and move it back and forth slightly to resynchronize the mouse. If resynchronizing fails, disable mouse acceleration and repeat the procedure.

#### **4.5.5 Single And Double Mouse Mode**

The information above applies to the Double Mouse Mode, where both the remote and local mouse pointers are visible and need to be synchronized. The freeView IP 100 also supports a Single Mouse Mode, where only the remote mouse pointer is visible. Enable this mode in the open Remote Console and click in the window area to activate it. The local mouse pointer will be hidden and the remote mouse pointer can be controlled directly. To leave this mode, it is necessary to define a mouse hotkey in the Remote Console Settings Panel. Press this key to free the captured local mouse pointer.

#### **4.5.6 Recommended Mouse Settings**

The following are suggestions for mouse modes for various operating systems:

### **MS Windows 2000/2003 (Professional and Server), XP**

It is recommended to use the USB mouse option. Choose USB without Mouse Sync. For a PS/2 mouse choose Auto Mouse Speed. For XP disable the “enhance pointer precision” option 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, use Single Mouse Mode.

### **MAC OS X**

It is recommended that the Single Mouse Mode be used.

## **4.5.7 Video Modes**

The freeView IP 100 supports most common video modes. When running X11 on the host system, do not use any custom mode lines with special video modes, otherwise, the device may not be able to detect the video mode. It is recommended that a standard VESA video mode is used instead.

## 5 Usage

### 5.1 Prerequisites

The freeView IP 100 features an embedded operating system and applications offering a variety of standardized interfaces. This chapter will describe both these interfaces, and how to use them in detail. The interfaces are accessed using the TCP/IP protocol, thus they can be accessed through the Ethernet interface.

### 5.2 HTTP/HTTPS

Full access is provided by the embedded web server. The freeView IP 100 can be managed using a standard web browser. The web interface can be accessed using the insecure HTTP protocol, or the encrypted HTTPS protocol. Whenever possible, use HTTPS for increased security.

#### Telnet

A standard Telnet client can be used to access an arbitrary device connected to the freeView IP 100's serial port via a terminal mode.

The primary interface of the freeView IP 100 is the HTTP interface. This is covered extensively in this chapter. Other interfaces are addressed in subtopics.

In order to use the Remote Console window of the managed host system, the browser has to support Java Runtime Environment (JRE) version 1.1 or higher. If the browser does not have Java support (such as on a PDA), the web interface can be accessed and configured, but the remote console will be unavailable.

**Important:** It is recommended that the latest version of Sun's JVM is installed.

For an insecure (HTTP) connection to the device, the following browsers are recommended:

- Microsoft Internet Explorer version 6.0 or higher on Windows 98, Windows ME, Windows 2000 and Windows XP
- Netscape Navigator 7.0 or Mozilla 1.6 on Windows 98, Windows ME, Windows 2000, Windows XP, Linux and other UNIX-like Operating Systems

In order to access the remote host system using a securely encrypted connection, a browser that supports the HTTPS protocol is required. Strong security is only assured by using a key length of 128-bit. Some older browsers do not support 128-bit encryption.

Using the Internet Explorer, the current key length supported can be found under "Help", "About Internet Explorer". The dialog box contains a link that leads to information on how to upgrade the

browser to a state of the art encryption scheme. Figure 5-1 shows the dialog box presented by the Internet Explorer 6.0.



**Figure 5-1: Encryption Key Length in Internet Explorer**

Newer web browsers support strong encryption by default.

## **5.3 Logging In And Logging Out**

### **5.3.1 Logging In**

Launch the web browser and enter the address of the freeView IP 100 in the Address Bar. The address used can be an IP address or a host and domain name, in the case where the DNS server has a symbolic name. For example, type the following in the address line of the web browser when establishing an unsecured connection:

**http://<IP address of freeView IP 100>**

When using a secure connection, type in:

**https://<IP address of freeView IP 100>**

The login page will be displayed (Figure 5-2).



**Figure 5-2: Login Screen**

The device has a built-in super user that has full access to the device. The default username and password for the super user are show in Table 5-1.

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

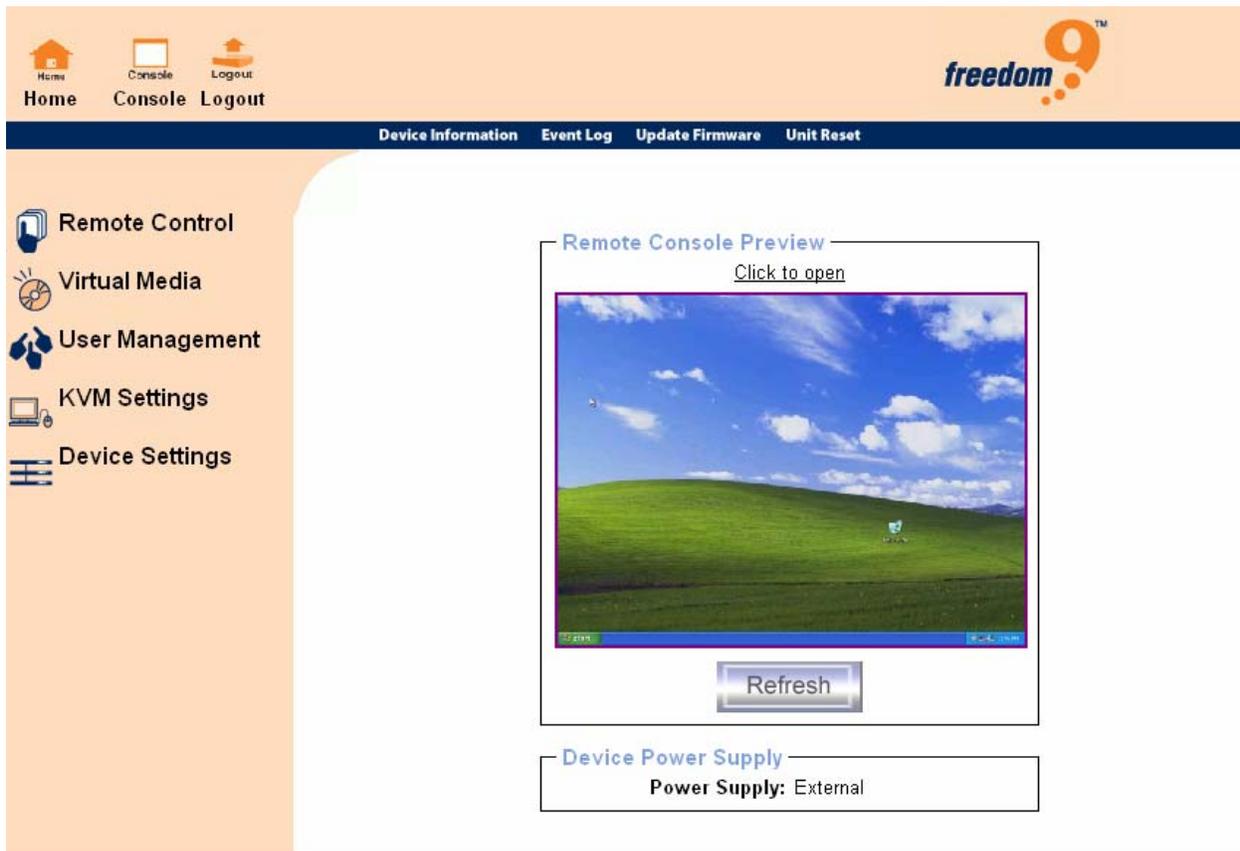
**Table 5-1: Default User Settings**

**Note:** The super user cannot access the device via the serial interface.

**Note:** Change the super user password as soon as possible. Failure to do so will pose a severe security risk and will allow unauthorized users to access the device.

## Navigation

After logging into the freeView IP 100, the main page shown in Figure 5-3 will be displayed. This page consists of three parts: the buttons on the upper side allow the user to navigate within the web interface (see Table 5-2 for details). The lower left frame contains a navigation bar which allows the user to switch between the different sections of the unit. The lower right frame displays details of the menu item selected on the left frame.



**Figure 5-3: Main Page**

|   |   |
|---|---|
|  | Return to the main page of the freeView IP 100. |
|  | Show the remote console.                        |
|  | Log out of the web interface.                   |

**Table 5-2 Web Interface Icons**

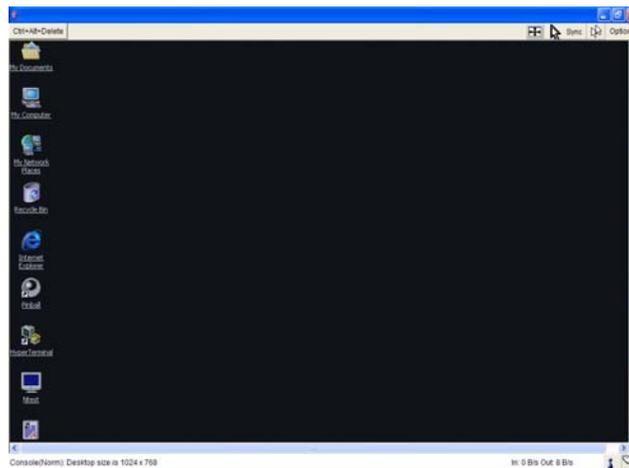
### 5.3.2 Logging Out

To log out of the web interface, click the Logout button on the main window. The user will also be logged out automatically after 30 minutes of inactivity.

## 5.4 The Remote Console

### General description

The Remote Console is the redirected screen, keyboard and mouse of the remote host system connected to the freeView IP 100.



**Figure 5-4: Remote Console**

The Remote Console window is a Java Applet that establishes its own connection to the freeView IP 100. The protocol used by the Remote Console is RFB (Remote Frame Buffer Protocol). Currently, RFB uses port number 443 to establish a connection. For proper operation, ensure that the local network environment allows traffic on port 443.

**Note:** If the freeView IP 100 is connected to the Internet through a proxy server without NAT, the Remote Console will not be available from the WAN interface because web proxies are not able to relay the RFB packets.

In case of problems, consult the network administrator for proper network configuration.

## 5.5 Main Window

Starting the Remote Console will open another additional window which displays the screen content of the host system. The Remote Console will behave the same as if it was being used locally, including the keyboard and mouse. However, the reaction time for the keyboard and mouse will have a slight delay. The severity of the delay depends on the bandwidth available to access the unit. Also, special keyboard combinations (e.g. Ctrl-Alt-Del in Windows) will affect the local system and not the remote system. See the next section for more details.

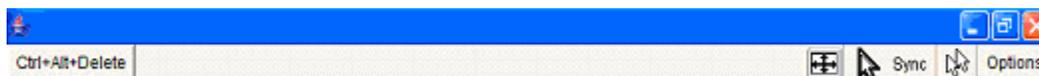
**Note:** If a keyboard whose language is different from the host system's default language is used (e.g. a US English local keyboard is used to control a remote host running a German operating system), the local language will be used instead of the remote language. In the previous example, US characters will be sent to the host instead of German characters. To emulate the remote host language, select the appropriate language using the Local Keyboard option in the dropdown menu. See the next section for more details.

The Remote Console window will automatically adjust to fit the size of the remote screen. However, the Remote Console window can be resized manually in the local window system the same way as other applications.

**Note:** The Remote Console window must be selected in the local operating system in order for mouse and keyboard input to be sent to the remote host.

### 5.5.1 Remote Console Control Bar

The top bar of the Remote Console window shown in Figure 5-5 contains the control bar. The control bar displays the state of the remote device and also allows the user to change the Remote Console settings.



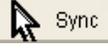
**Figure 5-5: Remote Console Control Bar**

**Ctrl+Alt+Delete** 

This button sends the key combination “Control-Alt-Delete” to the remote system (see Section 6 for instructions on defining new key combination buttons).

**Auto Adjust button** 

If the video display becomes distorted, click this button and wait a few seconds while the device tries to automatically readjust the video settings.

**Sync mouse button** 

This button activates the mouse synchronization process. Choose this option 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. This button is only available when using double mouse mode.

**Single/Double Mouse Mode** 

This button switches between Single Mouse Mode (only the remote mouse pointer is visible) and Double Mouse Mode (both remote and local mouse pointers are visible and need to be synchronized). Single mouse mode is only available if using SUN JVM 1.3 or higher.

**Options** 

This button opens the Options menu



**Figure 5-6: Remote Console Options Menu**

A short description of the options follows.

### Monitor Only

Toggles Monitor Only mode on and off. If Monitor Only is enabled, remote console interaction is disabled and only monitoring is possible.

### Exclusive Access

Toggles Exclusive Access mode if the user has the appropriate access level. When Exclusive Access is enabled, other users cannot open the Remote Console until the current user disables Exclusive Access or logs off the system.

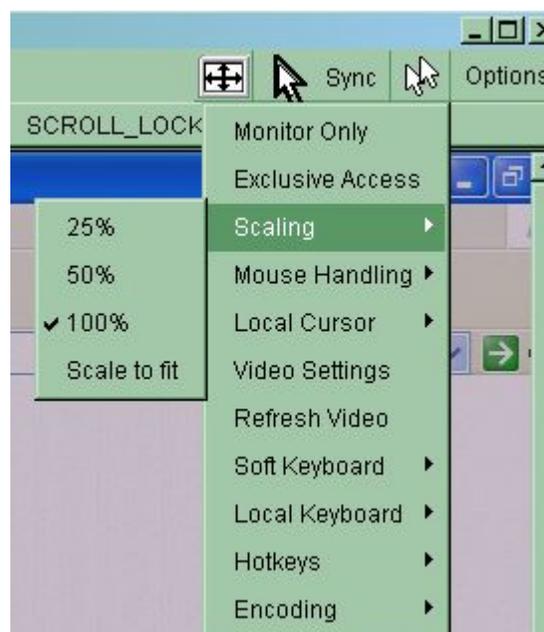
A change in access mode is also visible in the status line (Figure 5-7).



**Figure 5-7: Remote Console Exclusive Mode**

### Scaling

Allows the user to scale down the display of the Remote Console. The user can still use both the mouse and the keyboard, however the scaling algorithm may distort some items on the display.



**Figure 5-8: Remote Console Options Menu – Scaling**

## Mouse Handling

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

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

**Intelligent Sync:** Use this option if fast sync does not work or if the mouse settings have been changed on the host system. **Note:** Intelligent Sync takes more time than Fast Sync. Use the auto adjustment function or manual correction in the Video Settings panel to setup the picture.

## Local Cursor

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



Figure 5-9: Remote Console Options Menu – Local Cursor

## Video Settings

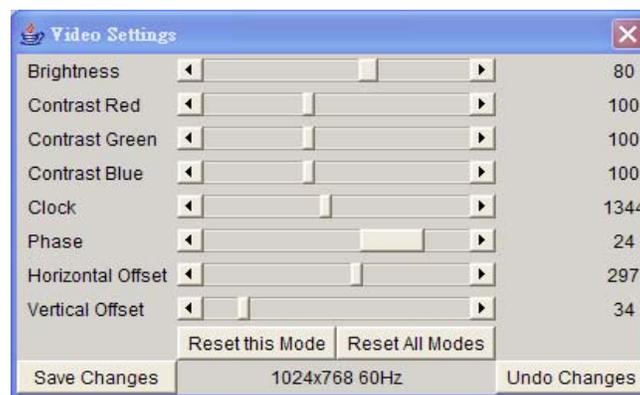
This option opens a panel for changing the video settings for the freeView IP 100. The unit features two different dialogs, which influence the video settings:

## Video Settings Through The Web Interface

This option enables the local video port. This option determines whether or not the video output from the host is transmitted to the local monitor.

The Noise Filter option defines how the freeView IP 100 reacts to small changes in the video input signal. A large filter setting uses less network traffic and leads to a faster video display, but small changes in the display may not be recognized and updated on the remote immediately. A small filter setting displays all changes on the remote host instantly but will produce more network traffic (depending on the quality of the video input signal). The default setting should be suitable for most situations.

## Video Settings Through The Remote Console



**Figure 5-10: 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. The default settings in conjunction with the auto adjustment procedure should be adequate for common configurations. If the picture quality is still poor after auto adjustment, change this setting together with the sampling phase to achieve a better quality.

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

**Horizontal Position:** Adjusts the horizontal position of the screen.

**Vertical Position:** Adjusts the vertical position of the screen.

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

**Reset all Modes:** Reset all modes to the factory-made defaults.

**Save Changes:** Save changes permanently.

**Undo Changes:** Restore last saved settings.

### Soft Keyboard



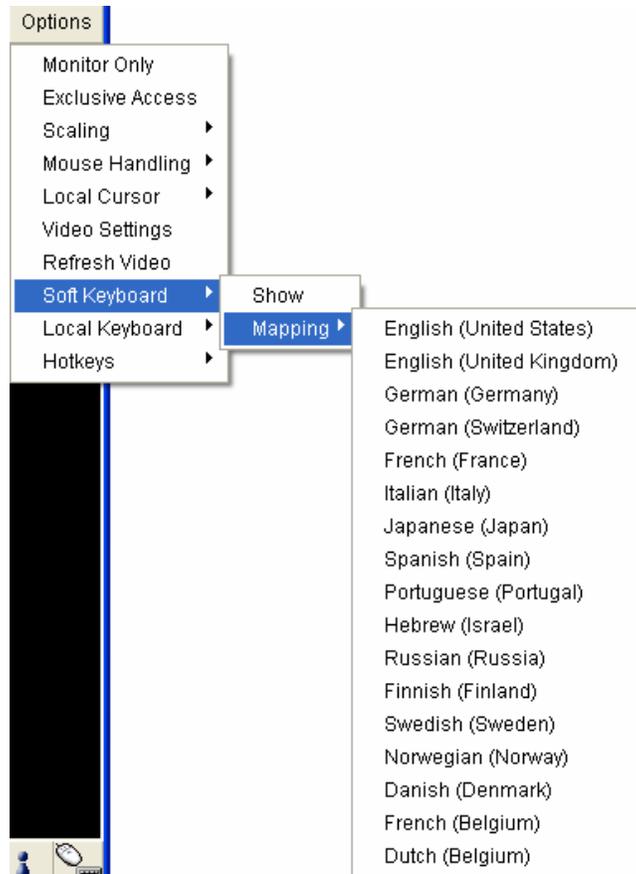
**Figure 5-11: Soft Keyboard**

- **Show**

Opens the Soft-Keyboard screen (Figure 5-11). The Soft-Keyboard is necessary in the case where the host system uses a completely different language and country mapping from the administration machine.

- **Mapping**

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



**Figure 5-12: Soft Keyboard Mapping**

- **Local Keyboard**

Used to change the language mapping of the Remote Console Applet. Under normal circumstances, the applet automatically determines the appropriate value. However, the applet may not determine the correct value depending on the particular JVM and the browser settings. A typical example is a German localized system that uses an US-English keyboard mapping. In this case the Local Keyboard will need to be changed to the correct setting manually.

- **Hotkeys**

Opens a list of defined hotkeys. By choose an entry, the selected command will be sent to the host system.

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

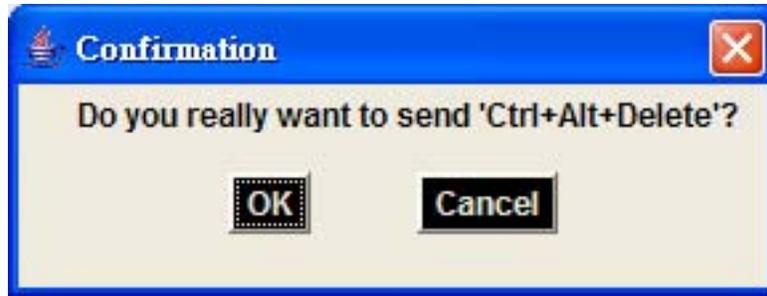


Figure 5-13: Remote Console Confirmation Dialog

## Encoding

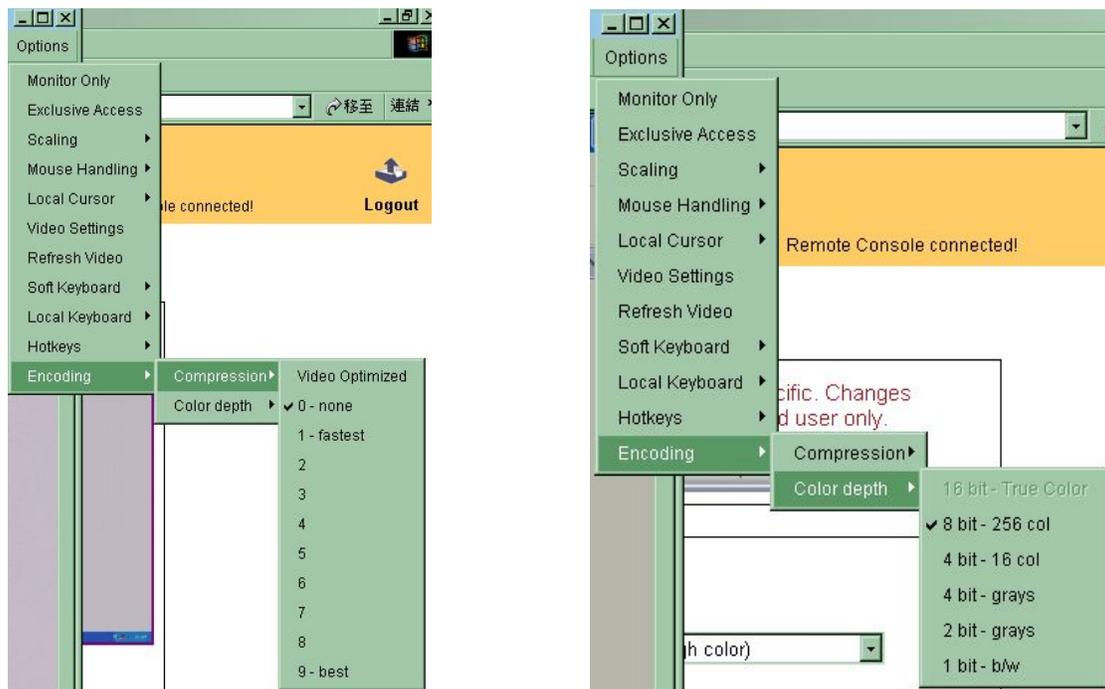


Figure 5-14: Encoding

Allows the user to adjust both the compression rate and the colour depth individually. Depending on the selected compression rate, the data stream between the freeView IP 100 and the Remote Console will be compressed in order to save bandwidth. Increasing the compression rate requires more resources from the freeView IP 100, thus should not be used when multiple users are accessing the remote console simultaneously.

The default color depth is 16 Bit (65536 colors). The other color depths are intended for slower network connections since they require less bandwidth. 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-quality 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.

## 5.5.2 Remote Console Status Line

### Status line

The status line shows both the console and the connection state. The size of the remote screen is displayed as well. Figure 5-15 shows a Remote Console with a resolution of 1024x768 pixels. The value in brackets describes the connection to the Remote Console. “Norm” indicates a standard connection without encryption, “SSL” indicates a secure connection.



**Figure 5-15: 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.



**Figure 5-16: Bandwidth Usage**

For more information about Monitor Only and Exclusive Access settings, see the next section.

## 6 Menu Options

### 6.1 Remote Control

The Remote Control menu allows the user to access the host system via web interface or Telnet.

#### 6.1.1 KVM Console

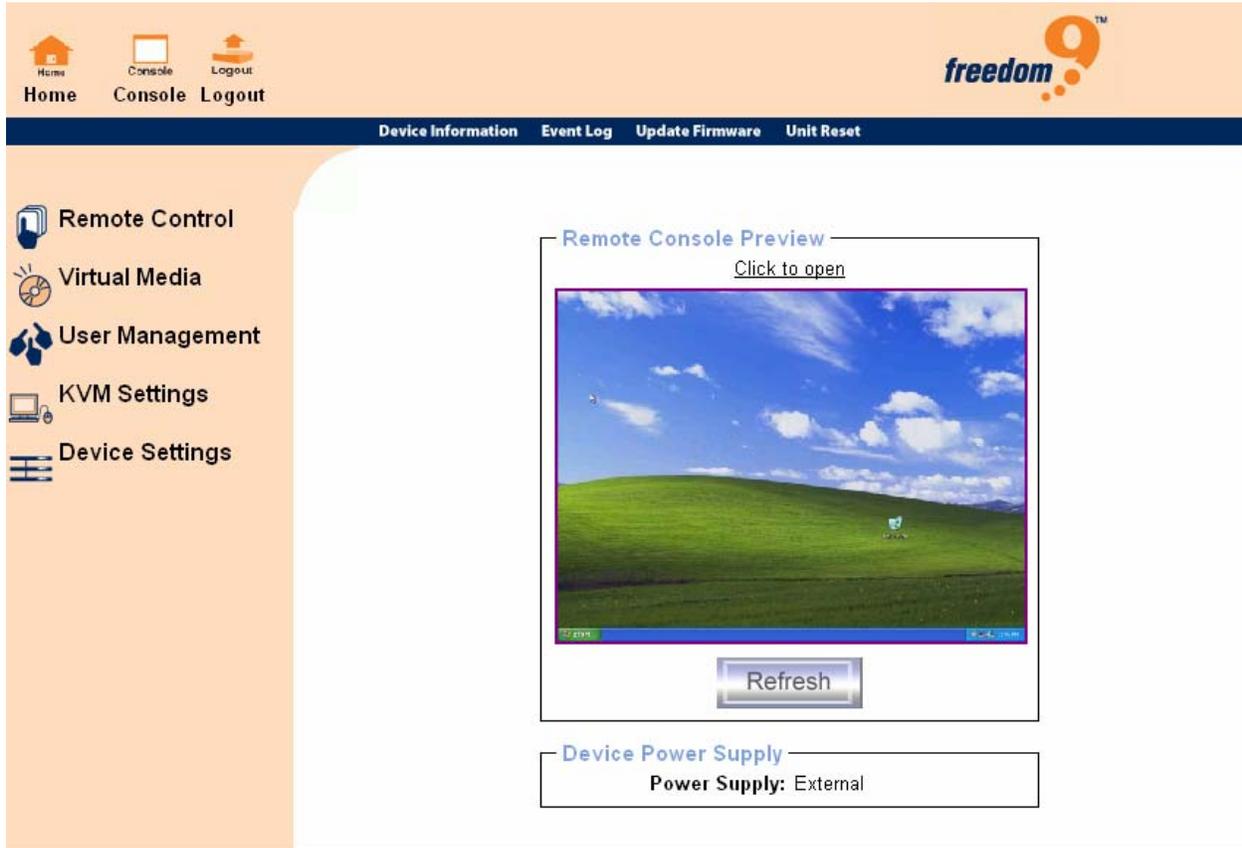
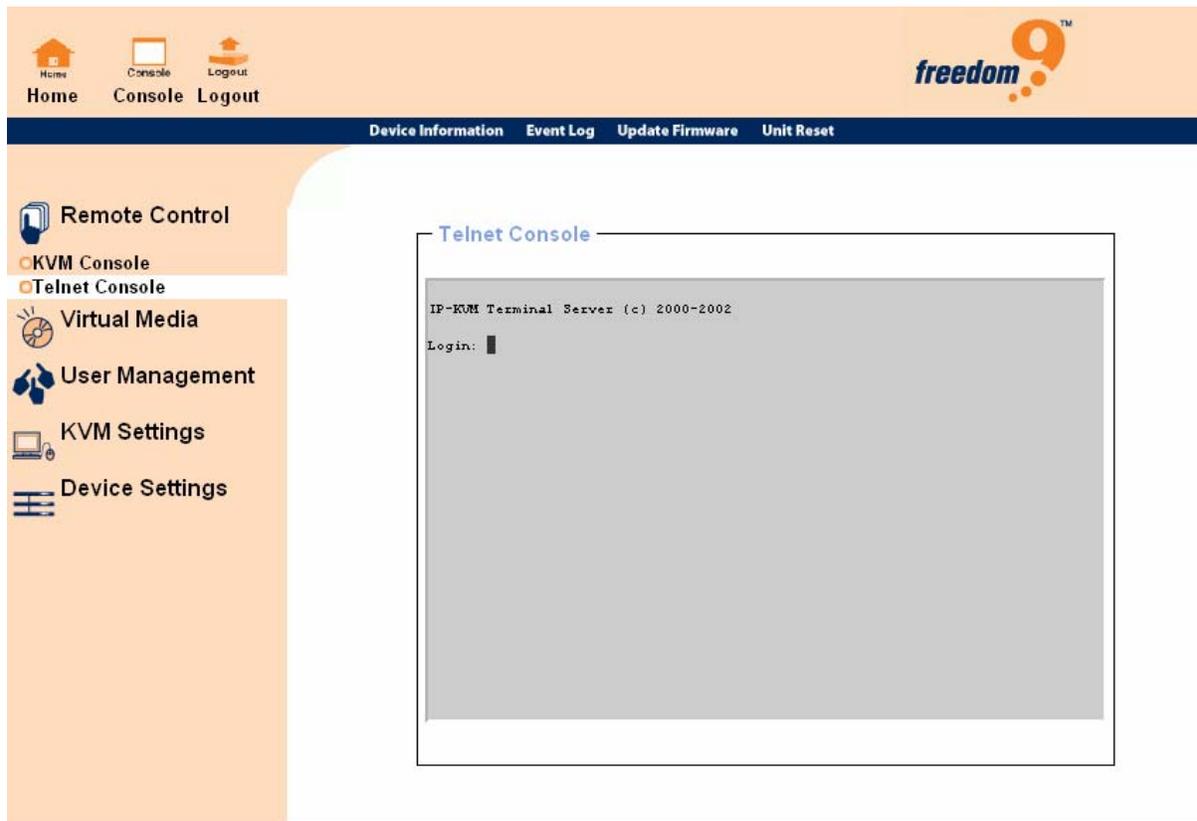


Figure 6-1: KVM Console

There are several methods to open the Remote Console window: click the Console icon on the top bar, click the menu entry KVM Console on the left menu bar, or click on the console picture on the right. To refresh the static picture of the remote host screen, click on the “Refresh” button.

## 6.1.2 Telnet Console



**Figure 6-2: Telnet Console**

The freeView IP 100 features a Telnet server that enables the user to connect to the host via a standard Telnet client. If the Telnet program uses a VT100, VT102 or VT220 terminal emulation (or a similar emulation), it is possible to perform a console redirection as long as the host machine is using a text based operating system (e.g. Unix).

Connecting to the freeView IP 100 requires a telnet client on the local machine. To access the device, run the telnet program and specify the IP address of the unit. For example, if the unit's IP address is 192.168.1.22, type in "telnet 192.168.1.22" in Unix or Windows. Once connected, the user will be prompted for username and password. The credentials for authentication are identical to those of the web interface.

Once the user has successfully logged into the device, a command line will be presented and the user can enter management commands.

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 device parameters. In terminal mode the connection is made from the local machine to the device connected to the serial port on the unit (if the serial settings are set correctly). All user input on the local machine are redirected to the device connected to the serial port and the response is displayed on the Telnet interface.

The following list shows the commands available in mode command and their usage.

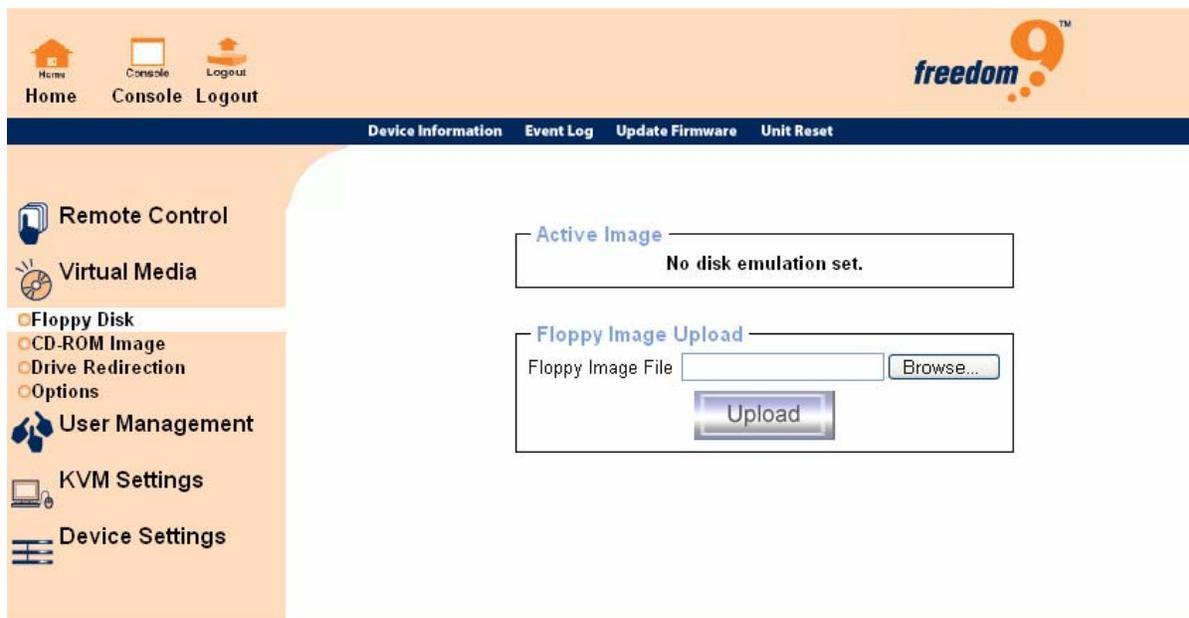
| Command  | Description   |
|----------|---|
| help     | Displays the list of available commands   |
| cls      | Clears the screen   |
| quit     | Exits the current session and disconnects from the client   |
| version  | Displays the release information  |
| terminal | Starts the terminal passthrough mode for the serial port. The key sequence “esc exit” switches back to the command mode. The command has an optional parameter (1 or 2) to select the desired serial port for passthrough access (only number 1 is supported at this time). |

**Table 6-1: Telnet Commands**

## 6.2 Virtual Media

The Virtual Media menu allows the user to set up virtual media devices. Virtual media allows the user to access floppy drives, CD-ROMs, or external drives on the host machine from the client, and vice versa.

### 6.2.1 Floppy Disk

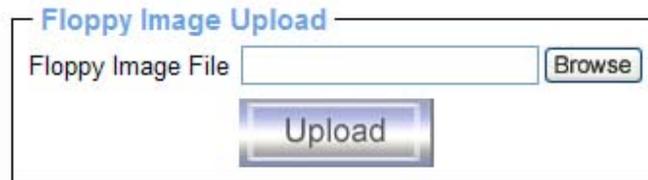


**Figure 6-3: Virtual Floppy Disk Screen**

#### Upload a Floppy Image

To upload a floppy image to the freeView IP 100 from the local client for use on the host machine, follow these steps:

- Create an image of the floppy disk. See the next section for instructions on creating a floppy disk image.
- Type in the path of the image in the web interface. The path can be entered manually, or can be browsed by using the “Browse...” button on the interface.



**Figure 6-4: Select Image File**

- The maximum image size is 1.44MB. To use a larger image, mount this image via a Windows Share (SAMBA) (see the next Section titled “Use Image on Windows Share (SAMBA) for details”).
- Click on the “Upload” button to initiate the transfer of the selected image file to the freeView IP 100’s onboard memory. This image file is kept in the onboard memory of the device until the end of the current session, until the user logs out, or when the device is rebooted.

## **6.2.2 CD-ROM Image**

### **Use Image on Windows Share (SAMBA)**

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

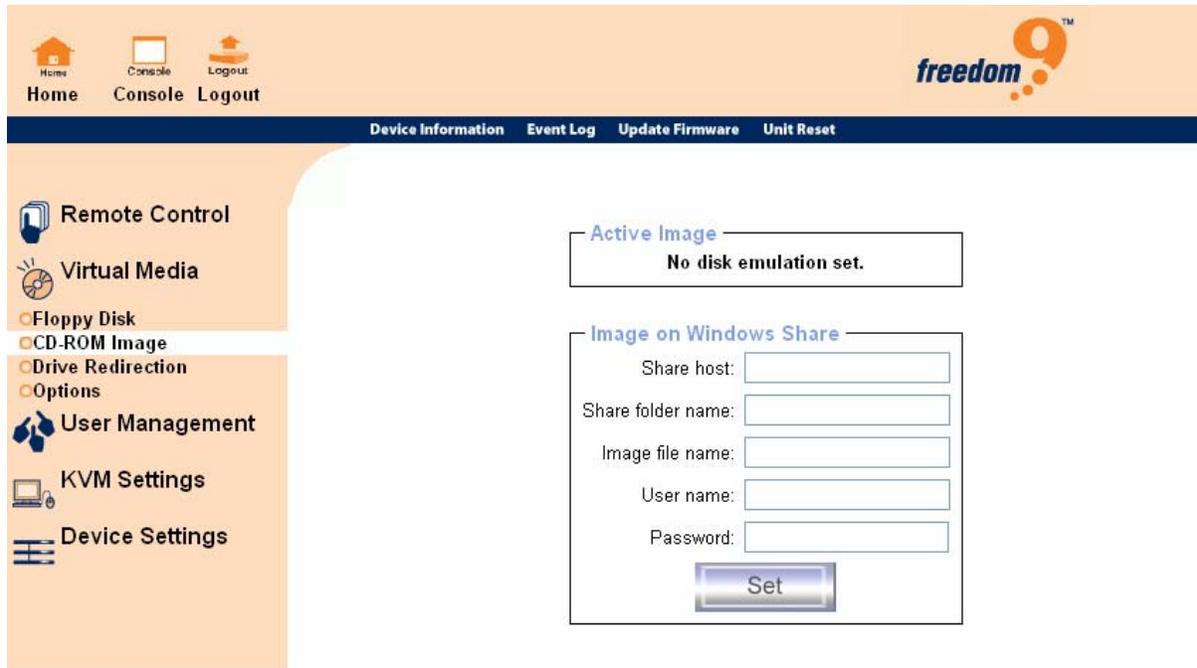


Figure 6-5: Virtual CD-ROM Image Screen

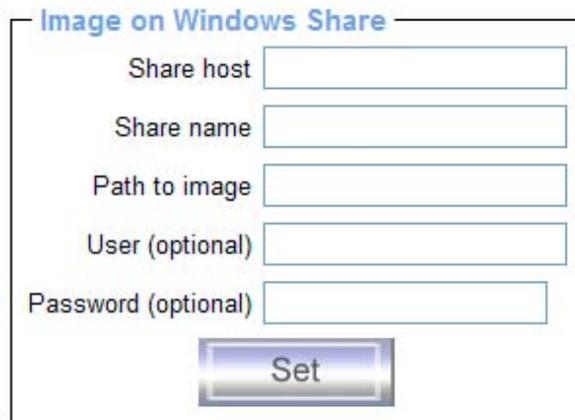


Figure 6-6: Select Windows Share

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

**Share host:** The server name, or its IP address.

**Share name:** The name of the share to be used.

**Path to image:** The path of the image file on the share.

**User (optional):** If necessary, specify the user name for the share. If unspecified, and a guest account is activated, the guest account information will be used as the login.

**Password (optional):** If necessary, specify the password required for the user name.

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

The specified image file must be accessible on the network from the freeView IP 100. It is important to specify correct IP addresses and device names. Otherwise, the device may not be able to access the referenced image file.

Additionally, ensure that the specified share is configured correctly, including granting administrator permissions to the share. Drives should be shared by the system administrator (or “root” on UNIX systems). Contact the network administrator for details.

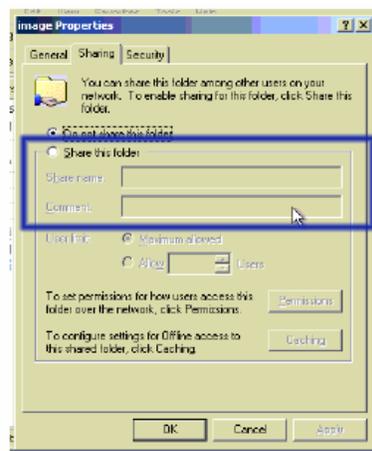
### Windows 2000/XP

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



**Figure 6-7: Windows Explorer Context Menu**

Select “Sharing” to open the configuration dialog.



**Figure 6-8: Share Configuration Dialog**

Adjust the settings for the selected directory.

- Enable sharing on the directory by selecting “Share this folder”.
- Enter a name for the share. A short description for this folder can also be added in the “Comment” field.
- Adjust the permissions if required by clicking on “Permissions”.
- Click “OK” to set the options for this share.

### **Unix, Solaris, Linux**

To access the share via SAMBA, SAMBA has to be configured properly. 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.

For additional options see the Section titled *Options* for details.

## **6.2.3 Creating An Image**

### **Floppy Images**

#### **Unix, Solaris, Linux**

To create an image file, use the “dd” command in the operating system. This is a standard command included with most Unix, Solaris, and Linux distributions.

To create a floppy image file, copy the contents of a floppy to a file using the following command:

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

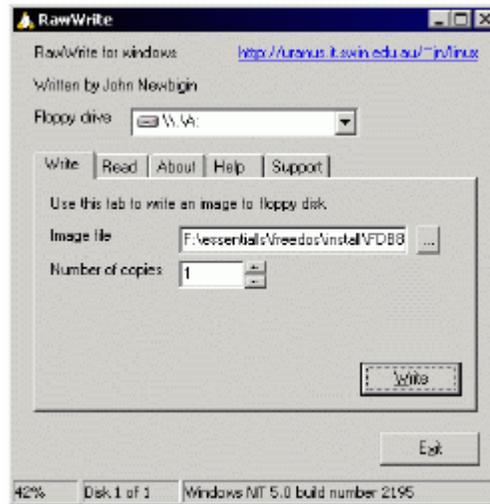
In this example, **dd** reads the entire disc from the device `/dev/fd0`, and saves the output in the specified output file `/tmp/floppy.image`.

#### **MS Windows**

A third party utility is required to create a floppy disk image. One such utility is RawWrite written by John Newbiggin which can be found here:

<http://uranus.it.swin.edu.au/~jn/linux/rawwrite.htm>

Note that this is a third party software and is only mentioned as a reference and is neither endorsed or supported by freedom9.



**Figure 6-9: RawWrite for Windows Selection Dialog**

From the menu, select the tab “Read”. Enter (or select) the name of the file in which the floppy content should be saved. Click on the “Copy” button to initiate the image creation process.

## CD-ROM/ISO Images

### Unix, Solaris, Linux

To create an image file, use the “dd” command in the operating system. This is a standard command included with most Unix, Solaris, and Linux distributions.

To create a CDROM image file, copy the contents of the CDROM to a file. The following command can be used:

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

In this example, **dd** reads the entire disc from the device `/dev/cdrin`, and saves the output in the specified output file `/tmp/cdrom.image`.

### MS Windows

To create the image file, use a third party CD imaging tool. Copy the whole contents of the disc into one single image file on the local hard disk.

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



Figure 6-10: Nero Selection Dialog

## 6.2.4 Drive Redirection

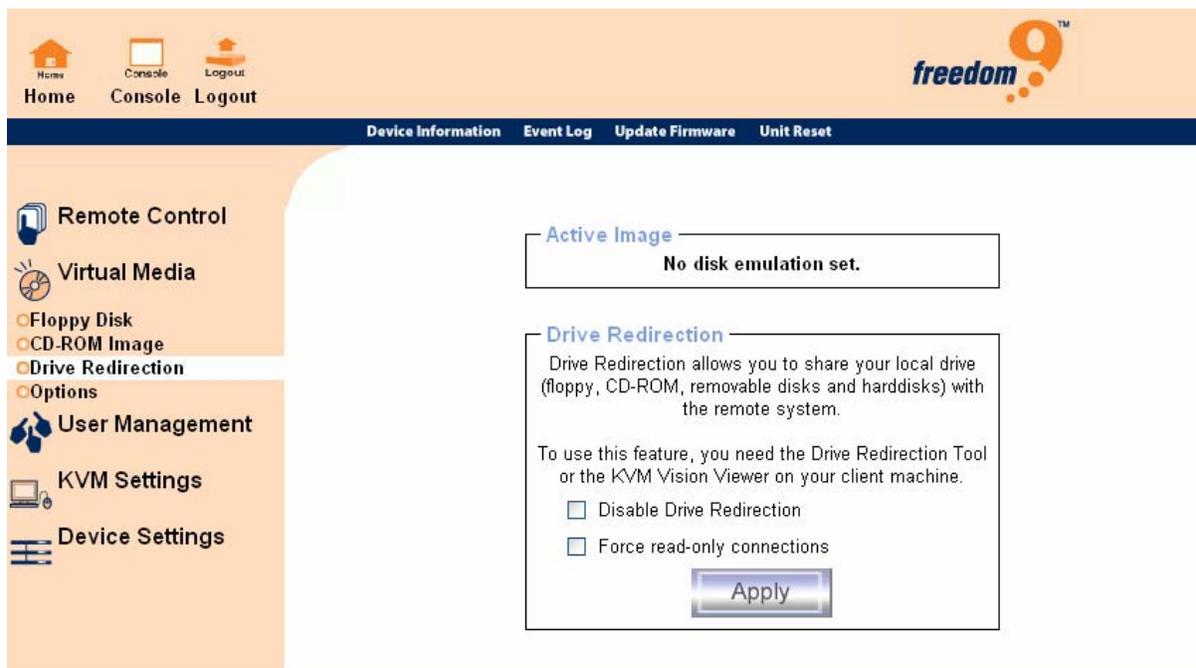


Figure 6-11: Drive Redirection Menu

## Driver Installation

Follow the KVM Vision Viewer Setup Wizard to install the driver from the included CD-ROM.

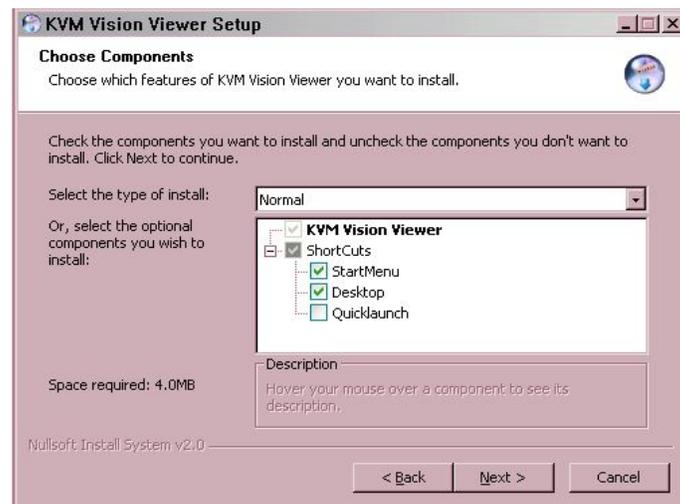




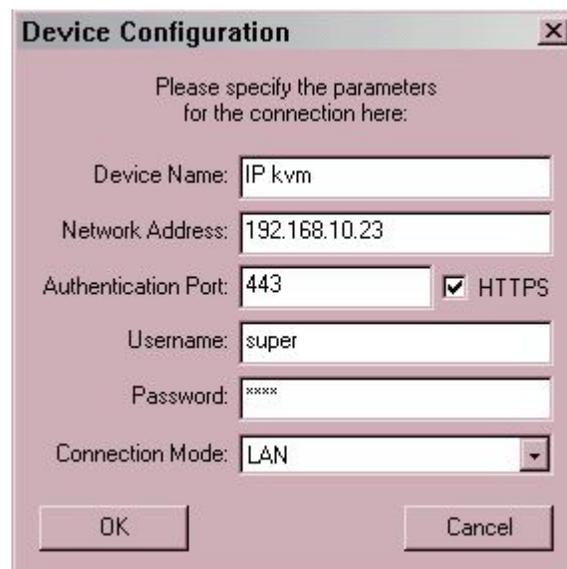
Figure 6-12: KVM Vision Viewer Setup

### Create a New Device

- Start KVM Vision Viewer
- Click on “**Device**” and select “**New Device**” to create a new device



**Figure 6-13: Create a New Device**



**Figure 6-14: Device Configuration Dialog**

**Device Name:** Enter a name for the device.

**Network Address:** Enter the IP address of device.

**Authentication Port:** This is a fixed number “443”.

**Username:** The factory default Username is “super”

**Password:** The factory default Password is “pass”.

**Connection Mode:** Select whether the connection mode is “LAN”, “DSL”, “UMTS”, “ISDN 128k” or “ISDN/Modem V9.0”.

- Click OK. The new device will be added as shown in Figure 6-15.



Figure 6-15: New Device Added

### Drive Redirection Settings

- Move the cursor to the new device that has been created.
- Click on “Device” then select “Drive Redirection” and “Redirect local drive”.

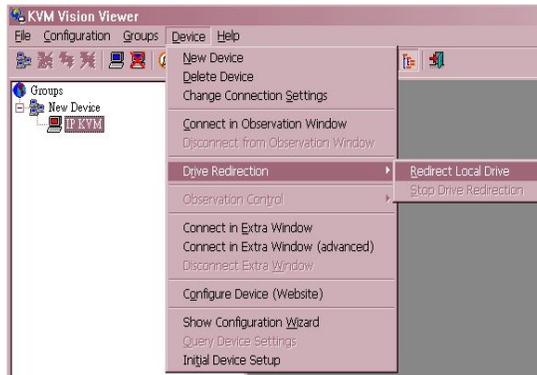


Figure 6-16: Drive Redirection Setting

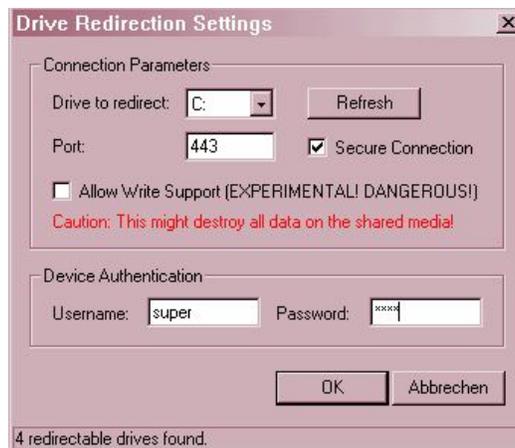


Figure 6-17: Drive Redirection Dialog

**Drive to redirect:** Select the local drive to be shared with the remote computer, which can be a floppy disc, CD-ROM, USB drive or hard drive.

**Port:** This should be set to “443”.

**Allow Write Support:** Allows the host to write to the shared drive. Note: This feature may result in the data on the shared drive being erased, back up all data before enabling this feature.

**Device Authentication:** The factory default Username is “super” and the default Password is “pass”.

- Click OK. The new device icon will be changed as shown in Figure 6-18.



**Figure 6-18: Drive Redirection Completed**

**Note:** Drive Redirection is only available with Microsoft Windows 2000 and the later.

**Note:** 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.

**Note:** While connecting to a legacy KVM switch, select PS/2 mouse for **Keyboard/Mouse setting**. Otherwise Hot-keys cannot be used.

## 6.2.5 Options



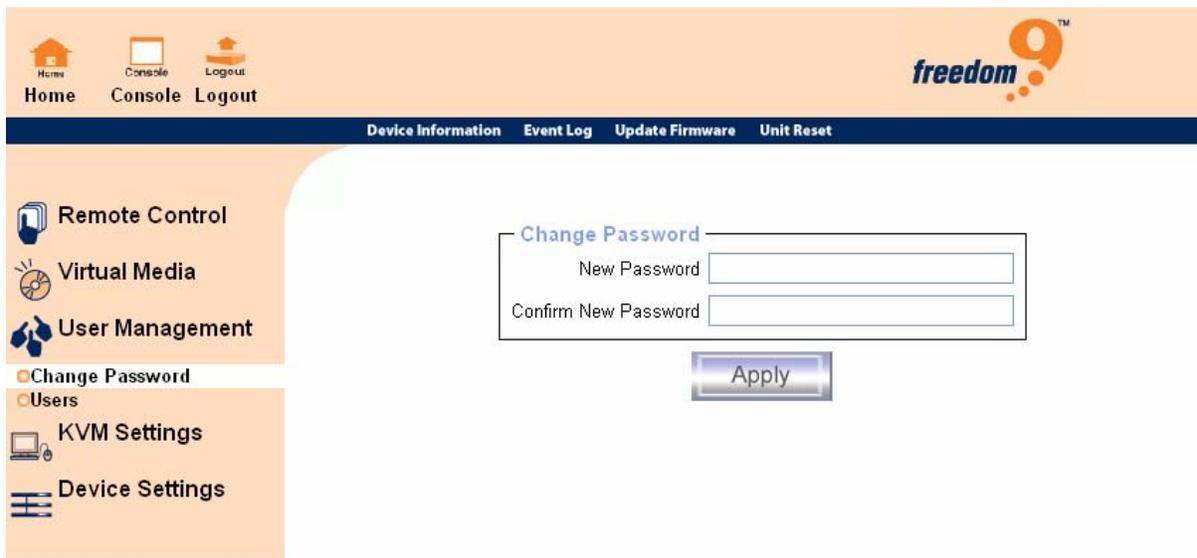
**Figure 6-19: USB Mass Storage Option**

Set this option to disable the mass storage emulation (and hide the virtual drive) if no image file is currently loaded. If not set, and no file image is loaded, the host system may hang on boot due to changes in the boot order, or the boot manager (LILO, GRUB). This mainly affects Windows versions 2000 and XP, but other OS might be affected as well. This behavior depends on the BIOS version used in that machine.

## 6.3 User Management

The User Management menu allows the user to manage user accounts on the freeView IP 100.

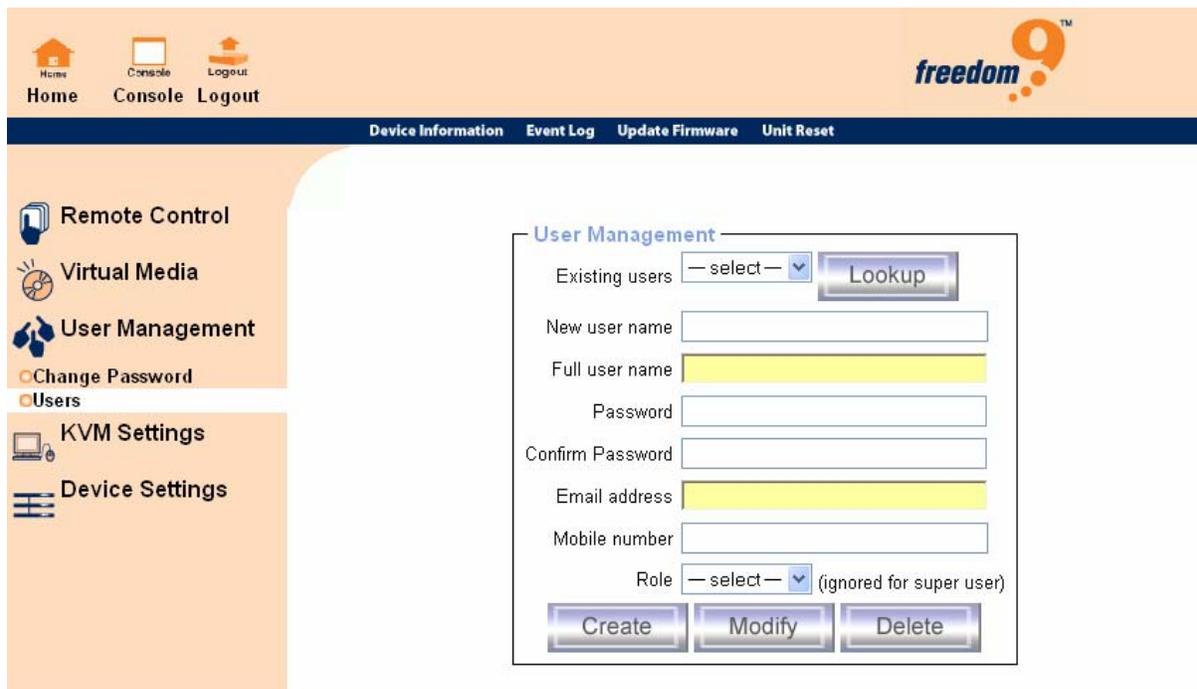
### 6.3.1 Change Password



**Figure 6-20: Set Password**

To change the current user's password, enter the new password in the upper entry field. Retype the password in the field below. Click "Apply" to submit the changes.

## 6.3.2 Users And Groups



**Figure 6-21: Set User**

The freeView IP 100 comes with 2 pre-configured user accounts that have fixed permissions. The account “super” has all possible rights to configure the device and use all of the functions available. The account “user” only has permission to open and use the Remote Console.

By default, both accounts have the password pass. Remember to change these passwords immediately after the device has been installed and accessed for the first time.

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

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

**New user name:** The new user name for the selected account.

**Password:** The password for the login name. It must be at least four characters long.

**Confirm password:** Confirm of the password above.

## 6.4 KVM Settings

The KVM Settings menu allows the user to change settings related to the remote console.

## 6.4.1 User Console

The settings for the User Console are user specific. Meaning the super user can customize these settings for every users separately. Changing the settings for one user does not affect the settings for the other users.

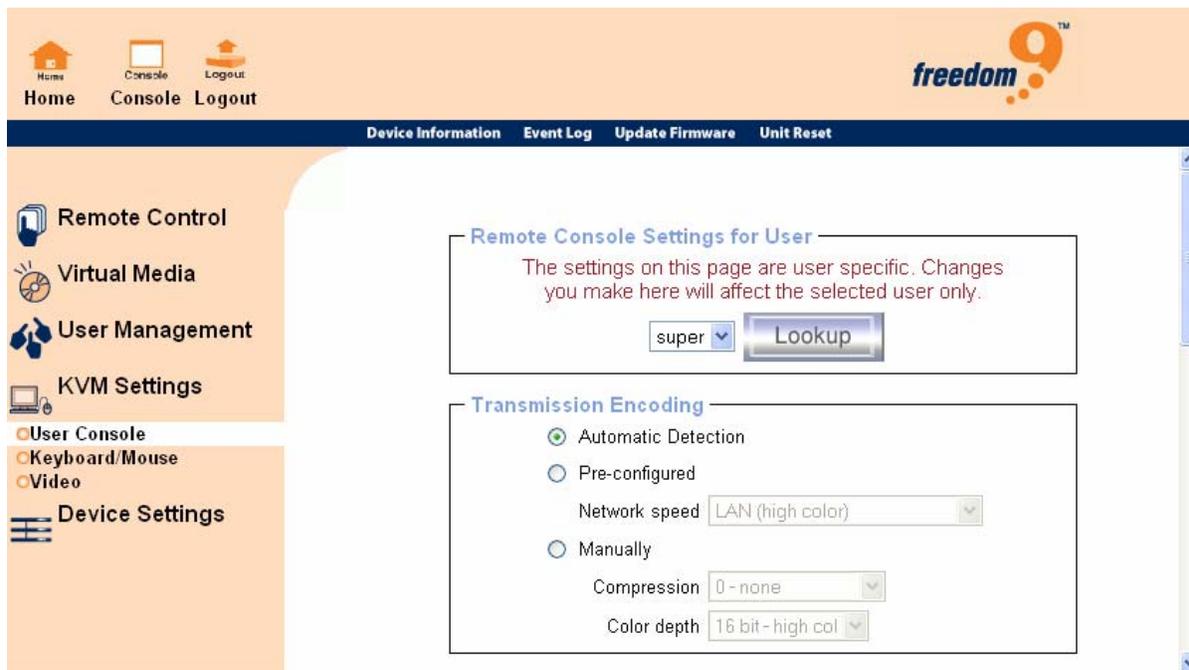


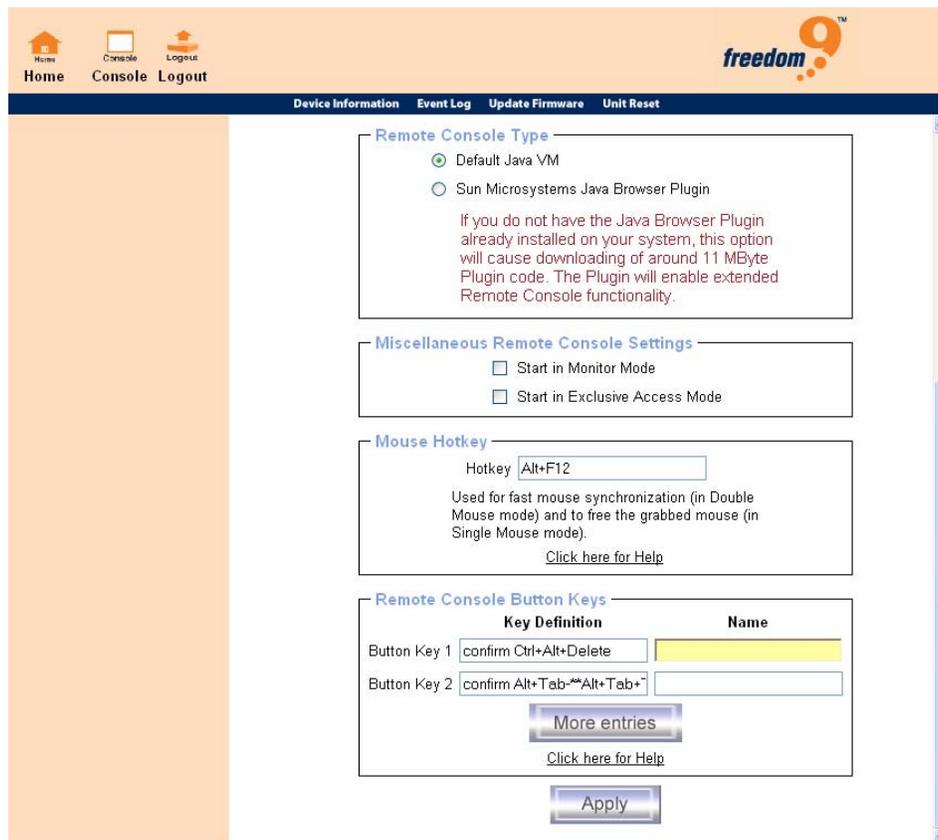
Figure 6-22: User Console Settings (Part 1)

**User select box:** This selection box displays the user ID which is being modified. The “super” user can change the settings of other users.

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

- **Automatic detection:** The encoding and the compression level is determined automatically from the available bandwidth and the current content of the video image.
- **Pre-configured:** The pre-configured settings deliver the best result because of optimized adjustment of compression and colour depth for the indicated network speed.
- **Manually:** Allows both the compression rate and the colour depth to be adjusted individually. Depending on the selected compression rate the data stream between the freeView IP 100 and the Remote Console will be compressed in order to save bandwidth. Increasing the compression rate requires more resources from the freeView IP 100, thus should not be used when multiple users are accessing the remote console simultaneously. The default color

depth is 16 Bit (65536 colors). The other color depths are intended for slower network connections since they require less bandwidth. 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-quality 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.



**Figure 6-22: User Console Settings (Part 2)**

**Remote Console Type:** Specifies which Remote Console Viewer to use, the Default Java-Virtual Machine or Sun Microsystems Java Browser Plugin.

- **Default Java VM:** Selects the default Java Virtual Machine of the Browser. This may be the Microsoft JVM or the Sun JVM depending on the configuration. Use of the Sun JVM may also be forced by selecting Sun Microsystems Java Browser Plugin
- **Sun Microsystems Java Browser Plugin:** Instructs the web browser of the local system to use the JVM from Sun Microsystems. The JVM in the browser is used to run the code for the Remote Console window, which is a Java Applet. If this box is checked and the appropriate Java plug-in is not already installed on the system, it will be downloaded and installed automatically. Once installation begins, follow the step by step instructions in install the virtual

machine. The advantage of downloading Sun's JVM is that it 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.

### **Miscellaneous Remote Console Settings:**

- **Start in Monitor Mode:** Sets the initial value for the monitor mode. By default the monitor mode is off. If this feature is turned on, the Remote Console window will start in read only mode.
- **Start in Exclusive Access Mode:** Enables 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 exclusive access or logs off.

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

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

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

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

"keycode" is the key to be sent. Multiple key codes can be 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 will 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.

## 6.4.2 Keyboard/Mouse



**Figure 6-23: Keyboard and Mouse Settings**

**Host Interface:** Sets which interface the mouse is connected to. The choices are “Auto” for automatic detection, “USB” for a USB mouse, and “PS/2” for a PS/2 mouse.

**Note:** To use the USB and/or PS/2 interface, the correct cabling (USB and/or PS/2) needs to be connected between the freeView IP 100 and the host server. If the managed host does not support USB keyboards at the BIOS level, and a USB interface is being used, remote keyboard access will not be available during the boot process of the host. If both USB and PS/2 interfaces are connected and “Auto” is selected as the host interface, the device will select “USB” if available, otherwise it falls back to “PS/2”.

To have 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 and must be selected in the Host interface option

**PS/2 Keyboard Model:** Selects the keyboard layout. Available options are “Generic 101-Key PC” for a standard keyboard layout, “Generic 104-Key PC” for a standard keyboard layout extended by three additional windows keys, “Generic 106-Key PC” for a Japanese keyboard, and “Apple Macintosh” for an Apple Macintosh keyboard.

**USB Mouse Type:** Selects the USB mouse type. Available options are “MS Windows 2000 or newer” for MS Windows 2000 or Windows XP, or “Other Operating Systems” for MS Windows NT, Linux, or OS X. In “MS Windows 2000 or newer” mode the remote mouse is always synchronized with the local mouse.

### Mouse Speed:

- **Auto mouse speed:** Select this option if mouse acceleration is enabled on the host system. The freeView IP 100 will try 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 mouse and the remote pointer.

A fixed scaling can also be set which determines the number of pixels the remote mouse pointer is moved when the local mouse pointer is moved by one pixel. This option only works when the mouse settings on the host are linear (i.e. mouse acceleration is disabled).

## 6.4.3 Video

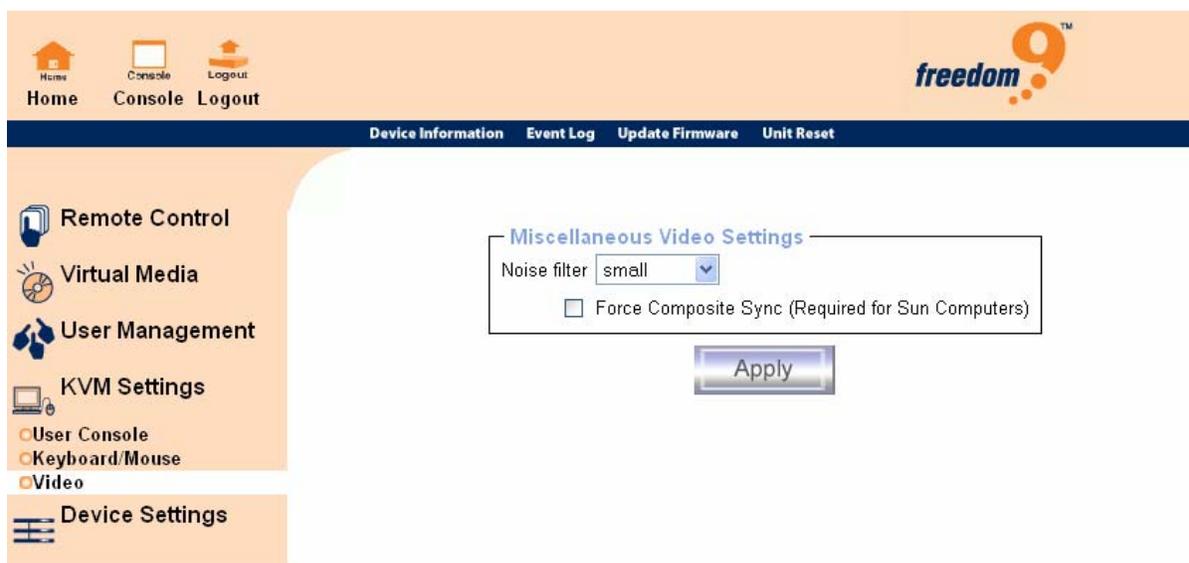


Figure 6-24: Video Settings

### Miscellaneous Video Settings

- **Noise filter:** This option defines how the freeView IP 100 reacts to small changes in the video input signal. A large filter setting uses less network traffic and leads to a faster video display, but small changes in the display may not be recognized and updated on the remote immediately. A small filter setting displays all changes on the remote host instantly but will produce more network traffic (depending on the quality of the video input signal). In general, the default setting should be suitable for most situations.

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

## 6.5 Device Settings

The Device Settings menu allows the user to configure the freeView IP 100 itself.

### 6.5.1 Network

The Network Settings panel as shown in Figure 6-25 allows network related parameters to be changed. Each parameter will be explained below. Once applied the new network settings will immediately come into effect.

**Note:** See Section 4 for instructions on installing the freeView IP 100 initially.

**Note:** Changing the device's network settings may result in loss of connection if the supplied network settings are incorrect.

The screenshot displays the 'Network Settings' page of the freeView IP 100 web interface. The page is organized into three main sections:

- Network Basic Settings:** Contains fields for IP auto configuration (set to 'None'), IP address (192.168.123.22), Subnet mask (255.255.255.0), Gateway IP address, Primary DNS server IP address, and Secondary DNS server IP address.
- Network Miscellaneous Settings:** Contains fields for Remote Console & HTTPS port (Default: 443), HTTP port (Default: 80), TELNET port (Default: 23), and Bandwidth Limit (kbit/s). It also includes checkboxes for 'Enable TELNET access' (checked) and 'Disable Setup Protocol'.
- LAN Interface Settings:** Shows current LAN interface parameters: autonegotiation on, 100 Mbps, full duplex, link ok. It includes dropdown menus for LAN interface speed (Autodetect) and LAN interface duplex mode (Autodetect).

An 'Apply' button is located at the bottom of the settings area.

**Figure 6-25: Network Settings**

**IP auto configuration:** This option determines if the device should get its network settings from a DHCP or BOOTP server, or none at all (manual IP address). For DHCP, select “dhcp”, and for BOOTP select “bootp” accordingly. If “none” is selected, then IP auto configuration is disabled.

**IP address:** The IP address in of the unit.

**Subnet Mask:** The subnet mask of the local network.

**Gateway IP address:** In order for the freeView IP 100 to be accessible from networks other than the local network, 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. If this field is empty, the unit will not be able to perform name resolution.

**Secondary DNS server IP Address:** IP address of the secondary Domain Name Server. It will

be used if the Primary DNS Server cannot be contacted.

**Remote Console and HTTPS port:** Port number which the device's Remote Console server and HTTPS server are listening on. If left empty the default value will be used.

**HTTP port:** Port number which the device's HTTP server is listening on. If left empty the default value will be used.

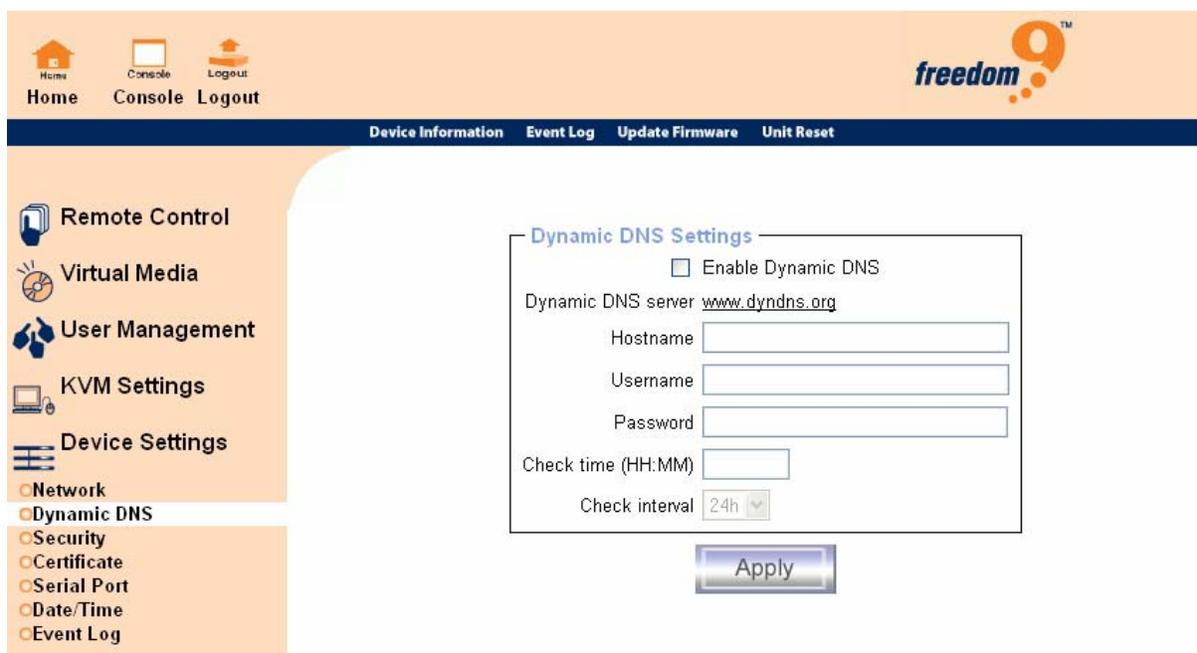
**Telnet port:** Port number which the device's Telnet server is listening on. If left empty the default value will be used.

**Bandwidth limitation:** The maximum network traffic generated by the device. Value in kbit/s.

**Enable Telnet access:** Select this option to allow access to the freeView IP 100 using the Telnet Gateway see Section 6.5.5 for more details.

**Disable Setup Protocol:** Enable this option to exclude the freeView IP 100 from the setup protocol.

## 6.5.2 Dynamic DNS



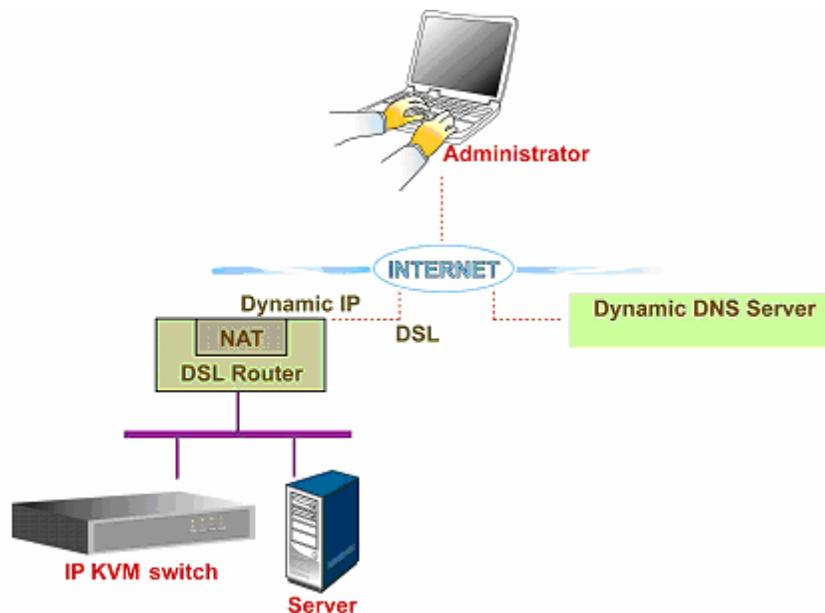
The screenshot displays the 'Dynamic DNS Settings' configuration page. At the top, there is a navigation bar with 'Home', 'Console', and 'Logout' buttons, and a 'freedom 9' logo. Below this is a secondary navigation bar with 'Device Information', 'Event Log', 'Update Firmware', and 'Unit Reset' links. The left sidebar contains a menu with 'Remote Control', 'Virtual Media', 'User Management', 'KVM Settings', and 'Device Settings'. Under 'Device Settings', there are sub-menus for 'Network', 'Dynamic DNS', 'Security', 'Certificate', 'Serial Port', 'Date/Time', and 'Event Log'. The 'Dynamic DNS' sub-menu is selected. The main content area shows the 'Dynamic DNS Settings' form with the following fields:
 

- Enable Dynamic DNS
- Dynamic DNS server: [www.dyndns.org](http://www.dyndns.org)
- Hostname: [Text Input Field]
- Username: [Text Input Field]
- Password: [Text Input Field]
- Check time (HH:MM): [Text Input Field]
- Check interval: 24h (Dropdown Menu)

 An 'Apply' button is positioned at the bottom center of the form.

**Figure 6-26: Dynamic DNS**

A freely available Dynamic DNS service (e.g. dyndns.org) can be used in the scenario shown in Figure 6-27:



**Figure 6-27: Dynamic DNS Scenario**

The freeView IP 100 is reachable from the internet via the IP address of the DSL router, which is dynamically assigned by the service provider. Since the administrator does not know the IP address assigned by the provider at any given time, the freeView IP 100 connects to a special dynamic DNS server at regular intervals and registers its IP address there. The administrator can then contact the dynamic DNS server and find the IP address of the device.

The administrator has to register the device that is with the Dynamic DNS service provider and assign a hostname (URL) to it. The Dynamic DNS service provider will assign a nickname and a password to the administrator. The hostname and the account information are needed to determine the IP address of the registered device.

The following steps detail how to enable Dynamic DNS:

- Ensure that the LAN interface of the freeView IP 100 is properly configured.
- Enter the Dynamic DNS Settings configuration dialog as shown in Figure 6-26.
- Enable Dynamic DNS and specify the settings appropriately (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 name of the server where the device registers itself at regular intervals. Currently, this is a fixed setting since only dyndns.org is presently supported.

**Hostname:** This is the hostname of the device 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:** The username provided by the Dynamic DNS Server. Spaces are not allowed in the username.

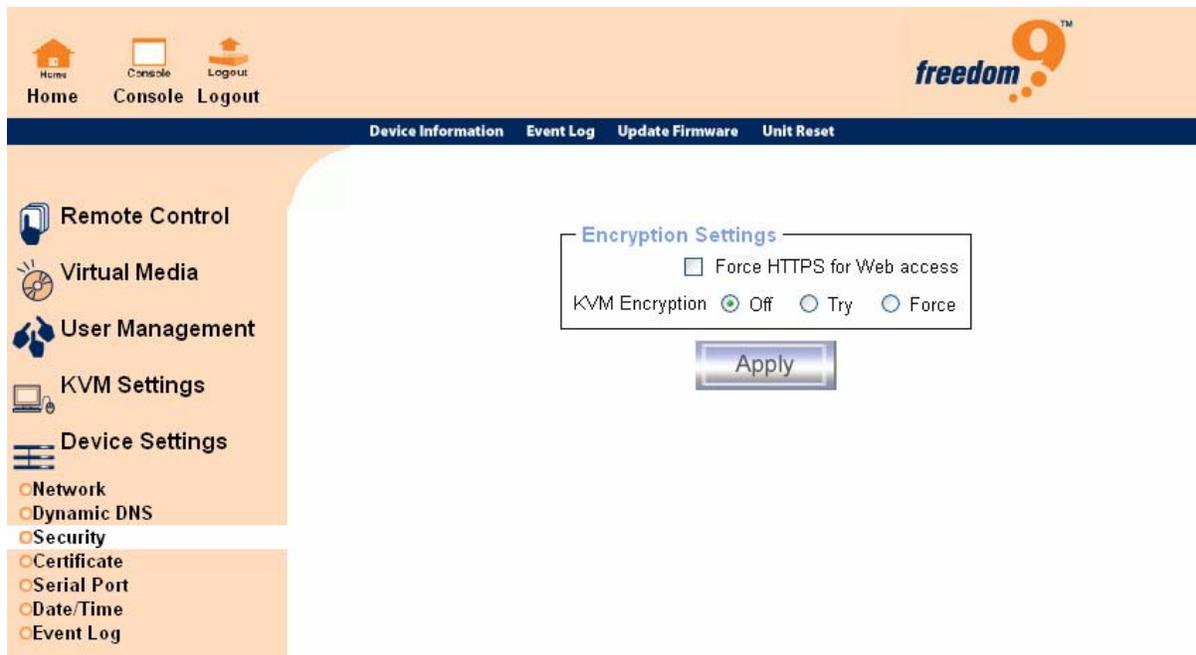
**Password:** The password provided by the Dynamic DNS Server.

**Check time:** The time which the device registers itself with the Dynamic DNS server.

**Check interval:** The time interval which the device registers itself with the Dynamic DNS based on the Check time parameter above.

Note: The freeView IP 100 has its own independent real-time clock. Ensure the time setting on the device is correct, see the section titled “Date and Time”.

### 6.5.3 Security



**Figure 6-28: Device Security**

**Force HTTPS:** When enabled, this option restricts access to the web interface to HTTPS connections only. The freeView IP will not listen on the HTTP port for incoming connections.

For instructions on creating a customer SSL certificate that is used to identify the freeView IP 100, see the Section 6.5.4 titled “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 create an encrypted connection. If an encrypted connection cannot be made, an unencrypted connection will be used. If set to “Force”, the applet tries to create an encrypted

connection. If an encrypted connection cannot be made, an error will be reported.

## 6.5.4 Certificate

**Figure 6-29: Certificate Settings**

The freeView IP 100 uses the Secure Socket Layer (SSL) protocol for any encrypted network traffic between itself and a connected client. During the connection establishment, the device has to expose its identity to a client using a cryptographic certificate. By default, this certificate and the underlying secret key is the same for all freeView IP 100's and will not match the network configuration that will the device is connected to. The certificate's underlying secret key is also used for securing the SSL handshake. Hence, there is still a potential security risk when using the default SSL certificate, but it is more secure than no encryption at all.

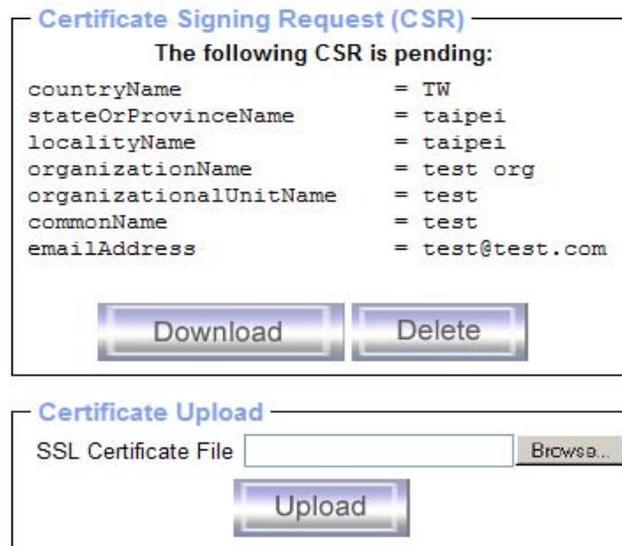
It is possible to generate and install a new certificate that is unique for a particular freeView IP 100. In order to do this, the freeView IP 100 can generate a new cryptographic key and the associated Certificate Signing Request (CSR) that needs to be certified by a certification authority (CA). A certification authority verifies that the device and identity are legitimate and signs and issues a SSL certificate for the device.

The following steps are necessary to create and install a SSL certificate for the freeView IP 100:

- Create an SSL Certificate Signing Request using the panel shown in Figure 6-29. Complete the fields on the page. The fields are explained below. Once completed, click on the “Create”

button which will initiate the Certificate Signing Request generation. The CSR can be downloaded to the local machine with the “Download CSR” button (see Figure 6-30).

- Send the saved CSR to a CA for certification. Once the CA has completed their authentication process, a new certificate will be issued for the device..
- Upload the certificate to the freeView IP 100 using the “Upload” button as shown in Figure 6-30.



**Certificate Signing Request (CSR)**

The following CSR is pending:

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

Download Delete

---

**Certificate Upload**

SSL Certificate File  Browse...

Upload

**Figure 6-30: SSL Certificate Upload**

After completing these three steps, the freeView IP 100 will have its own certificate that is used for identifying the card to its clients.

**Note:** If the CSR on the device is lost or destroyed, it cannot be recovered. The steps above must be completed again in order to obtain a new certificate.

**Common name:** This is the network name of the freeView IP 100 once it is installed in the network (usually the fully qualified domain name). It is identical to the name that is used to access the device 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 unit is accessed using HTTPS.

**Organizational unit:** This field is used for specifying which department within an organization owns the device.

**Organization:** The name of the organization.

**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, CA for Canada, or US for the USA.

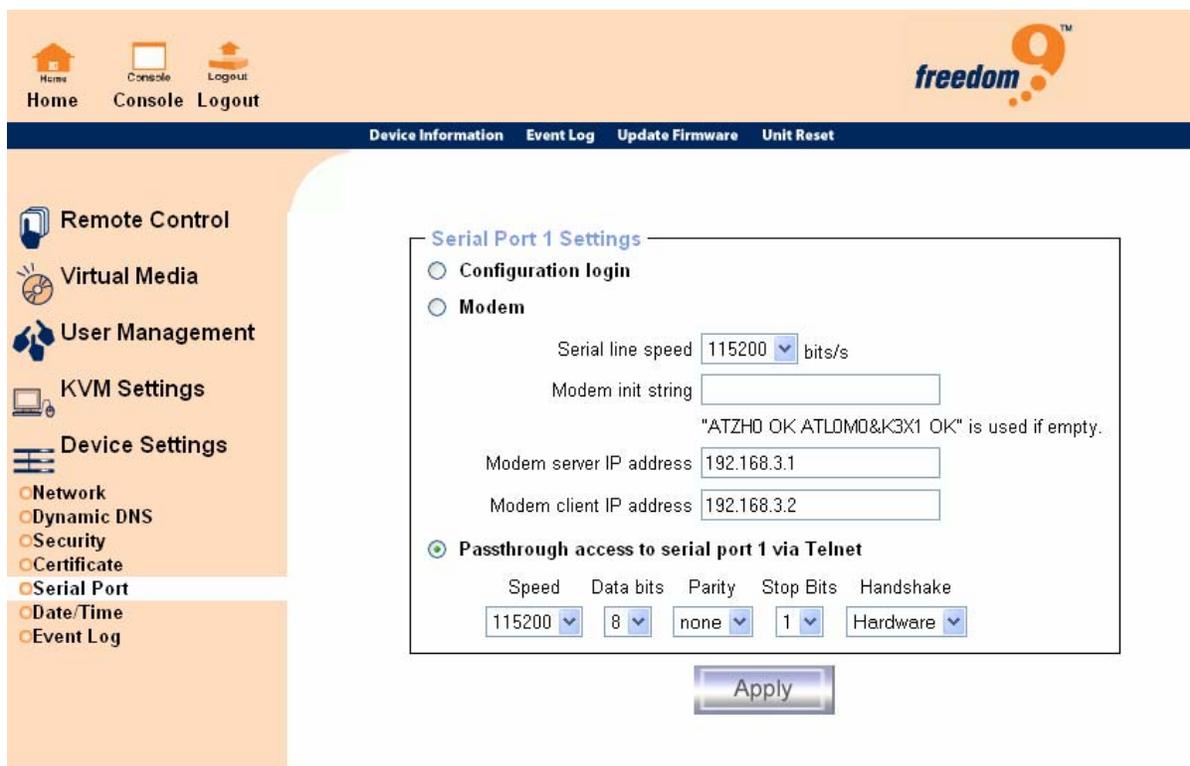
**Challenge Password:** Some certification authorities require a challenge password to authorize later changes to the certificate (e.g. revocation of the certificate). The minimum length of this password is 4 characters.

**Confirm Challenge Password:** Confirmation of the Challenge Password

**Email:** The email address of a contact person that is responsible for the unit and its security.

**Key length:** This is the length of the generated key in bits. 1024 Bits is sufficient for most cases. Longer keys may result in slower response time of the device during connection establishment.

### 6.5.5 Serial Port



**Figure 6-31: Serial Port**

The freeView IP 100's Serial Settings (Figure 6-31) allows the user to specify what type of device is connected to the serial port and how to use it.

**Configuration or console login:** Do not use the serial port for any special function, use it only for the initial configuration (see Table 4-1).

**Modem:** The freeView IP 100 offers remote access using a telephone line in addition to the standard access over the Ethernet network. The modem needs to be connected to the serial

interface of the freeView IP 100.

A user can connect to the freeView IP 100 using a telephone line the same way that it would connect to an Internet Service Provider (ISP). By dialing the telephone number of the modem using third-party modem software on the local computer, the user can connect to the device through normal telephone lines. The connection is established using the Point-to-Point Protocol (PPP). Before connecting to the device, ensure that the console computer is configured correctly. For instance, Windows based operating systems default to PPP for dial-up network connections, which is correct.

The Modem Settings panel sets the parameters used by the client to connect to the device. An explanation of the parameters is included below.

- **Serial line speed:** The speed the freeView IP 100 uses to communicate with the modem. Most modems available today will support the default value of 115200 bps. If an older modem is used and problems occur, try lowering this value.
- **Modem init string:** The initialization string used by the freeView IP 100 to initialize the modem. The default value will work with all standard modern modems directly connected to a telephone line. If a special modem is used or if the modem is connected to a local telephone switch that requires a special dial sequence to establish a connection to the public telephone network, change this setting by entering the correct a new string. Refer to the modem's manual about the AT command syntax to use.
- **Modem server IP address:** This IP address will be assigned to the freeView IP 100 itself during the PPP handshake. Since it is a point-to-point IP connection, almost any IP address is permitted, but it cannot be the same as the Ethernet connection of the device or the client. The default value will work in most cases.
- **Modem client IP address:** This IP address will be assigned to the console computer during the PPP handshake. Since it is a point-to-point IP connection, almost any IP address is permitted, but it cannot be the same as the Ethernet connection of the device or the client. The default value will work in most cases.

**Passthrough access to serial port via Telnet:** If this option is enabled, a device with a serial interface (e.g. a managed switch) can be controlled by the local computer. Select the appropriate options for the serial port and use the Telnet Console, or a standard Telnet client to connect to the device.

## 6.5.6 Date And Time

The screenshot shows the 'Date/Time Settings' page in the freeView IP 100 web interface. The page has a top navigation bar with 'Home', 'Console', and 'Logout' buttons, and a secondary bar with 'Device Information', 'Event Log', 'Update Firmware', and 'Unit Reset'. A left sidebar contains a menu with categories like 'Remote Control', 'Virtual Media', 'User Management', 'KVM Settings', and 'Device Settings'. Under 'Device Settings', 'Date/Time' is selected. The main content area is titled 'Date/Time Settings' and contains the following elements:

- UTC Offset: +/- 0 h (dropdown menu)
- User specified time**
  - Date: 1 / 10 / 2004 (mm/dd/yyyy)
  - Time: 4 : 41 : 06 (hh:mm:ss)
- Synchronize with NTP Server**
  - Primary Time server: [input field]
  - Secondary Time server: [input field]

Below the NTP Server section, a warning message reads: "The NTP Server configuration will be cleared if IP auto configuration is configured to either BOOTP or DHCP in the Network Settings and the DHCP/BOOTP server is not providing the NTP server information!". An 'Apply' button is located at the bottom of the settings area.

**Figure 6-32: Date and Time**

This page allows the user to set the internal real-time clock of the freeView IP 100 switch can be set up (Figure 6-27). The time can be set manually or using an NTP (Network Time Protocol) server. If an NTP server is not used, the internal clock will need to be reset if the unit loses power for several minutes. The alternative is to use an NTP server, which set up the internal clock automatically to the current UTC (Coordinated Universal Time, also known as GMT) time. Because the NTP server time is always UTC, the UTC offset must be correct in order for the device to have the correct time.

**Note:** The device does not adjust for daylight savings time automatically, so the UTC offset will have to be adjusted manually for daylight savings time.

## 6.5.7 Event Log

The screenshot shows the 'Event Log' configuration page. The top navigation bar includes 'Home', 'Console', and 'Logout'. Below this is a secondary navigation bar with 'Device Information', 'Event Log', 'Update Firmware', and 'Unit Reset'. The left sidebar contains a menu with 'Remote Control', 'Virtual Media', 'User Management', 'KVM Settings', and 'Device Settings'. Under 'Device Settings', there are sub-items: Network, Dynamic DNS, Security, Certificate, Serial Port, Date/Time, and Event Log (which is selected).

The main content area is titled 'Event Log Targets' and contains the following settings:

- List Logging Enabled**
  - Entries shown per page:  (Default: 20)
  - Clear internal log:
- NFS Logging Enabled**
  - NFS Server:
  - NFS Share:
  - NFS Log File:
- SMTP Logging Enabled**
  - SMTP Server:
  - Receiver Email Address:
  - Sender Email Address:
- SNMP Logging Enabled**
  - Destination IP:
  - Community:
  - [Click here to view the IP-KVM SNMP MIB](#)

Below the 'Event Log Targets' section is the 'Event Log Assignments' section, which contains a table:

| Event          | List                                |
|----------------|-------------------------------------|
| Board Message  | <input checked="" type="checkbox"/> |
| Security       | <input checked="" type="checkbox"/> |
| Remote Console | <input checked="" type="checkbox"/> |
| Host Control   | <input checked="" type="checkbox"/> |
| Authentication | <input checked="" type="checkbox"/> |

An 'Apply' button is located at the bottom of the 'Event Log Assignments' section.

**Figure 6-33: Event Log**

Important events such as a login failure or a firmware update are logged to a selection of logging destinations (see Figure 6-33). Each of these events belongs to an event group, which can be selected separately.

**List logging enabled:** This is the main method to log events. This method uses the internal log list of the freeView IP 100. To display the log, click on “Event Log” under the “Maintenance” menu. The number of log entries shown per page can be changed in this section, and the log can also be cleared by clicking the “Clear” button. **Note:** The maximum number of events that can be recorded in the log is 1000. Any entry added above this will overwrite the oldest entry in the log. Also, if the device is reset through the web interface, the log information will be stored. However, if the device loses power or a hard reset is performed, the log will be cleared.

**NFS Logging enabled:** If this option is selected, the freeView IP 100 will export the log information to a directory or static link on an NFS server. To write log data from more than one freeView IP 100 to the same NFS share, a unique file name must be defined for each device. Once the NFS settings are complete, click the "Apply" button. The NFS share will be mounted immediately. If the NFS share and the NFS server are not available, an error message will appear.

**Note:** Unlike the internal log file, the size of the NFS log file is not limited by the device. Every log event will be appended to the end of the file so it will grow continuously. Remember to clean out old log entries from the file regularly.

**SMTP Logging enabled:** If this option is selected, the freeView IP 100 will e-mail the log to an e-mail address specified in the Sender Email Address field. These e-mails contain the same information 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 feature, an SMTP server must be specified which is accessible by the device and does not require authentication. The information should be entered in the following format:

<serverip>:<port>

**SNMP Logging enabled:** If this option is selected, the freeView IP 100 will send an SNMP trap to a specified destination IP address every time a log event occurs. If the receiver requires a community string, it can be set 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 their own trap class that consists of several fields with detailed information about the event. A third party SNMP monitor is required to receive the traps.

## 6.6 Maintenance

### 6.6.1 Device Information

The screenshot shows the Freedom 9 web interface. At the top, there are navigation buttons for Home, Console, and Logout. Below this is a dark blue header with links for Device Information, Event Log, Update Firmware, and Unit Reset. On the left is a sidebar with icons and labels for Remote Control, Virtual Media, User Management, KVM Settings, and Device Settings. The main content area is titled 'Device Information' and contains the following details:

- Product Name:** IP-KVM
- Serial Number:** F2AB44950910A121
- Device IP Address:** 192.168.123.22
- Device MAC Address:** FE:00:00:46:0F:5E
- Firmware Version:** 04.00.03
- Firmware Build Number:** 1743
- Firmware Description:** Standard Edition
- Hardware Revision:** 0E

Below the device information is a link: [View the datafile for support.](#)

The 'Connected Users' section shows:

- super (192.168.123.181) active

Figure 6-34: Device Information

This section contains summary information about the device and its current firmware.

The 'Connected Users' section displays the following information:

| User                                 | Status      |
|--------------------------------------|-------------|
| test (62.238.0.39)                   | active      |
| test (80.145.25.183)                 | 26 min idle |
| test (212.183.10.29)                 | 20 min idle |
| test (62.153.241.228) RC (exclusive) | active      |

Figure 6-35: Connected Users

The Connected Users section shown in Figure 6-35 shows which users are connected to the device. The user's name, IP address, and current status are displayed. The letters "RC" beside a user's name means that the Remote Console is open. If the Remote Console is opened in exclusive mode, the term (exclusive) will be displayed.

### 6.6.2 Event log

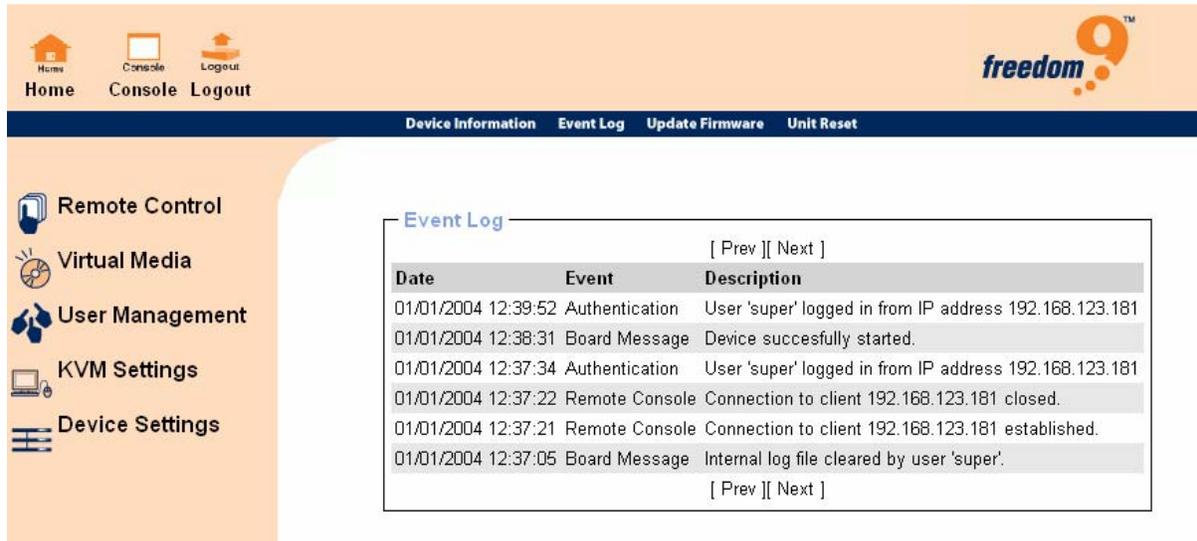


Figure 6-36: Event Log List

Figure 6-36 shows the log list including events that are logged by the freeView IP 100.

### 6.6.3 Update Firmware



Figure 6-37: Update Firmware

The freeView IP 100 is a complete standalone device. The software that runs on the device is called the firmware. The firmware of the freeView IP 100 can be updated remotely in order to add

new functionality or special features.

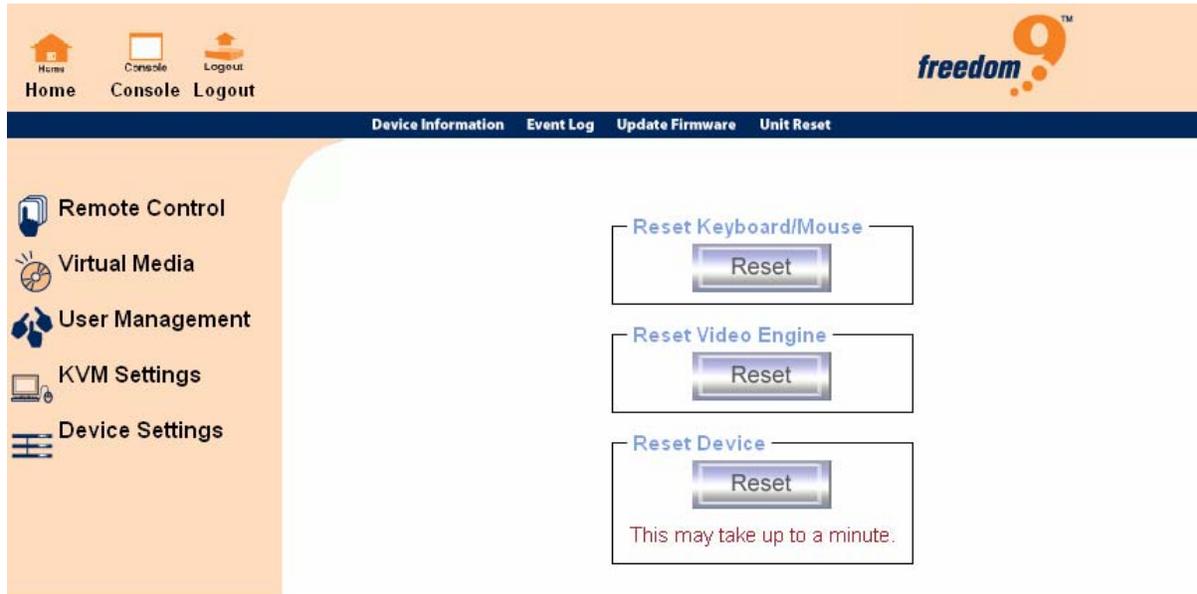
A new firmware update is a binary file which can be found on the freedom9 website at <http://www.freedom9.com>. If the firmware file is compressed (file suffix .zip) then it must be unzipped before it can be installed. Windows users can use WinZip from <http://www.winzip.com/> to unzip the file. Other operating systems will have their own unzip programs.

Before updating the firmware of the device, the new uncompressed firmware file has to be saved on the local machine.

To update the firmware, follow these steps:

- Save the firmware file on the local computer.
- Type in the path and filename of the firmware file, or click “Browse...” and search for the file on the system.
- Click “Upload”.
- Once the firmware file has been uploaded, it is checked to see if it is a valid firmware file and whether there were any transmission errors. In the case of an error, the Upload Firmware function will be aborted.
- Verify the new version of the firmware, and click “Update”. **Note:** This process is non reversible and might take a few minutes. Make sure the freeView IP 100 is not powered off during the update process, otherwise the device may be permanently damaged.
- After the firmware has been saved, a prompt will appear to reset the device manually. After the unit is reset, the new firmware will be loaded. However, the user will have to log into the unit again.
- Note: The firmware update procedure is thorough in looking for errors and inconsistencies, reducing the chances of an error occurring. However, only experienced staff or administrators should perform a firmware update. Ensure that the device is not powered off during the firmware upgrade.

## 6.6.4 Unit Reset



**Figure 6-38: Unit Reset**

This section allows the user to reset specific parts of the device. The parts include: the keyboard and mouse, the video engine, and the entire device itself. Resetting the device itself is mainly needed to activate a newly updated firmware. It will close all current connections to the administration console and to the Remote Console. The whole process will take about half a minute. Resetting sub devices (e.g. video engine) will take only a few seconds and does not result in closing connections.

**Note:** Only the super user is allowed to reset the device.

## 7 Troubleshooting

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

**A 001:** Make sure the mouse settings on the device match the mouse model. There are some circumstances where the mouse synchronization process could behave incorrectly, refer to Section 5.5.1 for more details.

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

**A 002:** Try to correct the brightness and contrast settings (see Section 6.4.3) until the picture improves. Use the auto adjustment feature to correct a flickering video.

**Q 003:** Can't log into the freeView IP 100.

**A 003:** Verify the username and password. Be default, the user "super" has the password "pass". Also, ensure that the web browser is configured to accept cookies.

**Q 004:** The Remote Console window can't connect to the host.

**A 004:** A firewall may be preventing access to the Remote Console. Make sure that TCP port numbers 80 or 443 are open for incoming TCP connection establishments.

**Q 005:** No connection can be established to the freeView IP 100.

**A 005:** Check whether the network connection is working (ping the IP address of device). If not, check the network hardware and check if the device is powered on. Check whether the IP address of the device and all other IP related settings are correct. Check that there isn't an IP conflict on the network (multiple devices using the same IP address). Verify that all of the IP infrastructure of your LAN, like routers etc., is correctly configured.

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

**A 006:** A 'Hot-key' needs to be defined for special key combinations. See Section 5.5.1 for more details.

**Q 007:** The web interface of the device looks abnormal.

**A 007:** Ensure the web browser cache settings are correct. Particularly, check that the cache settings are not set to "Never check for newer pages". Otherwise, the device interface may be loaded from the browser cache and not from the device.

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

**A 008:** This is likely a Windows XP problem. Try not to move the mouse when XP goes into standby mode.

**Q 009:** Can't upload the signed certificate in MacOS X.

**A 009:** 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. If this does not work, try using a Mozilla based browser.

**Q 010:** Every time I open a dialog box with some buttons, the mouse pointers are not synchronous anymore

**A 010:** Ensure that the feature "Automatically move mouse pointer to the default button of dialog boxes" is disabled on the host system.

## **7.1 Certificates**

### **FCC**

This equipment has been tested and found to comply with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference

(2) This device must accept any interference received. Including interference that may cause undesired operation.

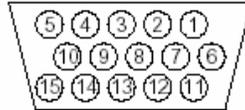
### **CE – Certificate**

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



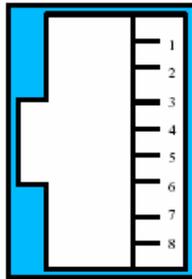
## A. Pin Assignments

### A.1 VGA HD-15



| Pin | Assignment    | Pin | Assignment    |
|-----|---------------|-----|---------------|
| 1   | Red           | 9   | 5 V           |
| 2   | Green         | 10  | GND sync      |
| 3   | Blue          | 11  | Not connected |
| 4   | Not connected | 12  | SDA, DDC, ... |
| 5   | GND           | 13  | HSYNC         |
| 6   | GND red       | 14  | VSYNC         |
| 7   | GND green     | 15  | DATA_CLOCK    |
| 8   | GND blue      |     |               |

### A.2 RJ 45 Connector Ethernet



| Pin | Assignment    | Pin | Assignment    |
|-----|---------------|-----|---------------|
| 1   | TX +          | 5   | Not connected |
| 2   | TX -          | 6   | RX -          |
| 3   | RX +          | 7   | Not connected |
| 4   | Not connected | 8   | Not connected |

### A.3 RJ 45 Connector ISDN

Same as above.

### A.4 Serial SUB-D 9 Connector 1



| Pin | Assignment | Pin | Assignment |
|-----|------------|-----|------------|
| 1   | DCD        | 6   | DSR        |
| 2   | RX         | 7   | RTS        |
| 3   | TX         | 8   | CTS        |
| 4   | DTR        | 9   | RI         |
| 5   | GND        |     |            |

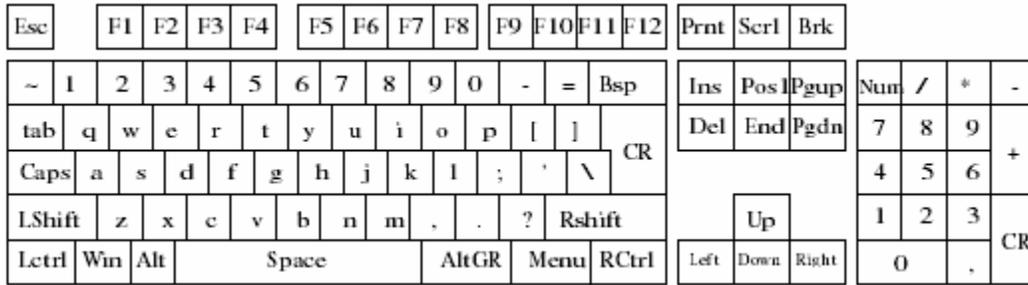
#### A.5 KVM 15 pin connector



| Pin | Assignment | Pin | Assignment    |
|-----|------------|-----|---------------|
| 1   | VGA Red    | 9   | MS Data       |
| 2   | VGA Green  | 10  | KBD VCC       |
| 3   | VGA Blue   | 11  | MS Clock      |
| 4   | KBD Data   | 12  | SDA, DCC, ... |
| 5   | KBD Clock  | 13  | HSYNC         |
| 6   | GND        | 14  | VSYNC         |
| 7   | GND        | 15  | DATA_CLOCK    |
| 8   | GND        |     |               |

## B. Key Codes

Table B-1 shows the key codes used to define keystrokes or hotkeys for several functions. Note that these key codes do not represent necessarily key characters that are used on international keyboards. The names are based on a standard 104 key PC keyboard with an US English language mapping. The layout for this keyboard is shown in Figure B-1. However, most modifier keys and other alphanumeric keys used for hotkey purposes in application programs are in the same position as a US English keyboard, no matter what language mapping is used. Some of the keys have aliases which means they can have 2 different key codes (separated by a comma in the table).



**Figure B-1: English (US) Keyboard Layout**

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

**Table B-1: Key Names**

### C. Video Modes

Table C-1 lists the video modes supported by the freeView IP 100. Do not use custom video settings besides that are not listed in the following table. Otherwise the freeView IP 100 may not be able to detect them.

| Resolution (x, y) | Refresh Rates (Hz)               |
|-------------------|----------------------------------|
| 640 x 350         | 70, 85                           |
| 640 x 400         | 56, 70, 85                       |
| 640 x 480         | 60, 67, 72, 75, 85, 90, 100, 120 |
| 720 x 400         | 70, 85                           |
| 800 x 600         | 56, 60, 70, 72, 75, 85, 90, 100  |
| 832 x 624         | 75                               |
| 1024 x 768        | 60, 70, 72, 75, 85, 90, 100      |
| 1152 x 864        | 75                               |
| 1152 x 870        | 75                               |
| 1152 x 900        | 66                               |
| 1280 x 960        | 60                               |
| 1280 x 1024       | 60, 75                           |

Table C-1: Supported Video Modes

### D. Rack Mount Kit Installation Diagram

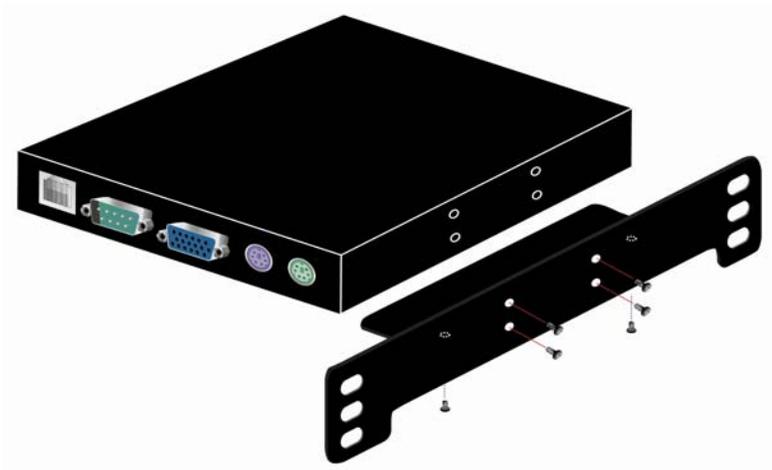


Figure D-1: Rack Mount Installation Diagram