MINICOM
ADVANCED SYSTEMS

Smart CAT5 Switch 16 IP
Operating Guide

Table of Contents

Welcome

The Smart CAT5 Switch 16 IP system is produced by Minicom Advanced Systems Limited.

Technical precautions

This equipment generates radio frequency energy and if not installed in accordance with the manufacturer's instructions, may cause radio frequency interference.

This equipment complies with Part 15, Subpart J of the FCC rules for a Class A computing device. This equipment also complies with the Class A limits for radio noise emission from digital apparatus set out in the Radio Interference Regulation of the Canadian Department of Communications. These above rules are designed to provide reasonable protection against such interference when operating the equipment in a commercial environment. If operation of this equipment in a residential area causes radio frequency interference, the user, and not Minicom Advanced Systems Limited, will be responsible.

Changes or modifications made to this equipment not expressly approved by Minicom Advanced Systems Limited could void the user's authority to operate the equipment.

Minicom Advanced Systems Limited assumes no responsibility for any errors that appear in this document. Information in this document is subject to change without notice.

No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Minicom Advanced Systems Limited.

© 2005 Minicom Advanced Systems Limited. All rights reserved.

Trademarks

PS/2 is a registered trademark of International Business Machines Corporation. All other trademarks and registered trademarks are the property of their respective owners.

Section 1: The Smart CAT5 Switch 16 IP system

This section explains how to configure and operate the Smart CAT5 Switch 16 IP (Smart 16 IP) system remotely over IP.

When Operating the Smart 16 IP Switching system locally through the On Screen Display (OSD) or Control software see Section 2 page 56.

1. Configuring the IP system

The Smart 16 IP's communication interface is based on TCP/IP, and it comes configured with the values listed below.

- DHCP - disabled
- IP address - 192.168.1.22
- Net mask - 255.255.255.0
- Default Gateway - None

If the above values are unsuitable, change the IP configuration. This can be done in a number of ways:

2. Configuration via Device Setup program

You can download the Device Setup software from Minicom's Website www.minicom.com. Connect Smart 16 IP to the same subnet as your computer. Run the Device Setup program and assign a Network configuration to the unit.

3. Configuration via DHCP server

If you activate DHCP, Smart 16 IP will try to contact a DHCP server in the network to which it is physically connected. If a DHCP server is found it may provide a valid IP address, gateway address and subnet mask. Before connecting the Smart 16 IP to your local subnet complete the corresponding configuration of your DHCP server.

We recommended configuring a fixed IP assignment to the MAC address of Smart 16 IP. You can find the MAC address on the outside of the shipping box and also labeled on Smart 16 IP's underside. If the DHCP connection fails on boot up, Smart 16 IP will boot with the last known IP configuration. So for the initial use this would be the preconfigured IP address as set out above.

4. Configuration via local console

There are two ways of doing this:

    (A) Connect the NULL modem cable to the computer's Serial port and to Smart 16 IP's Serial 1 port. Use any Terminal software to connect to Smart 16 IP. The screen shots below use Windows Hyperterminal.

1. Choose Start/Programs/Accessories/Communications/Hyperterminal.

2. When prompted enter a name and click OK. The Connect To box appears. See Figure 1.

3. Fill in the connection details. In the Connect using box, select the Serial port to which the Null modem cable is connected and click OK. The COM 1 properties box appears. See Figure 2.

Figure 1 Connect To box
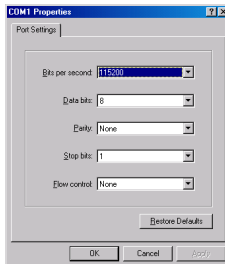
Figure 2 COM 1 Properties box

4. Set the port settings to the following values:

- Bits/second - 115200
- Data bits - 8
- Parity - None
- Stop bits - 1
- Flow Control - None

5. Click OK. The Hyperterminal appears. See Figure 3.
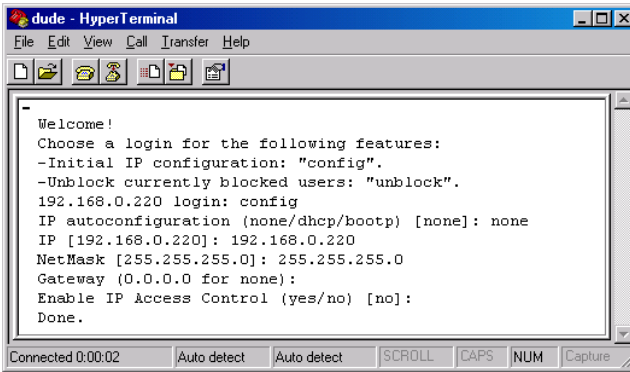
Figure 3 The Hyperterminal

6. Press **Enter**. Some device information and a prompt appear.

7. Type **config** and press **Enter**. Configuration questions appear. DHCP can be enabled or disabled. You can change the IP address, net mask and default gateway. Pressing **Enter** without entering values keeps the default values. To contact Smart 16 IP from outside the LAN configure a gateway. To remove an already configured gateway, type 0.0.0.0.

   The last question – enable IP access control – concerns switching IP packet filtering on or off. This can re-enable access to Smart 16 IP after an incorrect IP access configuration has been activated. Page 44 has more information on IP access control.

8. Confirm the settings, Smart 16 IP resets the configuration.

(B) Use a crossover Ethernet cable to connect the Smart 16 IP to the computer back-to-back.

Set the IP address of the computer to 192.168.1.20 and type 192.168.1.22 into the Address box of the web interface to carry out the IP configuration.

5. Mouse, Keyboard and Video configuration

The correct operation of the client mouse depends on the following two settings.

Smart 16 IP mouse setting

To make the remote keyboard and mouse work properly the Smart 16 IP settings for the host's mouse and keyboard types must be correct. Check the settings in the Smart 16 IP Web interface. See page 20.

Host system mouse settings

The host operating system has various settings for the mouse driver. Smart 16 IP works with accelerated mice and is able to synchronize the host with the client mouse pointer. This is further discussed on page 14.

The following may prevent proper mouse synchronization.

Special vendor-specific Mouse drivers disrupt the synchronization process. Ensure these are not on the host system

Windows XP has a setting ' enhanced pointer precision'. Deactivate it.

Check the correct setting by moving the mouse of your administration system to the upper left corner of the Remote Console and moving it there slightly forth and back. This will force mouse synchronization in that corner of the screen. Once that is done you may observe the behavior of your client mouse in accordance to the host one. If both mice desynchronize quickly one of the above may be the reason.

6. Smart 16 IP Video Modes

Smart 16 IP recognizes a limited number of common video modes. When running X-Window on the host system, don't use any custom modelines with special video modes. If you do, Smart 16 IP may not be able to detect these. Use any standard VESA video mode. Refer to Appendix A on page 79 for a list of all known modes.

You can adjust up to 4 Custom Video Modes if your video mode differs from the standard VESA video mode.

Set the Custom Video Modes in the Video settings section.

7. Operating the Smart 16 IP system

Operate the Smart 16 IP system through one of the following interfaces:

1. HTTP/HTTPS - Any standard Web browser. Depending on the Web browser, you can access the Smart 16 IP card using the unsecured HTTP protocol or, in case the browser supports it, the encrypted HTTPS protocol. We recommend using HTTPS when possible.

2. SNMP (Simple Network Management Protocol) - Any standard SNMP client can use this protocol.

3. Telnet - Use a standard Telnet client to access an arbitrary device connected to one of the Smart 16 IP's serial ports via a terminal mode.

All the above interfaces are accessed using the TCP/IP protocol. They can thus be used via the built-in Ethernet adapter or modem.

This chapter deals with the HTTP interface. The other two interfaces are explained on pages 37 and 19.

The Web browser must come with a Java Runtime Environment version 1.1 or higher. Without Java support, you can still maintain the remote host system using the administration forms displayed by the browser.

We recommend the following browsers for an unsecured connection:
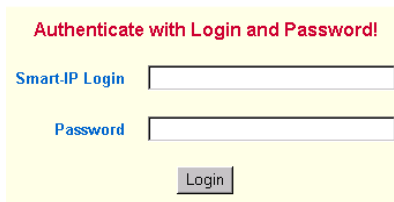
- Microsoft Internet Explorer version 5.0 or higher with Windows 98, ME, 2000 and XP

- Netscape Navigator 7.0 or Mozilla 1.0 with Windows 98, ME, 2000, and XP, Linux and other UNIX like operating systems

To access the remote host system using a securely encrypted connection you need a browser that supports the HTTPS protocol. Strong security is only assured by using key length of 128 Bit. We recommend the following browsers.

- Microsoft Internet Explorer version 5.5 or higher with Windows 98, ME, 2000 and XP

- Netscape Navigator 7.0 or Mozilla 1.0 with Windows 98, ME, 2000, and XP, Linux and other UNIX like operating systems

8. Logging in

Type the configured IP address into the Web browser. Either http://192.168.1.22 for an unsecured connection. Or https://192.168.1.22 for a secured connection. The Login screen appears. See Figure 4

Figure 4 The Login screen

Initially there is only one user configured who has unrestricted access to all Smart 16 IP features. Type the default Login name 'super' and Password 'smart' and click **Login**. The Smart 16 IP Home page appears. See Figure 5.
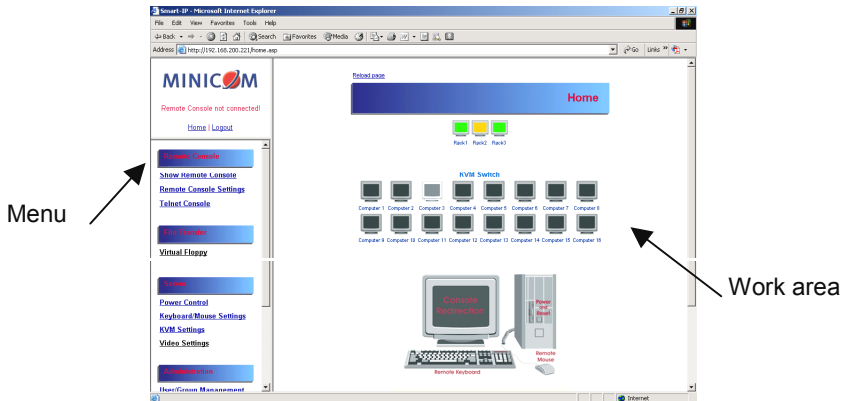
Figure 5 The Smart 16 IP Home page

9. Timeout

After half an hour of non-activity the system automatically logs out. Clicking anywhere on the screen will lead back to the Login screen.

10. The Work area

The Work area has a short summary about your Smart 16 IP.

- Server Power Status – Always on

- Firmware Version - installed on your Smart 16 IP

- Device management – self contained or connected to a management device

- Users - all currently logged in users and IP addresses. (Note: when connected through a proxy server the IP address will be that of the proxy server).

  RC – Remote Control open. **Exclusive** – Exclusive mode. **Idle** – time since last activity.

11. Remote Console

From the menu click **Show Remote Console**. The remote console appears. See Figure 6.
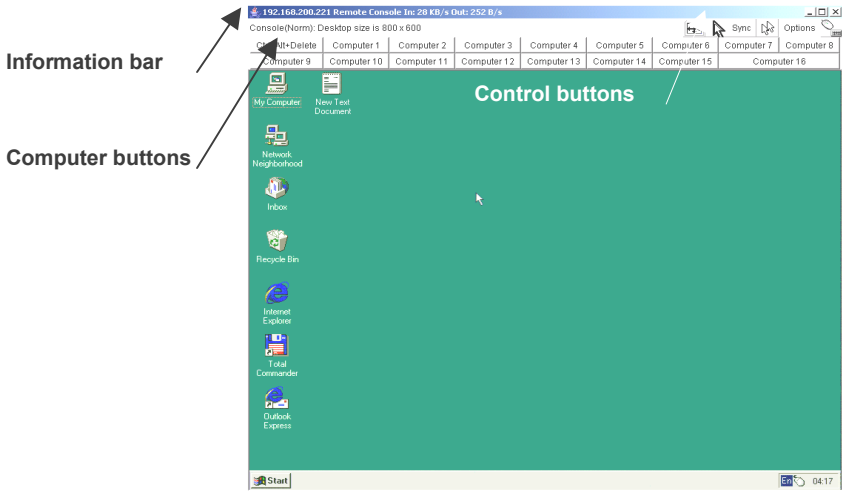
Figure 6 The remote console

You can work on it with the keyboard and mouse. The delay with keyboard and mouse reactions - if any - depends on the line connection bandwidth.

12.   Keyboard layout

Your host keyboard changes its layout to match the remote host system. So for example if the host system uses a US English keyboard layout, special keys on a German keyboard won't work but will function as US English keys.

To solve this problem, adjust the remote system keyboard to the same mapping as your host one. Alternatively, use the Soft-Keyboard that is part of the Remote Console applet.

The Remote Console window is a Java Applet that tries to establish its own TCP connection to Smart 16 IP. The protocol that is run over this connection is not HTTP or HTTPS but a protocol called RFB (Remote Frame Buffer Protocol). Currently RFB tries to establish a connection to port number 443. Your local network environment must allow this connection to be made, i.e. your firewall and, in case you have a private internal network, your NAT (Network Address Translation) settings must be configured accordingly.
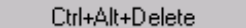
In case Smart 16 IP is connected to your local network environment and your connection to the Internet is available using a proxy server only without NAT being configured, the Remote Console is very unlikely to be able to establish the according connection. This is because today's Web proxies are not capable of relaying the RFB protocol. In case of problems, please consult your network administrator in order to provide an appropriate network environment.

The Remote Console window shows the remote screen at its optimal size. However, you can always resize the Remote Console window in your host window system.

Hint: The Remote Console window on your local window system is just one window among others. To make the keyboard and mouse work, your Remote Console window must have the local input focus.

13.   The Control buttons /toolbar icons

The control buttons/toolbar icons have the following functions:

Ctrl+Alt+Delete   - Sends the hotkey combination to the remote system.

Auto adjust - Adjusts the screen to the best video quality

Sync **Sync mouse** - Synchronizes the host and remote mice. Necessary when using accelerated mouse settings on the host system. There is generally no need to change mouse settings on the host.

- Discussed on page 16.

Click the Options button to get the following options:

Monitor Only - When turned on, the Remote Console does not accept keyboard / mouse input. The top right hand icon appears like this .

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

Readability Filter - Turn the filter on in scaling mode to preserve most of the screen details. Only available with a Java Virtual Machine version number of 1.3 or higher

Scaling - Scale down the Remote Console. Not all display details will be preserved.

Mouse handling - The submenu for mouse handling offers 3 options for synchronizing the host and the client mouse pointer - explained on pages 14 and 16. The option for 'Fast Sync' shows the hotkey if you defined one using the Remote Console Settings.

Local cursor - Choose a cursor shape for the host mouse. The number of available shapes depends on the Java Virtual Machine, only version 1.2 or higher offers the full list.

Chat Window - Opens the Chat window

Video Settings – To adjust the video settings.

Refresh video - Refreshes the video

Soft Keyboard - Opens the soft-keyboard menu:

- Click Show. The soft-keyboard appears.

- Click Layout. Choose layout

- Click Mapping. Choose the desired language and country

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

KVM keys – Each key represents a port. See page 26 to define hotkeys to switch to each port. The keys also appear in the toolbar.

Hotkeys - Button Keys simulate keystrokes on the remote system that cannot be generated locally. To define hotkeys see page 18.

Encoding – Choose the desired options from the Compression and Color Depth drop down menus.

Information bar - Shows the console and connection state and remote screen size. The value in round brackets describes the connection to the remote system: Norm stands for a standard connection without encryption; SSL stands for a secured connection. Double click the bar to see a history of all the status information.

The Chat window

Use the Chat window to chat with others logged into the system. Figure 7 illustrates the Chat window.
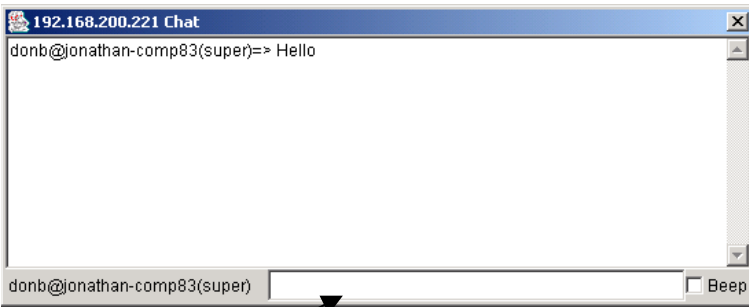
Type here

Figure 7 Chat window

All messages are broadcast to ALL connected users. There is no option to direct a message to a particular user only. There is no message history, so messages can only be received after opening the Remote Console. Type your message and press Enter. To end the Chat, close the Chat window.

The Video settings

From the Options menu choose Video Settings. The Video Settings box appears. See Figure 8.
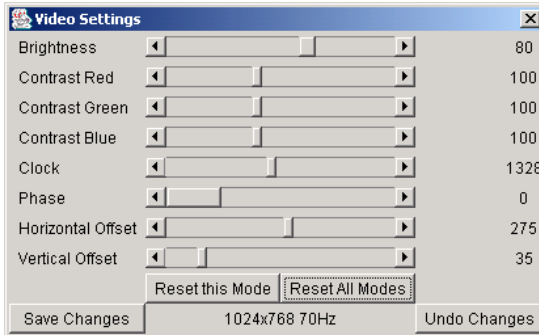
Figure 8 The Video settings

The parameters have the following functions:

Brightness - Brightness control.

Contrast Red/Green/Blue- RGB contrast control.

Clock - Sets the horizontal frequency for a video line, this depends on the video mode. Different video cards may require different values. The default settings and auto adjustment procedure should be adequate for all common configurations. If not change this setting together with the sampling phase.

Phase - Sets the phase for video sampling.

Horizontal Offset - Moves the picture in a horizontal direction.

Vertical Offset - Moves the picture in a vertical direction.

Brightness and contrast affect all modes and KVM ports globally; the other settings are changed specifically for each mode on each KVM port.

Reset this Mode - Resets mode to factory defaults.

Reset All Modes - Resets all modes to factory defaults.

Save Changes - Saves changes.

Undo Changes - Undoes changes that have not yet been saved.

Video Settings access

In the User/Group Permissions section on page 32, it explains how to set access levels for all parameters including Video Settings access. A Remote Console user can always change Brightness, Contrast and picture positions, whatever his Video Settings access rights. A user who has permission to change the Video Settings can also change the Clock and Phase parameters and use the reset buttons.

Hint. Always press the Auto Adjust video button before operating the computer. The screen should be inside the borders of Remote Control window. If the video doesn't synchronize properly or there is a lot of incoming traffic, reset all modes and synchronize video again to improve video transfer.

14. Mouse synchronization

There are two ways to synchronize the host and remote mice:

(a) Choose **Options** / **Mouse Handling** / **Fast Sync**. This corrects a temporary, but fixed skew.

(b) Intelligent Sync If the fast sync doesn't work or the mouse settings have been changed on the host system use the Intelligent Sync option.

To do so:

1. Ensure the picture is correctly adjusted, Click Auto Adjust or manually correct the picture using the Video Settings.

2. Choose **Options** / **Mouse Handling** / **Intelligent Sync**.

Pressing the ▶ Sync button usually leads to a fast sync, except when the KVM port or the video mode recently changed.

15. Mouse synchronization limitations

Synchronization may not work properly in the following cases:

1. For the intelligent sync to work, the picture MUST be correctly adjusted. Use the auto adjustment function or the manual correction in the Video Settings panel to adjust the picture. The video must also be of sufficiently good quality.

2. Special vendor-specific Mouse drivers disrupt the synchronization process. Ensure these are not on the host system.

3. **For Windows XP and 2003 Server**

   For Windows XP and 2003 Server deactivate **Enhanced pointer precision**. To do so:

   From the **Control Panel** select **Printers and Other Hardware.** Click the **Mouse** icon. The Mouse Properties box appears. See Figure 9. Select the **Pointer Options** tab.

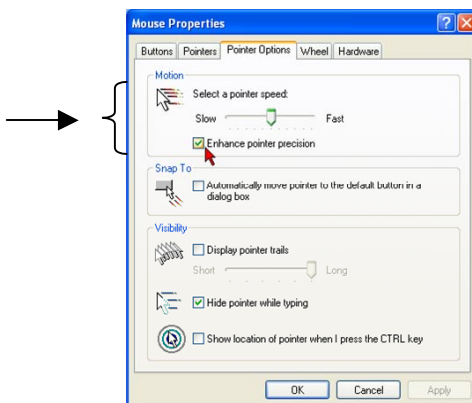**Figure 9 Pointer tab**

   The **Motion** section slider bar must be in the center, and the **Enhanced pointer precision** box must be unchecked. Click OK to save changes.

   For Windows 2000 Pro and 2000 Server

   For Windows 2000 Pro and 2000 Server deactivate **Mouse Acceleration**.

   To do so:

   From the **Control Panel** select **Mouse**. Select the **Motion** tab. See Figure 10.
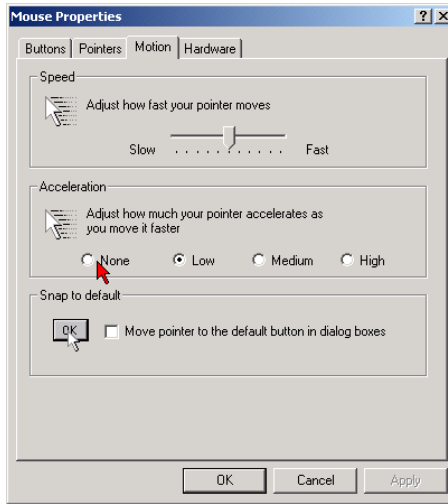
Figure 10 Motion tab

The **Speed** section slider bar must be in the center, and the **Acceleration** section must be set to **None**. Click OK to save changes.

4. Disable Active Desktop. Or do not use a plain background, use a wallpaper.

Disabling mouse acceleration in for other Operating Systems

To disable mouse acceleration in for other Operating Systems, see Appendix C on page 82.

16. Single mouse mode

The information above applies to the Double Mouse Mode, where remote and host mouse pointers are visible and need to be synchronized. There is also the Single Mouse mode. In this mode only the client mouse pointer is visible.

Single Mouse mode needs a Sun Java Virtual Machine 1.3 or later.

Select the mode in the remote console – see Figure 6.

From the Options menu choose Mouse Handling/Mouse Mode/ Single Mouse

Mode. Or press ⬚ from the Control Buttons toolbar. The client mouse pointer can be controlled directly.

To leave this mode, you must define a mouse hotkey in the Remote Console Settings Panel – see section 17 below. Press this key to free the captured host mouse pointer.

17.   Remote Console Settings

From the Smart 16 IP Menu click Remote Console Settings. The Remote Console Settings window appears. See Figure 11.

Figure 11 The Remote Console Settings

The settings and their functions are now described. All settings are user specific. Choose a user from the Drop-down menu.

Transmission Encoding - Optimizes the speed of the remote screen depending on the number of parallel users and the bandwidth of the connection line.

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 – Choose the connection method.

Manually: Compression - For low bandwidth connections. 1 is the lowest and 9 the highest compression rate. The Smart 16 IP takes time to compress the data. This option shouldn't be used when many users want access simultaneously.

Color Depth – The lower the depth the faster the speed.

Various Remote Console Options

Start in Monitor Mode - Check this option to open the Remote Console window in read only mode. (No keyboard or mouse transferred to Host computer).

Exclusive Access- Enables the Exclusive Access mode at Remote Console startup. This forces the Remote Consoles of all other users to close. No one can open the Remote Console until this user disables the Exclusive Access or logs off.

Remote Console Type

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

Sun Microsystems Java Browser Plugin - Uses Sun Microsystems Java Browser Plugin - Sets the administration system's Web browser to use the JRE (Java Runtime Environment) of Sun Microsystems. JRE is used to run the code for the Remote Console window, which is actually a Java Applet. If the Java plug-in is not installed on your system, it will be downloaded and installed automatically. The download is about 15 Mbytes. JRE provides a stable and identical Java Runtime Environment across different platforms. The Remote Console software is optimized for this JRE version and offers wider range of functionality when run in SUN's JRE.

Tip! The software is on the Marketing & Documentation CD. So, if you have a slow Internet connection, pre-install the JRE on your administration machine.

ActiveX control - Use an ActiveX control instead of a Java applet - This is the ActiveX-Control of the KVM Vision Viewer - an application available separately. You must install the viewer on your local system. See the Viewer Guide for further information. This option only works with Microsoft Internet Explorer on Win32 Systems. (Download KVM Vision Viewer from www.minicom.com).

Mouse hotkey - Used for fast mouse synchronization in Double Mouse mode and to free the grabbed mouse when in single mouse mode.

Remote Console Button Keys - Button Keys simulate keystrokes on the remote system that cannot be generated locally. For example `Control + Alt + Delete' on Windows and DOS or `Control + Backspace' on Linux.

Define a new Button Key as follows:

Type the required keys e.g. Ctrl+Alt+Delete. The + sign means that the keys are pressed together. The – sign means the keys are pressed sequentially.

The * sign inserts a pause with a definable duration. See page 25.

To require a confirmation request before keystrokes are sent, write **confirm** at the start. E.g. confirm Ctrl+Alt+Delete.

For a list of key codes and aliases Smart 16 IP recognizes, refer to Appendix B on page 80.

Press **Apply** for the changes to take effect.

Home Page Refresh – Refreshes the Smart 16 IP Home page, so that direct Smart IP Links updates their status.

18.   Telnet Console

The Telnet Console offers a Java applet for the Telnet protocol to open a connection to Smart 16 IP. Its main use is the pass through option for the Serial port 1 see page 38. The Telnet access has to be enabled in the security settings as well, see page 44. It is also possible to connect with a standard Telnet client.

Access via Telnet

Connect via a standard Telnet client using Smart 16 IP's Telnet server. Use it for passthrough access to a device connected to serial port 1. Connect any serial device, which offers terminal access via its serial port and access it using the Telnet interface. Set the Serial settings - see page 37 - according to the requirements of the device.

Connect to Smart 16 IP in the usual way required by the Telnet client, e.g. in a UNIX shell: telnet 192.168.1.22 – (The IP address has been replaced by the one that is actually assigned to Smart 16 IP).

Type a username and password when prompted. These are identical to those of the Web interface. The user management of the Telnet interface is controlled just like the Web interface.

Once logged in, the command line appears to type management commands.

The interface supports both the command line and terminal modes. The command line mode is used to control or display some parameters. In terminal mode the passthrough access to serial port 1 is activated (if the serial settings were made accordingly). All inputs are redirected to the device on serial port 1 and the answers appear on the Telnet interface.

Telnet server commands

Click **help** to list the following commands:

cls - Clears screen

quit - Logs out current user and disconnects from the client.

version - Shows all available version numbers

terminal - Starts the terminal passthrough mode for serial port 1. The key sequence `<esc> exit' switches back to command modus.

19. Status via IPMI

The Status via IPMI function shows the current values and the min/max-thresholds of all fans, temperatures and voltages existing in the host system. Change the thresholds by editing the values and pressing Apply.

The first time you call this page, it can take up to two minutes until the sensor data appears.

Note: If IPMI is disabled, Status via IPMI and System Log via IPMI are not available (the menu options are not visible).

20. Event Log via IPMI

The Event Log via IPMI accesses the SEL (System Event Log) repository and reads every entry sequentially. The first time you use this function after starting Smart 16 IP the complete repository has to be read, what may take 1 or 2 minutes.

After reading all entries, Smart 16 IP displays them with their time, sensor and description in accordance with the filter settings. You have the choice between several pre-settings (i.e. last day, last week) or an exact declaration of the start and the end date.

Once you change the filter settings, click `Update' to update the shown entries. If the Get sensor names box is checked, all sensor IDs are shown with their respective names.

The time shown in the log entries is the SEL time, meaning it is independent of the system time. The SEL time is shown at the top of the log table. Click Clear Event Log to delete all entries in the SEL repository.

21. File transfer – Virtual Floppy

This feature does not currently work.
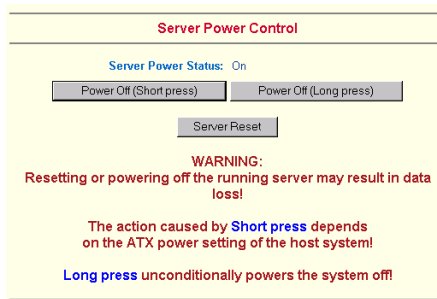
22. Power Control

The appearance of the power control window depends on the power control option connected to Smart 16 IP and on the currently activated setting (discussed on page 40). There are 4 options available: Power control disabled. Internal power. External power. Power control via IPMI.

Internal power

Once connected enable the internal power option using the Serial settings on page 37.

The Power Control panel enables access to the most important external buttons of your host system. These buttons are the reset and the ATX power button.

The power button represents the ATX power button on your host system. It is used to switch the power supply on and off. The ATX power button has 2 operation modes: a short press, and a press of about 4 seconds. As shown in Figure 12 these two modes are supported separately. The 2 operation modes are explained in the next section.

Figure 12 Internal Power Control

Note: The prerequisite for the remote power/reset button to work is a correct installation of Smart 16 IP.

The Remote reset and power button effects are as follows:

Reset - This is similar to pressing the reset button directly on the remote system. Pressing the reset button will result in a cold start of the system. This might damage open files and the file system itself.

Power (short press) - A short press on the ATX button is normally caught by the running operating system that tries to initiate a controlled shut down. Do this to switch off the system. If this does not work try the long press button.

After pressing, the power state displayed in the administration panel won't immediately reflect the requested change. A controlled shut down of the system may take some minutes. Observe the action caused by your button press using the Remote Console window or by reloading the Server Power Control panel.

Power (long press) - This will unconditionally power off the system. Even if you have submitted a short press before, this will shut down the power supply of the host system. The effect of the long button press can be immediately observed on

the panel that is loaded into the browser because of the button press. The power state will be off.

External power

If the external power option is enabled it will look like Figure 13.

Figure 13 External power control

The upper half is used to switch the power for the KVM port currently active. Use the KVM settings – see page 24 - to assign a port of the external power control to a KVM port. If no assignment exists, the option is disabled.

The lower half offers controls for switching each port of the external power control directly. Select the appropriate port and decide whether to power it off or on.

If IPMI is enabled, the power control functions are performed over IPMI requests. This may take a few seconds.

If IPMI is disabled, the power control functions are performed through the internal or external power control options.

23.   Keyboard & Mouse Settings

Smart 16 IP supports different keyboard and mouse types.

Click Keyboard & Mouse Settings. The settings appear as in Figure 14.

Figure 14 Keyboard & Mouse Settings

The elements of the Keyboard & Mouse Settings are explained below.

Host Interface – Only Auto or PS/2 are active. USB is for future applications.

Targeted KVM port

1. Choose a port to which a Host computer is connected.

2. Press Update to display the current values for the selected KVM port.

Without pressing Update alterations will **NOT** be made to the chosen port.

Keyboard Model - Choose the keyboard model for the chosen port. Select Generic 106-key PC when connecting to computers with a Japanese OS.

USB Mouse Type – Not active in the system, leave at default state.

Auto Mouse speed

When Mouse Acceleration on the Host computer is enabled, check **Auto Mouse speed**. We highly recommend disabling the Mouse Acceleration.

Fixed Mouse speed

When Mouse Acceleration on the Host computer is disabled, select Fixed Mouse Speed see Figure 15. Also in the Scaling drop-down menu select 1.00.

Repeat this procedure separately for each Host computer.

Figure 15 Mouse settings

G&D Equalizer – This supports to the mouse synchronization for Guntermann & Drunck KVM switches. These switches perform an internal rescaling of the mouse movements, which cause the existing algorithm to break if Smart 16 IP is connected behind such a switch. This option detects the rescaling and compensates for it, so that the mouse synchronization works. Do not select this option for the Smart 16 IP- it may disrupt the normal mouse synchronization.

Apply - Click to apply changes

Reset - If the keyboard or mouse seems to react irrationally click to reset the keyboard and mouse emulation. It is like disconnecting and reconnecting the keyboard and mouse connectors.

Adjust keyboard and mouse settings for all Smart 16 IP ports.

24.   KVM Settings

By default the Smart 16 IP is configured for 16 ports. When you want to add more, adjust the settings for the KVM ports. From the Smart 16 IP menu choose KVM Settings. The Smart 16 IP KVM settings appear. See Figure 16.
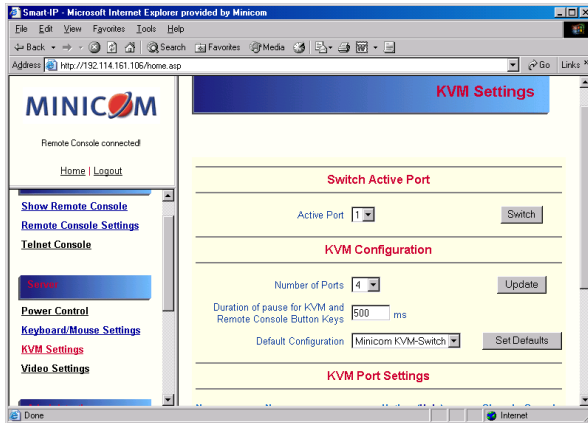
Figure 16 KVM Settings

The elements of the KVM Settings are explained below.

Active Port

To switch to a computer:

1. Choose a number in the Active port Drop-down list.

2. Press Switch . The computer screen appears in the Remote Console.

Number of Ports

To set the number of ports the KVM uses:

1. Choose a number in the Number of Ports Drop-down list.

2. Press Update . The number of rows chosen appears in the KVM Port Settings list. See Figure 17.

Duration of Pause

Define the pause time for KVM and Remote Console Button Keys in milli-seconds, represented by the * symbol in all hotkeys and button keys.

Default configuration

This is explained in the section below.

KVM Port Settings

Nr	Name	Hotkey (<u>Help</u>)	Show in Console	Power Control
1	Computer 1	LSHIFT-LSHIFT-*1-ENTER	☑	Assign
2	Computer 2	LSHIFT-LSHIFT-*2-ENTER	☑	Assign
3	Computer 3	LSHIFT-LSHIFT-*3-ENTER	☑	Assign
4	Computer 4	LSHIFT-LSHIFT-*4-ENTER	☑	Assign
5	Computer 5	LSHIFT-LSHIFT-*5-ENTER	☑	Assign
6	Computer 6	LSHIFT-LSHIFT-*6-ENTER	☑	Assign
7	Computer 7	LSHIFT-LSHIFT-*7-ENTER	☑	Assign
8	Computer 8	LSHIFT-LSHIFT-*8-ENTER	☑	Assign
9	Computer 9	LSHIFT-LSHIFT-*9-ENTER	☑	Assign

Figure 17 KVM Port Settings

25.   KVM Port Settings

1. Assign names for each port.

2. Define hotkeys to switch to each port.

Choose either Minicom default hotkeys by selecting Minicom KVM-Switch in the Default configuration box, and then click the Set Defaults button.

Or choose your own hotkeys. The syntax to define a new hotkey is as follows: <keycode> [+ | - | *] <keycode>.

For example LShift-LShift-*1-Enter. A + sign means that the keys are pressed together. The – sign means the keys are pressed sequentially. Lshift means the left Shift key.

The * sign inserts a pause with a definable duration. Add more than one pause if necessary. See Appendix B on page 80 for a list of key codes.

3. Press **Apply** at the bottom of the page. The settings are saved.

Smart 16 IP uses separate mouse synchronization settings - see page 14 - and video-settings - see page 13 - for each port.

Note:

It is still possible to apply OSD key combinations through the Remote Console for switching the KVM port. However, video and mouse synchronization settings will be shared among the ports and may be unintentionally changed for one of those ports.

If an external power option is enabled it is possible to assign a port of this control for power switching to each KVM port, see page 20.

Show in console – check this option to have a button with the port name appear on the top of the Remote console. Click the button to switch to that computer.

Power Control – Click Assign to configure the power option for each port. The following screen appears.

Figure 18 Power option

Select the Serial port to which Power switch is connected.

From the drop-down list select the outlets connected to the Power switch.

Appending a socket

Click ` Append ` to add the socket to the end of the list (it will be last to be powered on/off).

Inserting a socket

To insert a socket in the list:

1. In the currently included socket list highlight the socket above which you want to insert the new socket.

2. From the Drop-down list select the socket to be inserted.

3. Click ` Insert `. The new socket is added.

Each selection adds the outlet to the list at the bottom. The order of powering off/on, will be the order as set out in this list.

Changing the order

To change the order the outlets are powered on/off:

Highlight the desired outlet and move it using the arrows.

26.   Video Settings

From the Smart 16 IP Menu choose Video Settings. The Video settings appear. See Figure 19.

Figure 19 Video Settings

Enable local video port

This option decides if the video output on the local monitor connected to Smart 16 IP is active and passing through the incoming signal from the host system.

Use this option to switch off the local monitor connected to Smart 16 IP when accessing sensitive information on the Host computer.

Noise filter

Define how Smart 16 IP reacts to small changes in the video input signal. A large tolerance needs less network traffic and leads to a faster video display, but small changes in some display regions may not be recognized immediately. A small tolerance displays all changes instantly but may lead to a constant amount of network traffic even if display content is not really changing (depending on the quality of the video input signal). The default setting should be suitable for most situations.

Custom Video Modes

Add video modes to Smart 16 IP, which are not recognized using the factory settings, when for example using special model lines in an X-Window configuration on the host or with uncommon hosts or operating systems.

Click Add Custom Video Modes. The Custom Video Modes window appears see Figure 20.

Note! This option may affect the correct video transmission and is for advanced users only.

The maximum number of custom video resolutions is 4.

Figure 20 Custom Video Modes window

Custom Modes Handling – switch custom modes off, or use in addition to the standard video resolutions, or use exclusively - **Only**. With **Only** you can force a special video mode for Smart 16 IP.

To change the parameters for a mode, choose the number and press **Update**.

X Resolution - Visible number of horizontal pixels.

Y Resolution - Visible number of vertical pixels.

Horizontal Frequency (Hz) - Horizontal (line) frequency.

Vertical Frequency (Hz) - The vertical (refresh) frequency.

Total horizontal pixels - The total amount of pixels per line, including non-visible and blank areas.

Polarity - The polarity (positive/negative) of the synchronization signals. V means vertical, H means horizontal.

Description Give the mode a name. The name appears in the Remote Console when the custom mode is activated.

27.   User/Group Management

From the Smart 16 IP Menu choose User/Group Management. The User/Group Management settings appear. See Figure 21. The user and group management of Smart 16 IP is based on configurable users and groups. Each user or group can have different access capabilities.

The Smart 16 IP is factory set with a supervisor user called `super' with the password 'smart'. Change the super user password immediately after accessing the Smart 16 IP.
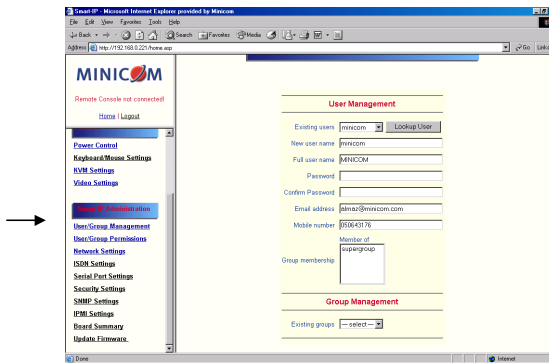
Figure 21 The User/Group Management settings

Existing user

Select an existing user for modification or deletion. Once selected, click
Lookup User to see the user information.

New user name

Enter a login name for a new user here. Ensure that it is not the same as an existing user or group.

Full user name

Write the full name of the new user.

Password / Confirm password

The password must be at least four characters. Confirm password.

Email address /Mobile number

These are optional.

Group membership/Member of/Not Member of

Each user can be a member of one or more groups and inherit the rights of that group. Use the arrows to add or remove a user from a group.

Existing groups

Select an existing group for copying, modification or deletion.

New group name

To create a new group, enter a new group name.

Create User button

Once the required fields are filled in, click the Create User button to create a new user.

Delete User button

To delete a user:

1. Select a user in the Existing users Drop-down list.
2. Click the Lookup button. The complete user information appears.
3. Click the Delete User button.

Note: The factory set supervisor user `super' cannot be deleted, but it can be renamed.

Modify User button

To modify a user:

1. Select a user in the Existing users Drop-down list.
2. Click the lookup button to get all the user's information.
3. All fields can be modified as required. The old password is not displayed, but can be modified.
4. Click the Modify User button.

Copy User

To copy an existing user's properties to a new user:

1. Select a user in the Existing user Drop-down list.

2. Enter a new user name in the New user name box.

3. Click the Copy User button. All properties of the selected user will be copied to the new one, except user specific permissions.

Group Management

The following headings appear under Group Management.

Create group button

To create a group:

1. Type a name into the New group name box

2. Click the Create group button.

Delete Group button

To delete a group:

1. Select a group in the Existing groups Drop-down list.

2. Click the Delete group button.

Modify Group

To modify an existing group select the group in the Existing group control. The group's name field can be modified. Finally click the Modify group button.

Copy Group

To create a group with the properties of an existing group:

1. Select a group in the Existing group Drop-down list.

2. Type a name into the New group name box.

3. Click the Copy Group button.

28. User/Group Permissions

From the Smart 16 IP Menu choose User/Group Permissions. The User/Group Permissions settings appear. See Figure 22.

Figure 22 User/Group Permissions

Each user or group has a set of access rights to the Smart 16 IP functions. The user 'super' always has unalterable full access rights. A newly created user has the access rights of all groups he belongs to.

You can change the access rights in the User/Group Permissions panel. The panel shows the changes to the access rights inherited by the user's ancestors only. This means an empty user permission list has exactly the same access rights as the groups he belongs to.

When one user creates a new user, he can alter his access rights. A user can change another user or group's access rights if he stands higher in hierarchy. The 'super' user stands at the top of the hierarchy, and can change everybody's access rights.

A user can never give more access rights than he himself has but he can always reduce the access rights.

To change access rights:

1. From the Drop down list select a user/group. The selection list shows only users and groups, which you have the right to change.

2. Click the Update button. The access rights of the user appear. The meaning of the Permissions is as follows:

Viewing a field. allow view means you can view it. deny access means you cannot view it.

Changing a field setting. Allow change means you can change it. (This doesn't give an automatic right to view the value, the allow view value must also be set). Deny change means you cannot change it.

Using a function. allow access means you can use it. deny access means you cannot use it.

3. Select the desired permission and click **Apply**.

29.   Network Settings

From the Smart 16 IP Menu choose Network Settings. The Network Settings appear. See Figure 23.

Figure 23 The Network Settings

In the Network Settings panel you can change the network parameters.

The initial IP configuration is usually done directly at the host system. However you can also connect to the Smart 16 IP using its pre-configured IP settings.

Warning! Changing the network settings of Smart 16 IP may result in losing the connection. If you remotely change the settings ensure that all values will give you access to the Smart 16 IP.

IP auto configuration

Choose between the 3 options.

None – no IP auto configuration. In this case type a static IP address in the appropriate settings below.

DHCP - When selected, Smart 16 IP will contact a DHCP (Dynamic Host Configuration Protocol) server in the local sub-net to obtain a valid IP address,

gateway address and net mask. Before you connect Smart 16 IP to your local sub-net, complete the corresponding configuration of your DHCP server.

BOOTP - When selected, Smart 16 IP will contact a BOOTP (Bootstrap Protocol) server in the local sub-net to obtain a valid IP address, gateway address and net mask.

IP address

Static IP address in the usual dot notation.

Subnet mask

The net mask of the local network.

Gateway IP address

In case the Smart 16 IP should be accessible from networks other than the local one, this IP address must be set to the local network router's IP address.

Primary DNS Server IP address

IP address of the primary Domain Name Server. This may be left empty, however Smart 16 IP won't be able to perform name resolution.

Secondary DNS Server IP address

This address will be used in case the Primary DNS Server can't be contacted.

Primary Time Server

IP address of the primary NTP (Network Time Protocol) compliant timeserver. Smart 16 IP will synchronize its own absolute time with the timeserver's one. This is important for writing log entries and for the Dynamic DNS Service.

Secondary Time Server

This address will be used in case the Primary Time Server can't be contacted.

Remote Console & HTTPS port

Port number at which Smart 16 IP's Remote Console server and HTTPS server are listening. If empty the default value is used.

HTTP port

Port number at which Smart 16 IP's HTTP server is listening. If empty the default value is used.

Telnet port

Port number at which Smart 16 IP's Telnet server is listening. If empty the default value is used.
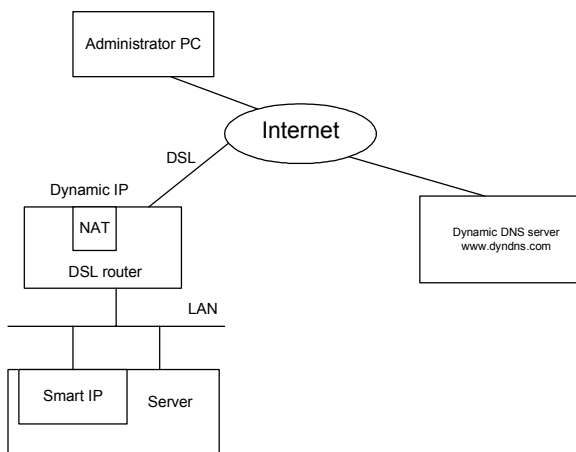
Bandwidth limitation

The maximum network traffic generated through the Smart 16 IP Ethernet device.

Disable Setup Protocol

Exclude the Smart 16 IP from the setup protocol.

30.   Dynamic DNS

Use the free Dynamic DNS service at www.dyndns.org. See Figure 24.

Figure 24 Dynamic DNS scenario

Smart 16 IP is reachable via the IP address of the DSL router, which is dynamically assigned by the provider. Since the administrator doesn't know the IP address assigned by the provider, Smart 16 IP connects to a special dynamic DNS server in regular intervals and registers its IP address there. The administrator can contact this server as well and pick up the same IP address belonging to his card.

The administrator has to register a Smart 16 IP that is supposed to take part in the service with the Dynamic DNS Server. He will get an approved nickname and password in return to the registration process. This account information is needed in order to determine the IP address of the registered Smart 16 IP.

To enable the Dynamic DNS:

1. Ensure the Smart 16 IP LAN interface is properly configured.

2. From the Smart 16 IP menu choose Network Settings / Dynamic DNS. The Dynamic DNS Settings appear. See Figure 25.

Figure 25 Dynamic DNS Settings

3. Check the Enable Dynamic DNS box.

4. Change the settings as desired.

Hostname - The Hostname registered during manual registration with the Dynamic DNS Server. Spaces are not allowed in the Hostname.

Username/Password – Fill in the Username and Password.

Check time - Smart 16 IP card registers itself in the Dynamic DNS server at this time.

Check interval - Interval for reporting again to the Dynamic DNS server by Smart 16 IP.

Smart 16 IP has its own independent real time clock. Ensure the time setting is correct by configuring a timeserver see page 35.

Smart 16 IP registers itself to the Dynamic DNS server slightly different from the time configured. To reduce load peaks on the server we add a random time (0-10 min) to the absolute time value.

31. Serial Port Settings

From the Smart 16 IP Menu choose Serial Port Settings. The Serial Port Settings appear. See Figure 26.

Figure 26 Serial Port Settings

In the Smart 16 IP Serial Settings specify the devices connected to the two Serial ports.

Serial Port 1

The port options are listed below

Configuration login –If this option is checked you can only use the port for the initial configuration and no other function.

Modem - Smart 16 IP has the option of remote access using a telephone line. Connect the modem to Serial 1 port. Using a telephone line means building up a dedicated point-to-point connection from your console computer to the Smart 16 IP. The Smart 16 IP acts as an Internet Service Provider (ISP) to which you can dial in. The connection is established using the Point-to-Point Protocol (PPP).

Before connecting to Smart 16 IP, configure your console computer accordingly. For instance on Windows based operating systems you can configure a dial-up network connection, which defaults to the right settings like PPP.

Serial line speed - Most modems today will support the default value of 115200 bps. For older modems lower the speed.

Modem Init String - Initialization string. The default value works with all modern standard modems connected to a telephone line. For special modems or if connected to a local telephone switch that requires a special dial sequence to connect to the public telephone network, change this setting by giving a new string. See the modem's manual about the AT command syntax.

Modem Server IP address – This address is used only when connecting to Smart 16 IP via a modem. When you dial into the Smart 16 IP the client computer will receive a Modem Client IP address from the Smart 16 IP. Open the Web browser and type Modem server IP address to login to the Smart 16 IP.

The Client IP (see paragraph below) must be in the same class C subnet as the server IP. This subnet should not conflict with the Ethernet subnet on the client side and with the Ethernet subnet on Smart 16 IP Network side.

Modem Client IP address - This address is assigned to your console computer during the PPP handshake. Since it is a point-to-point IP connection virtually every IP address is possible but ensure, it is not interfering with the IP settings of Smart 16 IP and your console computer. The default value will work in most cases.

IPMI over Serial - Check to use this serial port for IPMI 1.5 over serial. See page 47 for more information.

Passthrough access to serial port via Telnet - Connect an arbitrary device to the serial port and access it (assuming it provides terminal support) via telnet. Select the appropriate options for the serial port and use the Telnet Console (see page 42) or a standard telnet client to connect to Smart 16 IP. For more information, see page 19.

External Power Option – When the **External Power Option** is the Sentry Power Tower or Baytec RPC series connected to Serial port 1, configure it by clicking **change external power switch option**. The External Power Option for Serial port 1 window appears.

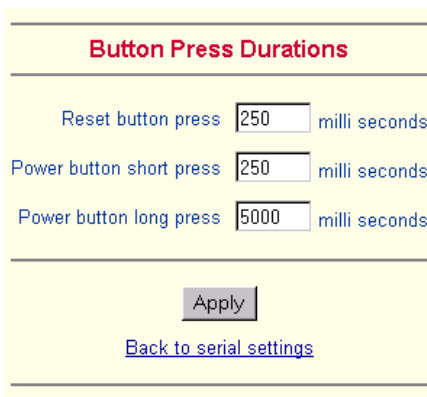Fill in the Username and password as defined by the Sentry Power Tower.

Figure 27 External Power Option for Serial port 1

Serial Port 2

This port provides the power control options, see page 20. Choose a suitable setting and fill in additional required options. Smart 16 IP supports the following:

Internal Power Option - This option gives access to the ATX power and reset functions of a single connected system. You can change the duration of each button press. To do so, click Change button press durations. The box below appears. Adjust the time as desired.

Figure 28 Button Press Durations box

External Power Option

To configure the External Power Option connected to Serial port 2, click **change external power switch option.** The following appears.

External Power Option for Serial Port 2

○ IPM 220-L (Inline Power Module)

○ SPC 800/1600

       Username [   ]

       Password [   ]

○ ePowerSwitch 4-port

◉ ePowerSwitch-Slave

○ Smart Start Jr.

                   Address   Type

      Master Unit [FF] [1x8 ▼]

[More Slave Units]

Figure 29 Serial Port 2 external power option

IPM 220-L (Inline Power Module) - External module option to switch power of a single system by putting it in the power supply line of the controlled system.

SPC 800/1600 - Using the Avocent™ SPC, switch power for more than one system connected to Smart 16 IP through a KVM switch. To use this device enter a username and password, which exist on the SPC and have the privileges to switch power for each port.

ePowerSwitch 4 port - Using this switch, switch power for more than one system connected to Smart 16 IP through a KVM switch.

ePowerSwitch-Slave – This also refers to the **Minicom DX Power Switch S 8 port**. Both switches are cascadable to up to 4 power switches with 8 ports. Smart 16 IP must be connected to the first switch of the cascade via a serial connection.

Smart Start Jr. – Check the box if this option is connected. Add Slave units if required.

32.   Security Settings

From the Smart 16 IP Menu choose Security Settings. The Security Settings appears. See Figure 30.
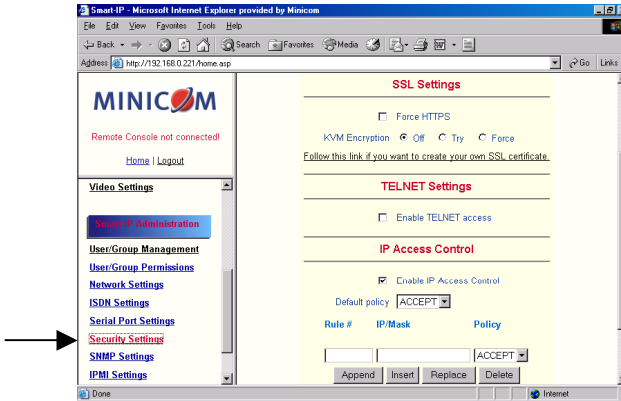
Figure 30 Security Settings

SSL settings

Force HTTPS - Access the Web front-end only using an HTTPS connection. Smart 16 IP won't listen on the HTTP port for incoming connections.

KVM encryption - Controls the encrypting of the RFB protocol, used by the Remote Console to transmit the screen data to the administrator machine and keyboard and mouse data back to the host.

Off - No encrypting used.

Try - Tries to make an encrypted connection. If unsuccessful, an unencrypted connection is used.

Force - Tries to make an encrypted connection.

SSL Certificate Management

Smart 16 IP uses the SSL (Secure Socket Layer) protocol for any encrypted network traffic between itself and a connected client. When connecting, Smart 16 IP reveals its identity to a client using a cryptographic certificate. This is the same for all Smart 16 IPs and won't match the network configurations applied to the card by its user. The certificate's underlying secret key is also used for securing the SSL handshake. Hence, this is a security risk (but better than no encryption at all).

You can generate and install a new certificate unique to a particular card. Smart 16 IP can generate a new cryptographic key and the associated Certificate Signing Request that needs to be certified by a certification authority (CA). A CA verifies you are who you claim to be and signs and issues a SSL certificate to you.

To create and install a Smart 16 IP SSL certificate:

1. From the Security Settings page choose **Create your own SSL certificate**.
The window appears as in Figure 31.

Figure 31 CSR

2. Fill in the fields:

Common name - Network name of Smart 16 IP once installed in the user's
network. It is identical to the name that is used to access the card with a Web
browser. In case the name given here and the actual network name differ, the
browser will pop up a security warning when the card is accessed over HTTPS.

Organizational unit - Specifies which department within an organization Smart
16 IP belongs.

Organization/Locality/City/State/Province - Organization to which Smart 16 IP
belongs + location.

Country - Use the 2 letter ISO code, e.g. DE for Germany.

Challenge Password/Confirm- Some certification authorities require a challenge
password to authorize later changes on the certificate. The minimum is 4
characters.

Email - Of a security contact person that is responsible for Smart 16 IP.

Key length - Length of the generated key in bits. 1024 Bits are supposed be sufficient for most cases. Larger keys may result in slower response time during the connection.

3. Click Create CSR .

4. Press **Download CSR** to download the CSR to your administration machine.

5. Send the CSR to a CA for certification. They will send a new certificate

6. Press **Upload** to upload the certificate to Smart 16 IP. The certificate uploads.

Important! If you destroy the CSR on Smart 16 IP there is no way to get it back! If you deleted it, repeat the above steps.

Telnet Settings

Enable Telnet access - Access over Telnet client. For better security disable Telnet access.

IP Access Control

This is used to limit access to a specific number of clients only. These clients are identified by their IP addresses.

The IP access control settings apply to the LAN interface only!

Enable IP Access Control - Enables access control based on IP source addresses.

Default policy - Controls arriving IP packets that don't match any of the configured rules. They can be accepted or dropped.

ATTENTION: If you set this to DROP and you have no ACCEPT rules configured, access to the Web front-end over LAN is disabled! To enable access, change the security settings via modem dial in or by temporarily disabling IP access control with the initial configuration procedure (see page 4).

Rule # - Type the rule number for which the following commands will apply. This is ignored, when adding a new rule.

IP/Mask - Specifies the IP address or IP address range for which the rule applies.

Numbers attached to an IP address with a `/' is the number of valid bits that are used for the given IP address. Examples:

192.168.0.22 or 192.168.0.22/32 matches the IP Address 192.168.0.22

192.168.0.0/24 matches all IP packets with source addresses from 192.168.0.0 to 192.168.0.255

0.0.0.0/0 matches any IP packet

Policy - Determines what to do with matching packets. They are accepted or dropped.

NOTE: The order of the rules is important. The rules are checked in ascending order until a rule matches. Rules below the matching one are ignored. The default policy applies if no match has been found.

Append a rule – To add a rule to the end of the rule list: Enter the IP/Mask and set the policy. Then press Append .

Insert a rule - To insert a rule according to the rule number: Enter the rule number, IP/Mask and set the policy. Then press Insert . All rules with higher numbers are shifted below.

Replace a rule - Enter the rule number, IP/Mask and set the policy. Then press Replace .

Delete a rule - Enter the rule number and press Delete .

Anti Brute Force Settings

Anti Brute Force Settings lets you block access to a specific user, for a fixed amount of time if a predefined number of unsuccessful login attempts by this user occurred.

Max. number of failed logins – insert a maximum number or leave it blank to disable Anti Brute Force.

Block time - Block time in minutes - insert a number or leave it blank.

To unblock blocked users. Connect to the Smart 16 IP Serial 1 port using terminal software, and type **unblock**. A list of blocked users appears. Select the users to unblock.

33.   SNMP Settings

The following information is available via SNMP:

- Serial number

- Firmware version

- MAC address / IP address / Netmask / Gateway of LAN interface

- Configured users

- Currently active users with login time (login time is only valid if time is synchronized on Smart 16 IP)

- Server's power state

- The following actions can be initiated via SNMP:

- Reset server

- Power on/off server

- Reset Smart 16 IP

The following events are reported by Smart 16 IP via SNMP:

- Login trial at Smart 16 IP failed

- Login trial at Smart 16 IP succeeded

- Denying access to a particular action.

- Server was reset.

- Server was powered on/off

From the Smart 16 IP Menu choose SNMP settings. The SNMP Settings appear. See Figure 32.
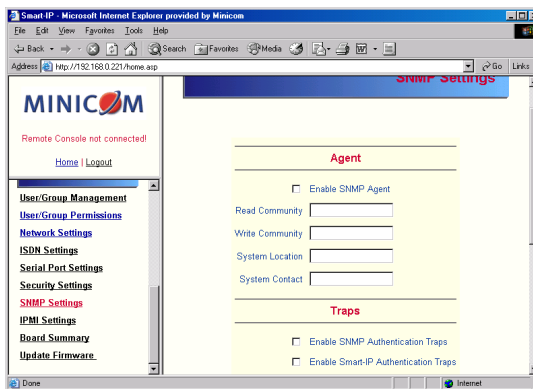

Figure 32 SNMP settings

You can change the following parameters:

Enable SNMP Agent - When checked, Smart 16 IP will answer to SNMP requests. If a community is blank, you cannot perform the request. E.g. if you want to disable the possibility to reset Smart 16 IP via SNMP, don't set a write community.

Read Community - This is the SNMP community, which allows you to retrieve information via SNMP.

Write Community - This community allows you to set options and reset Smart 16 IP or the host via SNMP.

System Location - Type a description of the physical location of the host. This will be used in reply to the SNMP request "sysLocation.0".

System Contact - Type a contact person for the host. This will be used in reply to the SNMP request "sysContact.0".

Enable SNMP Authentication Traps -When checked, an SNMP trap will be sent in case somebody has tried to access Smart 16 IP via SNMP using a wrong SNMP community.

Enable Smart 16 IP Authentication Traps - When checked, an SNMP trap will be sent if somebody tries to login via the Web front-end. Both successful and failed logins trials will be indicated. Furthermore, there will be notification about other security violations like trying to perform an action via Web front-end for which a user has no permission.

Enable Host Traps -When checked, Smart 16 IP will send SNMP traps whenever the host is reset, powered down or powered up.

Trap destinations Enter IP addresses, to which the traps will be sent. For every IP address, set an according community so that your management client can identify the SNMP traps.

After making the entries click Apply .

The Smart 16 IP SNMP MIB

Click the link to access the Smart 16 IP SNMP MIB file. With it, an SNMP client can communicate with Smart 16 IP. Copy the MIB file and import it to the SNMP client software.

34.   IPMI Settings

The Smart 16 IP IPMI (Intelligent Platform Management Interface) is an additional way to power on or off the system or to perform a hard reset. You can also show an event log of the host system and the status of some system sensors (i.e. temperature). If your host system supports IPMI, you can access it in one of the following ways:

- IPMI over Serial

- IPMI over LAN

Both require IPMI V1.5.

From the Smart 16 IP Menu choose IPMI Settings. The IPMI Settings appears. See Figure 33.
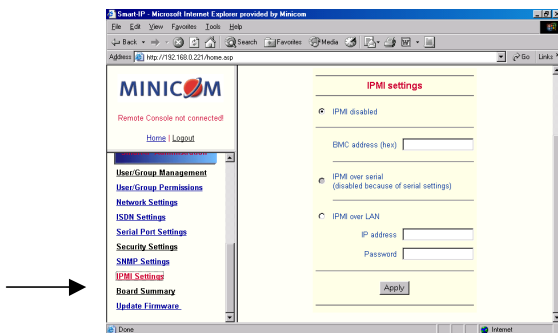

Figure 33 IPMI Settings

IPMI disabled - Disables IPMI. Status via IPMI and Event Log via IPMI are not available and the power on/off and reset functions won't use IPMI.

BMC address - Hexadecimal Baseboard Management Controller address. Needed for all types of communication to the IPMI-interface. Usually you can find this address in the BIOS of the host system. The default and common value is 20.

IPMI over Serial - If your host system supports IPMI V1.5 and has an Intel EMP (Emergency Management Port, usually COM2) connector, you can connect IPMI through serial port 1 on Smart 16 IP. Please note:

- Set the EMP port to Always enable and switch off the Restricted Mode.

- The BMC should accept a null username and a non-null password account as login.

- Passwords are 4 -16 characters long.

- Use a null modem cable for connection

IPMI over LAN - You can connect the IPMI over a LAN connection. You need a host system with IPMI V1.5 and a network adapter with a sideband connection to the BMC (mostly on board). In the IPMI Settings, enter the IP-address of this host system and the correct password for the LAN connection.

You can also access other IPMI systems when you enter their IP address.

35.   LDAP Settings

You can keep authentication information in a central LDAP directory. The purpose of LDAP is simply to confirm the password during login with the LDAP server. The user must exist on both the LDAP and Smart IP 16 side.

On login Smart IP 16 internal user management checks the user. If the user is verified the password is then checked against the LDAP server. If the password is verified the user is logged in and the user rights are taken from Smart IP 16 local user management

From the Smart 16 IP Menu choose LDAP Settings. The LDAP Settings appears. See Figure 34.

Figure 34 LDAP Settings

User LDAP Server - Enter the name or IP address of the LDAP server containing all the user entries. If you use a name, configure a DNS server in the network settings.

Base DN of User LDAP Server - Specify the distinguished name (DN) where the directory tree starts in the user LDAP server.

Type of external LDAP Server - Set the type of the external LDAP server. This is necessary since some server types require special handling. Also the default values for the LDAP schema are set appropriately. Choose between Generic LDAP Server, Novell Directory Service and Microsoft Active Directory. If you don't have Novell Directory Service or Microsoft Active Directory then choose Generic LDAP Server and edit the LDAP schema used (see below).

Name of login-name attribute - Name of the attribute containing the unique login name of a user. To use the default leave this field empty. The default depends on the selected LDAP server type.

Name of user-entry object class - The object class that identifies a user in the LDAP directory. To use the default leave this field empty. The default depends on the selected LDAP server type.

User search subfilter - Refine the search for users that should be known to the Smart 16 IP.

36. Maintenance

From the Smart 16 IP Menu choose Maintenance. The Smart 16 IP Maintenance window appears.

Board Summary - This contains information about the Smart 16 IP and its current firmware.

Updating firmware

You can receive firmware updates by email or download them from the Minicom Web site. Save the firmware file on the client computer.

To update the firmware:

1. Scroll down the Maintenance window. Under Maintenance features click Update Firmware. The Update Firmware window appears. See Figure 35.

Figure 35 Update Firmware window

2. Locate and upload the firmware file from your client system. In case of any errors the upload will be aborted.

   After a smooth upload the Update Firmware panel appears showing the current firmware version number and the uploaded firmware version number.

3. Press the Update button. The firmware updates. Warning! This process is irreversible; ensure the Smart 16 IP's power supply won't be interrupted during the update process, as this may cause damage.

4. When prompted reset Smart 16 IP manually by pressing the Reset Smart-IP button. When pressed all connections to the administration or Remote console close. 30 seconds later, Smart 16 IP runs with the new firmware. You must login again.

**Attention**: Only experienced staff members or administrators should perform a firmware update.

Direct SmartIP Links

You can set up direct links to any Minicom IP hardware over a LAN or WAN. Use the links to directly connect to these IP units without having to remember their IP addresses. You can also see the status of the remote IP units as explained below.

All the IP units must have firmware that supports direct connection functionality. Ensure that firmware of all units is updated to the latest version. See the User Guide of each IP unit to update the firmware.

To set up the direct connections:

1. Scroll down the Maintenance window to Maintenance Features. See Figure 36.
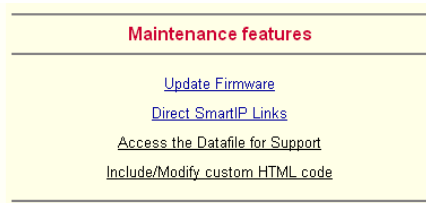

Figure 36 The Maintenance Features

2. Click Direct SmartIP Links. The Direct Connection Links page opens. See Figure 37.

Figure 37 The Direct Connections Links page

3. In the IP address column, type IP addresses of the other Minicom IP units. For up to 16 entries press More entries.

4. In the Device Name column type a description.

5. Click Apply. On the Home page Monitor icons representing the direct connection IP units appear. See Figure 38.
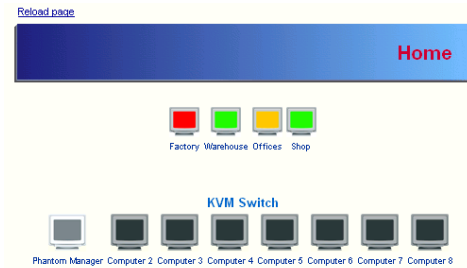
Figure 38 The Monitor icons

The icons are color coded as follows:

Icon	Meaning
Gray	**Powered off or disconnected from the network**
Green	**Powered on but no user is logged in**
Orange	**A user is logged in**
Red	**User is working with the remote console**

Note! If the state of one device changes, there may be a delay of some seconds until icon colors reflect the true situation especially where the network link of this device is going down.

To connect to an IP unit:

Click the desired icon on the Home page. The Login page of that IP unit appears.

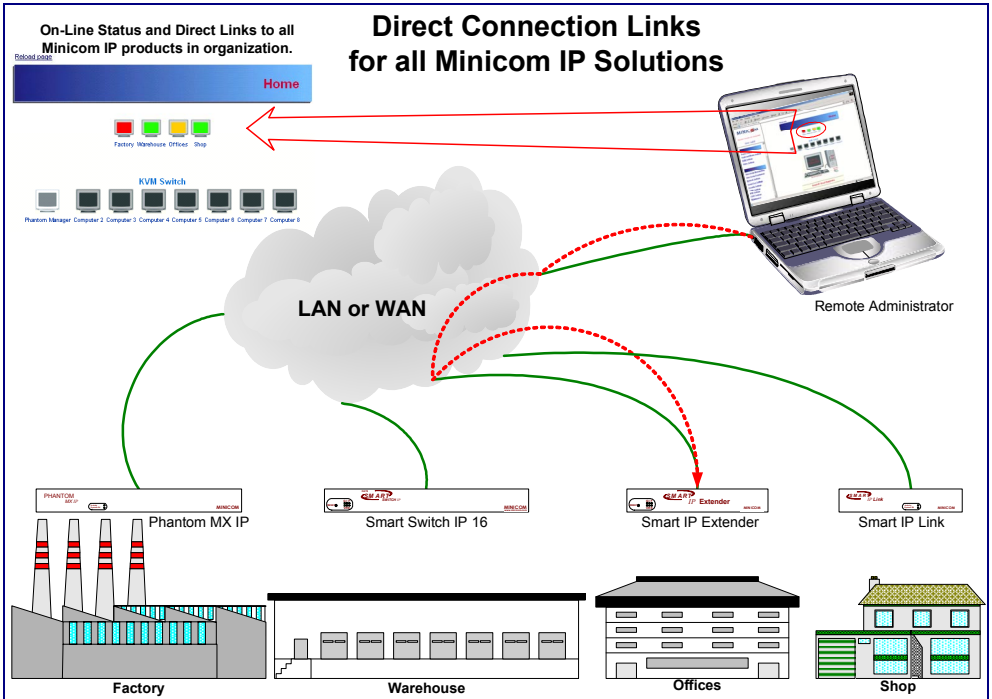Figure 39 below illustrates a direct connections link scenario.

Figure 39 Direct connections link scenario

Access the Datafile for support

Click the link to access the Smart 16 IP data file. The file contains support information, which will help us to troubleshoot your problem.

Include/modify custom HTML code

You can modify the HTML code of the Home page to include customized graphics and text. You can't save graphics on the Smart 16 IP therefore the graphics should be accessible on the Network. Define Primary and secondary DNS in the Network settings if needed.

37.   Frequently Asked Questions

Q 1: The remote mouse doesn't work or is not synchronized.

A: Ensure the Smart 16 IP mouse settings match the mouse model. Also see page 14

Q 2: Bad video quality or grainy picture

A: Use the brightness and contrast settings - see page 13. Use the auto adjustment feature to correct a flickering video.

Q 3: Login fails.

A: Was the correct user and password given? On delivery, the user "super" has the password "smart". Configure your browser to accept cookies.

Q 4: I use the Mozilla Browser 0.9.x., Netscape 6.x and https (secure http). When opening the Remote Console applet loading fails with Bad Magic Number Exception.

A: This is a bug in older versions of Mozilla. Don't use https, or upgrade your Browser.

Q 5: The Remote Console window can't connect to Smart 16 IP.

A: Maybe a firewall prevents access to the Remote Console. Ensure the TCP port numbers 443 or 80 are open for incoming TCP connections.

Q 6: Cannot connect to Smart 16 IP.

A: Check if the network connection is working (ping the IP address of Smart 16 IP). If not, check network hardware. Is Smart 16 IP powered on? Check if the IP address of Smart 16 IP and all other IP related settings are correct. Also verify that all the IP infrastructure of your LAN, like routers are correctly configured. Without a ping functioning, Smart 16 IP can't work.

Q 7: Special key combinations, e.g. ALT+F2, ALT+F3 are intercepted by the console system and not transmitted to the host.

A: Define a so-called 'Button Key' in the Remote Console settings.

Q 8: In the browser the Smart 16 IP pages are inconsistent or chaotic.

A: Ensure your browser cache settings are feasible, and are not set to something like "never check for newer pages". Otherwise Smart 16 IP pages may be loaded from your browser cache and not from the card.

Q 9: Windows XP doesn't awake from standby mode

A: This is possibly a Windows XP problem. Try not to move the mouse while XP goes into standby mode.

38. Glossary of terms

ACPI - A specification that enables the operating system to implement power management and system configuration.

ATX - Advanced Technology Extended: A particular specification of a motherboard introduced by Intel in 1995.

BMC - Board Management Controller: implements the IPMI based main board management functions.

DHCP - Dynamic Host Configuration Protocol: protocol for dynamically assigning IP configurations in local networks.

DNS - Domain Name System: protocol used to locate computers on the Internet by their name.

EMP - Emergency Management Port: provides remote emergency access and control of server resources. EMP offers operating system independent, fundamental remote management access regardless of the server's current state or network availability.

HTTP - Hypertext Transfer Protocol: the protocol used between web browsers and servers.

HTTPS - Hyper Text Transfer Protocol Secure: secure version of HTTP.

IPMI - Intelligent Platform Management Interface

MIB - Management Information Base: describes the structure of the management information that can be accessed via SNMP.

SNMP - Simple Network Management Protocol: a widely used network monitoring and control protocol.

SSL - Secure Socket Layer: encryption technology for the Internet used to provide secured data transmissions.

SVGA - Super VGA: A refinement of Video Graphics Array (VGA) that provides increased pitch and resolution performance.

Section 2: Operating the Smart 16 IP system locally

This section explains how to operate the Smart 16 IP Switching system locally through the On Screen Display (OSD) or Control software.

39.   Switching between computers

Switch between the connected computers by either:

- Keyboard hotkeys
- The OSD (On Screen Display)
- Control software

The OSD / Control software is also the place to adjust various settings as explained below.

40.   The keyboard hotkeys

To switch to the next computer forwards press **Shift** then, +. Release **Shift**, before pressing +.

To switch to the next computer backwards press **Shift** then, -. Release **Shift**, before pressing -.

Note! With a US English keyboard you can use the **+** key of the alphanumeric section or of the numeric keypad. With a Non-US English keyboard only use the + key of the numeric keypad.

41.   The OSD

To display the OSD:

Press **Shift** twice. The OSD Main window appears. See

Figure 40. Lines with blue text show active computers. Lines with grey text show inactive computers. The Type column indicates whether a computer "C" or another switch "S" is connected to the port.

Figure 40 The OSD Main window

42. Navigating the OSD

To navigate up and down use the Up and Down arrow keys.

To jump from one column to the next (when relevant) use the Tab key.

To exit the OSD or return to a previous window within the OSD press **Esc**.

43. Selecting a computer

To select a computer:

1. Navigate to the desired computer line.

2. Press **Enter**. The selected computer is accessed. A Confirmation label appears showing which computer is accessed.

Note! When the OSD is displayed you cannot select computers using the keyboard hotkeys.

44. The OSD settings - F2

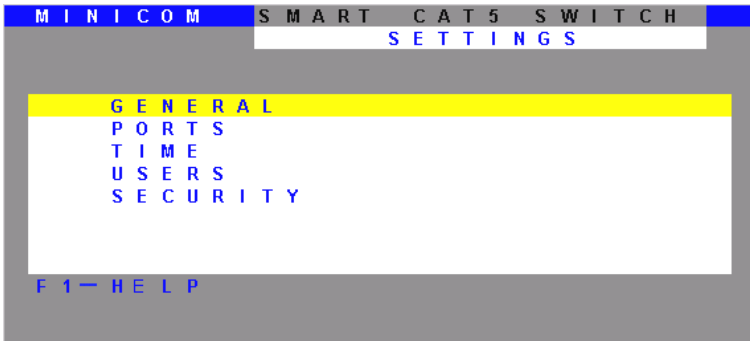Press **F2**. The OSD Settings window appears see Figure 41.

Figure 41 The Settings window

Note! When the OSD is password protected (explained below) only the Administrator has access to the F2 settings window.

45. The General settings

With the blue line on the word GENERAL, press **Enter**. The General settings window appears see Figure 42.
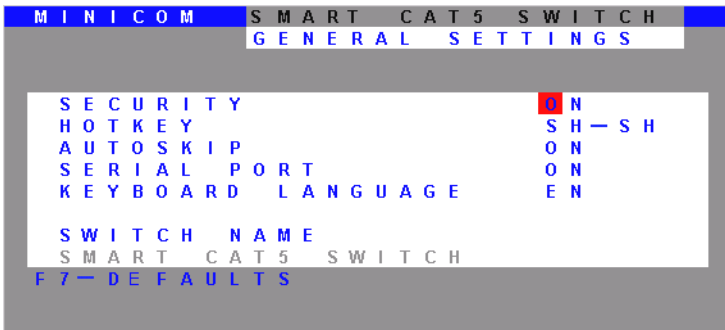

Figure 42 The General Settings window

From this window you can do the following:

Security

The OSD comes with an advanced password security system that contains 3 different security levels. Each security level has different access rights to the system.

These levels are as follows:

Administrator (Status A)

The Administrator can:

- Set and modify all Passwords and security profiles
- Fully access any computer
- Use all OSD functions

Supervisor (Status S)

The Supervisor can:

- Fully access any computer
- Access the following OSD functions only –**F4** Scan, **F5** Tune and **F6** Moving the Confirmation label.

User (Status U)

There are 6 different Users in the Smart 16 IP system. Each User has a Profile set by the Administrator that defines the access level to different computers. There are 3 different access levels, these are explained on page 63.

Activating password protection

By default OSD access is not password protected. Only the Administrator can password-protect the OSD or disable password protection.

To do so:

1. In the General settings window navigate to the Security line.
2. Press the Space bar to toggle between Security On and Off. The password box appears.
3. Type the Administrator's password (default is "admin").
4. Press **Enter**. The new security status is set.

Changing the OSD hotkey

By pressing **Shift**, **Shift** the OSD appears. You can replace **Shift**, **Shift** with any of the following:

- Ctrl, Ctrl
- Ctrl, F11
- Print Screen

To change the hotkey:

1. Navigate to the Hotkey line.

2. Press the Space bar to toggle between options. To display the OSD in future press the new hotkey.

Autoskip

With the Autoskip feature, the arrow keys only access the active computer lines on the OSD. When Autoskip is Off, The arrow keys access both active and inactive computer lines.

To change the Autoskip setting:

1. Navigate to the Autoskip line.

2. Toggle between the options using the Space bar.

Serial port

The Serial port is used for the Control Management program. Serial port On means the program can be used.

To change the Serial port setting:

1. Navigate to the Serial port line.

2. Toggle between the options using the Space bar.

Changing the Keyboard language

The keyboard is preset to US English, this can be changed to French (FR) or German (DE), as follows:

1. Navigate to the Keyboard language line.

2. Toggle between the options using the Space bar.

Editing the Switch name

You can substitute up to 18 characters in the line. A space constitutes a character. When there is more than one switch in the system give each Switch's OSD a different name.

46.   F7 Defaults

Press F7 to return the OSD to the factory default settings. Note! All changes made will be removed.

47.   The Ports settings

In the Settings window navigate to the Ports line and press **Enter**. The Ports settings window appears see Figure 43.

Figure 43 Ports Settings window

Editing the computer name

In this window you can edit the computer names with up to 15 characters.

To erase a character:

Select it and press the **Space bar**. Blank spaces remain in place of the erased character.

To erase an entire line:

Place the cursor at the beginning of the line. Keep the **Space bar** depressed until the line is erased.

Keyboard (KB)

The Smart 16 IP operates with Windows, Linux, HP UX, Alpha UNIX SGI, DOS, Novell, MAC-USB or Open VMS.

By default the keyboard mode is set to PS for Intel based computers.

For the other systems set the KB column as follows:

- U1 for HP UX
- U2 for Alpha UNIX, SGI, Open VMS
- U3 for IBM AIX

To change the setting:

1. On the desired line, press Tab to jump to the KB column.

2. Toggle between the options using the Space bar.

Adding/changing a hotkey (HKEY)

Cascade the Smart 16 IP by connecting another Smart Switch to a Computer port instead of a computer, and then connecting more RICCs to the second Switch.

You must define a different hotkey for the OSD of each Switch. The hotkeys can be any of the choices as set out above on page 59. Use the hotkey when you select the Switch's port in the first level OSD – the second level's OSD then appears.

To add/change a hotkey:

1. On the line to which the Switch is connected, press Tab to jump to the HKEY column.

2. Toggle between the options using the Space bar.

48. The Time settings

In the Settings window navigate to the Time line and press **Enter**. The Time settings window appears see Figure 44.

Figure 44 Time settings window

Scan (SCN) - Label (LBL) - Time out (T/O)

SCN - In the **SCN** column, change the scan period.

LBL - In the **LBL** column, change the display period of the Confirmation label showing which computer is currently accessed.

T/O - When password protection is activated you can automatically disable the Management keyboard, mouse and screen after a preset time of non-use. Set this Timeout period in the **T/O** column.

To set the above periods:

1. On the desired line press Tab to jump to the desired column.

2. Place the cursor over one of the 3 digits and type a new number. Enter a leading zero where necessary. For example, type 040 for 40 seconds.

   Typing 999 in the **LBL** column displays the label continuously. Typing 000 – the label will not appear.

   Typing 999 in the **T/O** column disables the Timeout function. Typing 000 – the Timeout function works immediately.

   Typing 999 in the **SCN** column displays the screen for 999 seconds. Typing 000 – the computer screen is skipped.

49.   Users

In the Settings window navigate to the Users line and press **Enter**. The Users settings window appears see Figure 45.

Figure 45 The Users settings window

There are 3 different access levels. These are:

- Y – Full access to a particular computer.

- V –Viewing access only, to a particular computer (No keyboard/mouse functionality)

- N – No access to a particular computer – A TIMEOUT label appears if access is attempted

To give each user the desired access level:

1. Navigate to the desired computer line and User column.

2. Toggle between the options using the Space bar.

50.   Security

In the Settings window navigate to the Security line and press **Enter**. The Security settings window appears see Figure 46.

Figure 46 The Security settings window

The 'T' column on the right hand side stands for Type of password.

There can only be 1 Administrator password, 1 Supervisor password, and 6 User passwords.

To change a user name or password:

1. Navigate to the desired line and column.

2. Type a new user name / password. User authentication is done solely via the password there is no security significance to the names.

By default the User Profile settings are full access.

51.   The OSD HELP window – F1

To access the HELP window press F1. The HELP window appears, see Figure 47.

Figure 47 The HELP window

Please note! All the functions set out in the Help window are performed from the Main window. The Help window is merely a reminder of the hotkeys and their functions.

52.   Scanning computers – F4

Where necessary adjust the scan time in the Time Settings window, see above.

To activate scanning:

1. Press **Shift** twice to open the OSD.

2. Press **F4**. Your screen displays each active computer sequentially, with the Scan label appearing in the top left corner.

To deactivate scanning:

Press **F4**.

53.   Tuning – F5

You can tune the image of any computer screen from the Select Computer window.

To adjust the screen image:

1. Navigate to the computer you wish to adjust.

2. Press **F5**. The screen image of the selected computer appears, together with the Image Tuning label.

3. Adjust the image by using the **Right** and **Left** Arrow keys.

4. When the image is satisfactory, press **Esc**.

Note! Picture quality is relative to distance. The further away a remote computer is from the Smart 16 IP, the lower the image quality, and the more tuning needed. So place the higher resolution computers closer to the Switch.

54.   Moving the label – F6

Position the Confirmation label anywhere on the screen.

To position the label from the Main window:

1. Navigate to the desired computer using the **Up** and **Down** arrow keys.

2. Press **F6**. The selected screen image and Identification label will appear.

3. Use the arrow keys to move the label to the desired position.

4. Press **Esc** to save and exit.

55. Using the Control software

As an alternative to the OSD operate the system with the Control software located on the Marketing & Documentation CD. With the OSD you operate the system and view the computer screens on the same monitor. The Control software requires 2 monitors: 1 for the software and 1 to view the computer screens.

With the Control software you can:

- View computers
- Edit OSD settings
- Save configurations for future use
- Read configurations from and write configurations to the Smart 16 IP Switch

Control software system requirements

- Pentium 166 or higher computer
- 16Mb RAM
- Windows 98 and later
- Free Serial port

Connecting the RS232 Serial cable

To run the software, connect the RS232 Serial cable to the computer containing the software, and to the Smart Switch. See the Installation Guide.

Installing and running the Control software

Note! The system must be fully connected **BEFORE** running the Control software. Failure to first connect the system will lead to the software working in demo mode.

To install the software:

1. Insert and start the Marketing & Documentation CD.
2. Choose Smart CAT5 Switch Softpack. The Smart CAT5 Switch Softpack window appears.
3. Choose **Install Smart CAT5 RS232 Control Software**. Once installed, a

    shortcut icon appears on the Desktop .

4. Double-click the icon to run the software. Or choose Start / Programs / Smart CAT5 RS232 Control / Smart CAT5 RS232 Control.

To run the software from the CD:

Choose Run Smart CAT5 switch RS232 Control Software from CD.

Selecting a Com port

During the Setup process you will be prompted to choose a Com port. Choose the Com port to which the RS232 Serial cable is connected. Failure to select the correct Com port will result in the software running in demo mode.

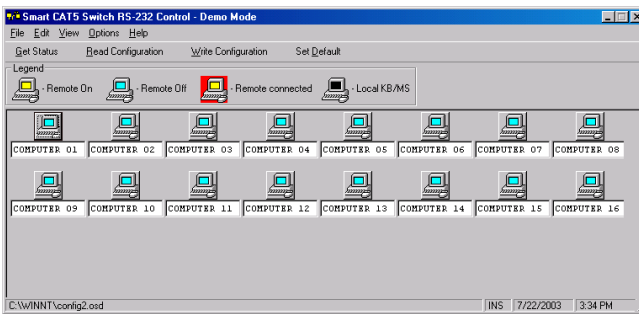Once Setup is complete the Control window appears. See the figure below.

Figure 48 The Control window

Computer icons

Icon	Meaning
	Computer is connected and switched on
	Computer is switched off or unconnected
	Computer that you are presently connected to
	Connected and switched on computer with a Local Workstation attached and presently being used locally. After remaining idle for the Timeout period, it changes to **yellow**.

When you first open the Control window the software automatically gets the status of the system, including the security access settings.

Communication Error

If a Communication Error box appears when trying to scan the system – see Figure 49.

Check that:

- The RS232 Serial cable is connected to the computer's and Smart 16 IP Manager's serial ports.

- The Com Port settings in **Options** / **Com Port** are set correctly. After changing the Com port exit and re-enter the Control software.
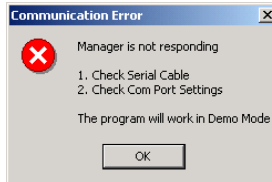

Figure 49 Communication Error

The View menu

From the **View** menu choose to display:

- All computers, or only active switched on computers.

- The Legend

- The toolbar

Selecting a computer

To select a computer:

Click on the computers icon. The system switches to that computer. The

connected icon appears with a red background . Control and monitor the selected computer from the keyboard and mouse connected to the Smart Switch.

The toolbar buttons

The toolbar buttons are explained below.

Get Status

If for whatever reason there is a break in communication between the Control software and the system, click Get Status to get the current status of the

computers in system. The system automatically updates the status before every switching.

Read Configuration

To see the current settings of the entire system (names, scan settings etc.) click Read Configuration . All current settings are received. You view the computer settings from the Control window and other settings from the **Edit** menu – discussed below.

Write Configuration

With the Control software you can make changes to all OSD settings. You can then save these configurations in a file to use in the future by selecting **Save** or **Save As** from the **File** menu.

Note! Save or Save As will have no affect on the OSD.

To change the OSD settings you must press Write Configuration or choose Write Configuration from the **File** menu after making changes. The changes will then be sent to the Smart system Manager, and the OSD will reflect these changes.

Renaming a computer

To rename a computer:

1. Type the new name in the box below the computer icon.

2. Click Write Configuration to send the new name to the system.

Or click **Save** or **Save As** from the **File** menu to save the change in a file and not alter the OSD names.

The Edit menu

You can edit all OSD fields. Edit the following from the Edit menu.

- Logo
- Passwords
- Settings

Logo and Passwords

You can edit the logo that appears at the top of the OSD window. You can also edit the names and passwords for the Administrator, Supervisor and 6 Users.

1. Edit the Logo and Passwords by choosing them from the Edit menu. See figures below.
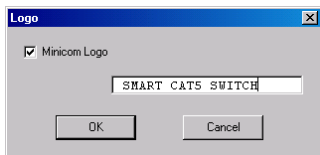

Figure 50 The logo

Figure 51 The names and passwords

2. Make the desired changes.

3. Click **OK**.

Settings

Choose Settings from the Edit menu. The Computers' Properties box appears. See Figure 52.
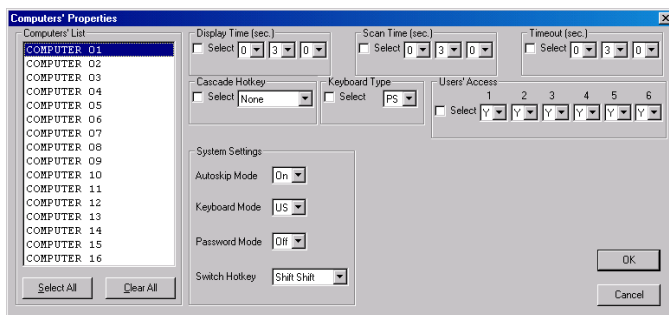
Figure 52 The Computers' Properties box

Here you can edit all the data that can be edited in the OSD. This includes:

Scan times, Timeout, Confirmation label display time, Keyboard type/mode, User access, Password mode, Autoskip mode, and Switch/System hotkey. These features are explained in the OSD section above.

To edit a setting:

1. In the Computer List, select the desired computer or group of computers.

2. Make the desired changes.

3. Check the Select box next to the changed setting.

4. Click **OK**.

Single computer settings

To see all the settings of a single computer, right click the computer icon. The settings appear as in the figure below.

Note! There is no Select box to check.
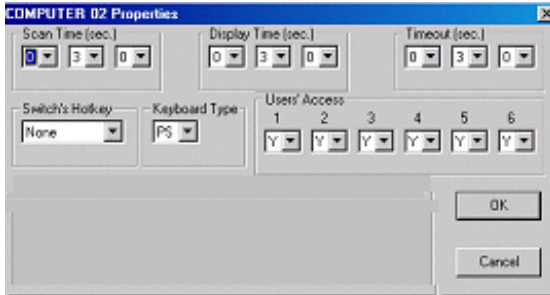
Figure 53 The single computer Settings box

Loading a saved configuration

To load a saved configuration:

From the **File** menu choose **Open**.

Reminder!

All changes done with the Control software are only reflected in the OSD **AFTER** pressing Write Configuration .

The factory default settings

To revert to the factory default settings:

On the toolbar press Set Default .

There is no need to press Write Configuration .

Password protection

When the Smart system is password protected, the Control software behaves in exactly the same way as the OSD. You must type in the required password to access the Control software. The access you gain depends on the security status – exactly as with the OSD.

To change the security access, close and reopen the Control software, and type in the different password.

Administrator (Status A)

The Administrator can:

- Set and modify all Passwords and security profiles
- Fully access any computer
- Use all functions

Supervisor (Status S)

The Supervisor can:

- Fully access any computer
- Scan computers.

User (Status U)

There are 6 different Users in the Smart 16 IP system. Each User has a Profile that defines the access level to different computers. There are 3 different access levels. These are:

- Y – Full access to a particular computer
- V –Viewing access only, to a particular computer (No keyboard/mouse functionality)
- N – No access to a particular computer

The Administrator defines the desired access levels of each User Profile. This is done in the Setting box. By default the User Profile settings are full access.

56.   Upgrading the Smart 16 IP firmware

With the Smart CAT5 Switch Update software program you can upgrade the firmware for the:

- OSD
- Manager
- RICCs

The Update software enables you to add new features and fix bugs in a quick and efficient manner. Install the Update software on any computer, even one not part of the Smart 16 IP system.

The software and latest firmware is on the Marketing & Documentation CD. To obtain the latest firmware for your system go to www.minicom.com .

System requirements for the Update software

- Pentium 166 or higher with 16 MB RAM and 10 MB free Hard Drive space.
- Free Serial port.
- Windows 98, 2000, ME, XP or Windows NT 4.0 SP (service pack) 3 or later, Windows 2003 Server.

Connecting the Smart 16 IP System

To update the firmware the Smart 16 IP system must be connected and switched on.

Connecting the RS232 Serial cable

To run the software, connect the RS232 Serial cable to the computer containing the software, and to the Smart 16 IP Switch. See the Installation Guide.

Installing the software

To install the Update software:

1. Insert the Marketing & Documentation CD. The CD menu runs automatically.
2. Choose Smart CAT5 Switch Softpack.
3. Either run the Update software straight from the CD or install it on the computer's hard drive and run it from there.

Starting and configuring the Update software

1. Start the Update software. The Smart CAT5 Switch Update window appears. See Figure 54.
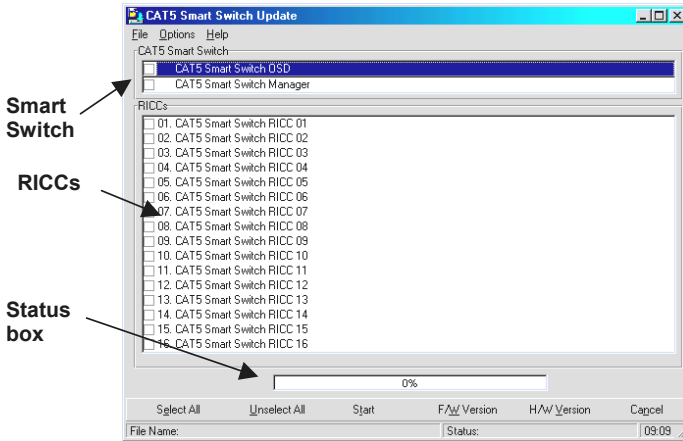
Figure 54 The Smart CAT5 Switch Update window

The table below explains the functions of the buttons and boxes in the Update window.

Button or Box	Function
Select All	Selects all RICCs
Unselect All	Unselects selected RICCs
Start	Starts firmware download
F/W Version	Displays the firmware version number
H/W Version	Displays the hardware version number
Cancel	Cancels selected function
10:06	System time
Status:	Displays download status
File Name:	Name of Update file

2. From the Options menu choose Com Port. The Com Port box appears. See Figure 55.
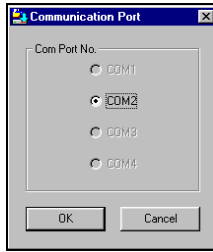
Figure 55 The Com Option box

3. Choose an available Com Port and click OK.

Note! The RS232 Serial cable must be connected to the selected Serial port.

Verifying the version numbers

Before upgrading the firmware, you must first verify which firmware and hardware versions you have.

The OSD version number

To verify the OSD version number:

1. Open the Smart CAT5 Switch Update program.

2. In the **Switch Unit** box, check the OSD option. See Figure 54.

3. Click F/W Version . The version number appears in the **Switch** box.

The H/W Version button is grayed out, as there is no hardware relevant to the OSD.

The Smart 16 IP Manager version number

To verify the Smart 16 IP version number:

1. Open the Smart CAT5 Switch Update program.

2. In the **Switch Unit** box, check the **Smart Switch Manager** option**.**

3. Click F/W Version . The firmware version number appears in the **Switch Unit** box.

4. Click H/W Version . The hardware version number appears in the **Switch Unit** box.

Verifying the RICC version number

Before you can check a RICC, you must uncheck the **Switch Unit** box options.

To verify the RICC version number:

1. Open the Smart CAT5 Switch Update program.

2. Check one or more or all of the RICCs.

3. Click F/W Version . The firmware version number appears after the RICC number.

4. Click H/W Version . The hardware version number appears after the RICC number.

When "**Not responding**" appears, there is no computer connected, or it is switched off.

Obtaining new firmware

Download the latest firmware for your system from www.minicom.com

Updating the firmware

Warning!

Never switch off any computer connected to the Smart 16 IP system during the updating process.

To update the firmware:

1. Open the Smart CAT5 Switch Update program.

2. In the Smart CAT5 Switch Update window, check the appropriate option in the **Switch Unit** box or the desired RICC.

3. From the **File** menu, choose **Open**. The **Open** box appears. See Figure 56.

4. Navigate to the folder that contains the firmware update file. You may only see the files that match the file selection mask.
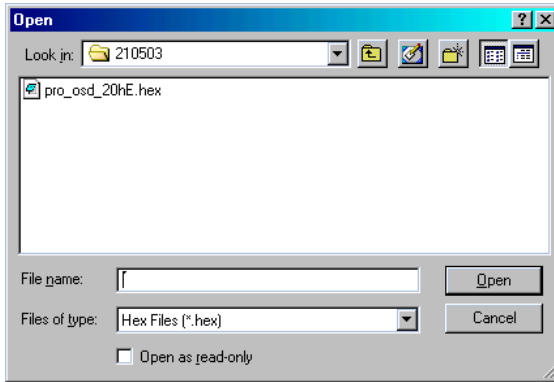
Figure 56 The Open box

5. Open the file.

6. Click **Start**. The Smart CAT5 Switch Update flashes the firmware. On completion the firmware version number appears.

7. Check that the updated version number is correct by pressing
   F/W Version
   .

Firmware Update generates one log file per session that displays a chronological list of actions. You can read the log file in any ASCII text editor. The log file is located in the Windows directory.

Reset

Reset the software for the Smart 16 IP Manager or RICCs when for example the unit hangs or when the mouse fails to work properly. Resetting is done via the Serial port, and avoids the need to shut down the computer.

NOTE! The Reset function does not affect the parameters of the unit settings.

Resetting the Switch or RICC units

To reset the Switch or RICC units:

1. For the Switch, check the Smart Switch Manager option in the **Switch Unit** box.

   For the RICCs, check one or more RICCs in the **RICC Units** box.

2. From the Options menu choose **Advanced** / **Reset**. The units reset. The system should now be operational.

Troubleshooting tips

When using Firmware Update software you may sometimes get a Communication Error message.

When updating a unit and a Communication Error message appears, do the following:

1. Check that the RS232 Serial cable's RS232 connector is connected to the Switch's Communication port.

2. Check that the RS232 Serial cable's DB9F connector is connected to the DB9M Serial port on the CPU's rear panel.

3. Restart the download process.

Electricity failure

When the electricity fails while updating the Smart 16 IP firmware, do the following:

If the electricity fails during the firmware update of the Switch, a **Communication Error** message appears. Simply resume the firmware update by opening the folder that contains the firmware update file and continue from there.

If the electricity fails during the firmware update of the RICCs a **Not Responding** or **Upgrade Error** message appears. Restart the upgrade from the beginning.

Appendix A: Smart 16 IP Video modes

The Smart 16 IP supports the following video modes. Do not use other custom video settings.

Resolution	Refresh rates (Hz)
640x350	70, 85
640x400	56, 70, 85
640x480	60, 67, 72, 75, 85, 90, 100, 120
720x400	70, 85
800x600	56, 60, 70, 72, 75, 85, 90, 100
832x624	75
1024x768	60, 70, 72, 75, 85, 90, 100
1152x864	75
1152x870	75
1152x900	66, 76
1280x960	60
1280x1024	60, 75
1600x1200	60

Appendix B: Key codes

Figure 57 illustrates the keys on a standard 104 key PC keyboard with a US English language mapping. These keys are used to define keystrokes or hotkeys for several Smart 16 IP functions. The keys may not represent keys used on international keyboards. Most modifier keys and other alphanumeric keys are in identical positions, whichever language mapping you are using.

Figure 57 US English keyboard layout

The table below lists keys that that have 2 ways of being written (Alternative) and also keys that are written in a different way to that which appears on the actual keyboard key (Key code).

Key	Key code	Alternative
~	~	TILDE
-	-	MINUS
=	=	EQUALS
<	<	LESS
/	/	SLASH
Bksp	BACK_SPACE	
Tab	TAB	
CR	ENTER	
Caps	CAPS_LOCK	
\	\	BACK_SLASH
Lshft	LSHIFT	SHIFT
Lctrl	LCTRL	CTRL
Win	WINDOWS	
Alt	LALT	ALT
AltGR	ATGR	
Esc	ESCAPE	ESC
Psc	PRINTSCREEN	

Key	Key code	Alternative
Scrl	SCROLL_LOCK	
Brk	BREAK	
Ins	INSERT	
Pos1	HOME	
Pup	PAGE_UP	
Del	DELETE	
Pdn	PAGE_DOWN	
↑	UP	
←	LEFT	
↓	DOWN	
→	RIGHT	

The numerical keypad codes

Key	Key code	Alternative
num	NUM_LOCK	
0	NUMPAD0	
1	NUMPAD1	
2	NUMPAD2	
3	NUMPAD3	
4	NUMPAD4	
5	NUMPAD5	
6	NUMPAD6	
7	NUMPAD7	
8	NUMPAD8	
9	NUMPAD9	
+	NUMPADPLUS	NUMPAD_PLUS
/	NUMPAD/	
*	NUMPADMUL	NUMPAD_MUL
-	NUMPADMINUS	NUMPAD_MINUS
CR	NUMPADENTER	

Appendix C: Disabling mouse acceleration

The following steps describe how to disable mouse acceleration in a number of different Operating Systems.

Windows 98 and Windows ME

1. From the Control Panel, click the Mouse icon.
2. From the Mouse Properties dialog box, click the Pointer Options tab.
3. Center the Pointer Speed slider bar
4. Click the Accelerate… button.
5. Deselect Pointer acceleration option.

Windows 98 SE and Windows NT4

1. From the Control Panel, click the Mouse icon.
2. From the Mouse Properties dialog box, click the Motion tab.
3. Set the Pointer speed slider bar completely to the left.

When a Microsoft Intellimouse driver is installed on Windows 98, Windows ME or Windows NT4

1. From the Control Panel, click the Mouse icon
2. From the Mouse Properties dialog box, click the Pointer Option tab
3. Center the Pointer Speed slider bar.
4. Click Advanced… button.
5. Deselect Enable pointer acceleration option

NetWare 6 servers running Java 1.4.1:

1. From the NetWare 6 Graphical User Interface (GUI) Environment tool Input tab, select Turn off mouse acceleration.
2. Click Apply and restart the GUI.

NetWare 6 servers running Java 1.3.1 CSP8 or CSP9:

1. Add the following command to the NetWare 6 sys:/java/nwgfx/xinitrc file:

xset m 1

2. Save the file and restart the GUI.

Linux

1. Execute the following command line parameter:

xset 0 255

2. Or-

xset m 0

Appendix D: USB SUN Combo keys

The connected PS/2 keyboard does not have a special SUN keypad to perform special functions in the SUN Operating System environment. So when a RICC USB or SUN is connected to a SUN computer, the RICC emulates these SUN keys using a set of key combinations called Combo keys. See the table below.

SUN key	Combo key
Stop	Left **Ctrl** + **Alt** + **F1**
Props	Left **Ctrl** + **Alt** + **F3**
Front	Left **Ctrl** + **Alt** + **F5**
Open	Left **Ctrl** + **Alt** +**F7**
Find	Left **Ctrl** +**Alt** + **F9**
Again	Left **Ctrl** + **Alt** + **F2**
Undo	Left **Ctrl** + **Alt** + **F4**
Copy	Left **Ctrl** + **Alt** + **F6**
Paste	Left **Ctrl** + **Alt** + **F8**
Cut	Left **Ctrl** + **Alt** + **F10**
Help	Left **Ctrl** + **Alt** + **F11**
Compose	Application key or Left **Ctrl** + **Alt** + Keypad ∗
Crescent	**Scroll Lock**
Volume Up	Left **Ctrl** + **Alt** + Keypad −
Volume Down	Left **Ctrl** + **Alt** + Keypad +
Mute	Left **Ctrl** + **Alt** + **F12**
Sun Left ◊ key	Left **Windows** key
Sun Right ◊ key	Right **Windows** key
Alt-Graph	Right **Alt** or **Alt Gr**
Stop A	Left **Ctrl** + **Alt** +1