Phantom MX IP

Operating Guide

Table of Contents

1. Numbering the Specters

After connecting the system, switch on the UPM and MX IP and then the computer(s).

You must give each Phantom Specter an ID number. The Auto numbering process through the Phantom OSD gives each Phantom Specter a sequential ID number.

For Auto numbering to work properly **ALL** connected computers **MUST** be switched on

To perform Auto numbering:

1. At the keyboard connected to the MX IP press **Shift Shift**. The OSD appears, see Figure 1.
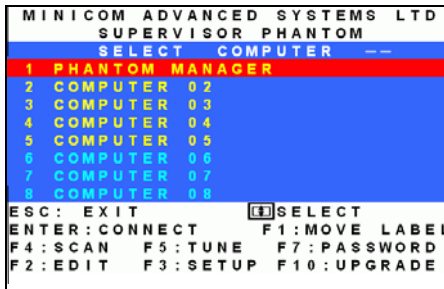
Figure 1 The Phantom OSD

2. Press **F7**. The Enter Password box appears. See Figure 2.

Figure 2 The Enter Password box

3. Type the default Administrators password ADMIN and press **Enter**. The Password window appears.
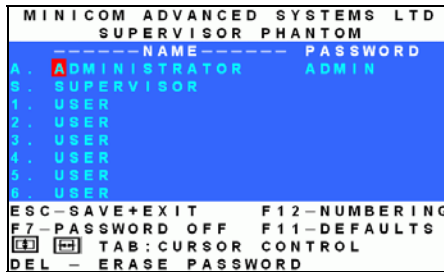
Figure 3 The Password window

4. Press **F12** to activate Auto numbering. A Confirmation label appears.

5. Press **Y** to confirm. The process activates. Wait until the process is complete.

6. Press **Esc** twice to save and exit the OSD.

Operating the Switching system through the OSD or Control software through the MX IP or UPM is explained in Appendix D.

The sections below explain how to configure and operate the MX IP system over IP.

2. Configuring the MX IP system

The MX IP's communication interfaces are based on TCP/IP, and it comes configured with the values listed below.

- DHCP - active

- IP address - 192.168.0.220

- 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:

3. Configuration via DHCP server

By default, MX IP will try to contact a DHCP server in the subnet to which it is physically connected. If a DHCP server is found it may provide a valid IP address, gateway address and net mask. Before connecting the MX 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 MX IP. You can find the MAC address on the outside of the shipping box and also labeled on MX IP's underside. If the DHCP connection fails on boot up, MX 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.

OPERATING GUIDE

4. Configuration via local console

There are two ways of doing this:

(A) Connect the NULL modem cable to the computer and to MX IP's Serial 1 port. Use any Terminal software to connect to MX 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 4.

3. Fill in the connection details. Select the Serial port to which the Null Modem cable is connected in the Connect using: box and click OK. The COM 1 properties box appears. See Figure 5.

Figure 4 Connect To box
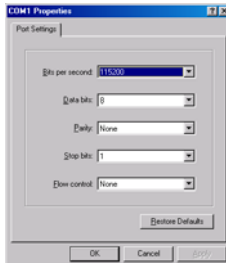
Figure 5 COM 1 Properties box

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 6.
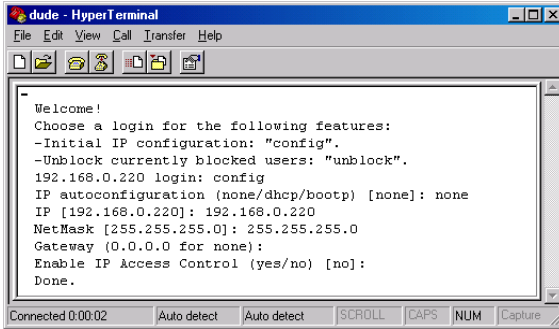
Figure 6 The Hyperterminal

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

7. Type **config** and press **Enter**. Configuration questions appear. DHCP must be disabled. You can change the IP address, net mask and default gateway. Pressing **Enter** without entering values keeps the default values. To contact MX 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 MX IP after an incorrect IP access configuration has been activated. Page 40 has more information on IP access control.

8. Confirm the settings, MX IP resets the configuration.

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

Set the IP address of the computer to 192.168.0.1 and type 192.168.0.220 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.

MX IP mouse setting

To make the remote keyboard and mouse work properly the MX IP settings for the host's mouse and keyboard types must be correct. Check the settings in the MX IP front-end. See page 19.

Host system mouse settings

The host operating system has various settings for the mouse driver. MX IP works with accelerated mice and is able to synchronize the host with the client mouse pointer. This is further discussed on page 15.

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. MX IP Video Modes

MX 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, MX IP may not be able to detect these. Use any standard VESA video mode. Refer to Appendix A on page 51 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 MX IP system

Operate the MX IP system through one of the following interfaces:

1. HTTP/HTTPS - Any standard Web browser. Depending on the Web browser, you can access the MX 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 MX 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 modem or built-in Ethernet adapter.

This chapter deals with the HTTP interface. The other two interfaces are explained on pages 35 and 47.

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://192.168.0.220 for an unsecured connection. Or https://192.168.0.220 for a secured connection. The Login screen appears. See Figure 7

Figure 7 The Login screen

Initially there is only one user configured who has unrestricted access to all MX IP features. Type the default Login name 'super' and Password 'smart' and click **Login**. The MX IP Home page appears. See Figure 8.
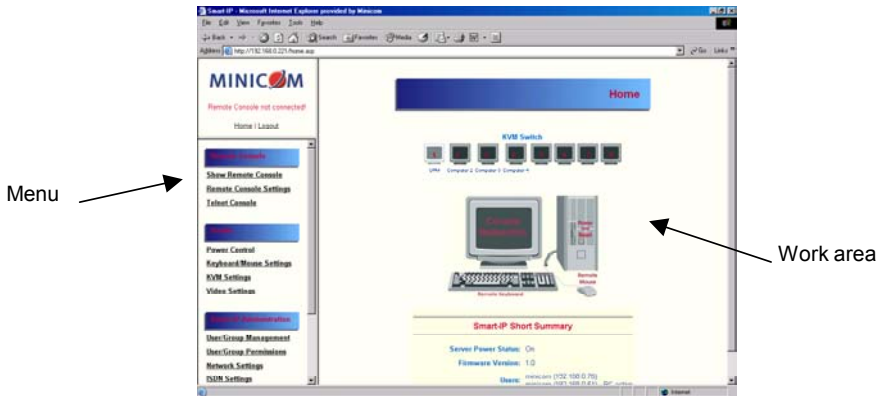
Figure 8 The MX IP Home page

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 MX IP.

- Server Power Status - On or Off

- Firmware Version - installed on your MX IP

- Device management – self managed 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 9.
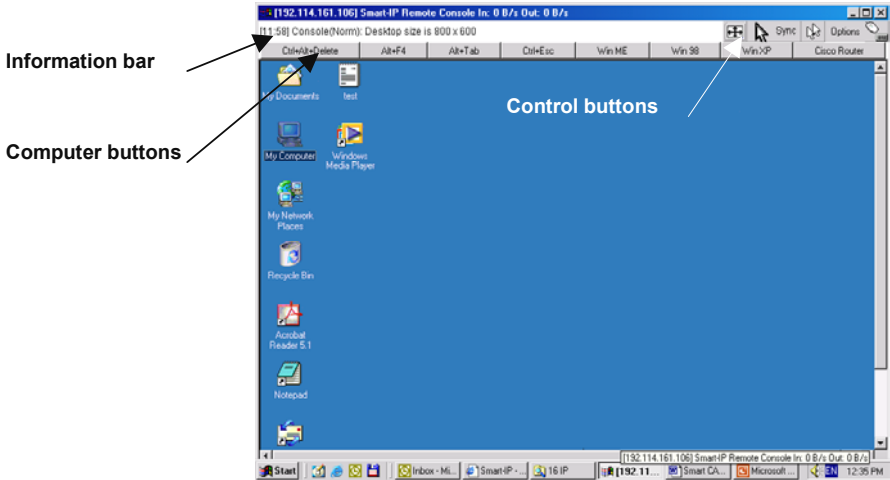
Figure 9 The remote console

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 MX 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.
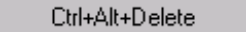
In case MX IP is connected to your local network environment and your connection to the Internet is available using a proxy server only without NAT being configured, the Remote Console is very unlikely to be able to establish the according connection. This is because today's Web proxies are not capable 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 visual 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 15 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 24 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.

14. The Chat window

Use the Chat window to chat with others logged into the system. Figure 10 illustrates the Chat window.
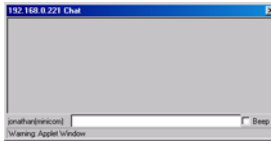
Figure 10 Chat window

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.

15. The Video settings

From the Options menu choose Video Settings. The Video Settings box appears. See Figure 11.
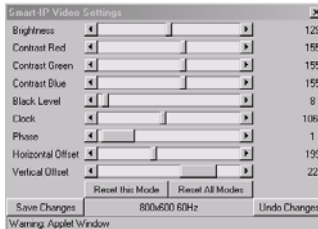
Figure 11 The Video settings

The parameters have the following functions:

Brightness - Brightness control.

Contrast Red/Green/Blue- RGB contrast control.

Black level - Sets the intensity of the color black.

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, Black level 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.

16.   Video Settings access

In the User/Group Permissions section on page 29, it explains how to set access levels for all parameters including Video Settings access. A Remote Console user can always change Brightness, Contrast, Black level 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.

17.   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.

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

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

19.   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 9.
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 20 below. Press this key to free the captured host mouse pointer.

20.   Remote Console Settings

From the MX IP Menu click Remote Console Settings. The Remote Console Settings window appears. See Figure 12.
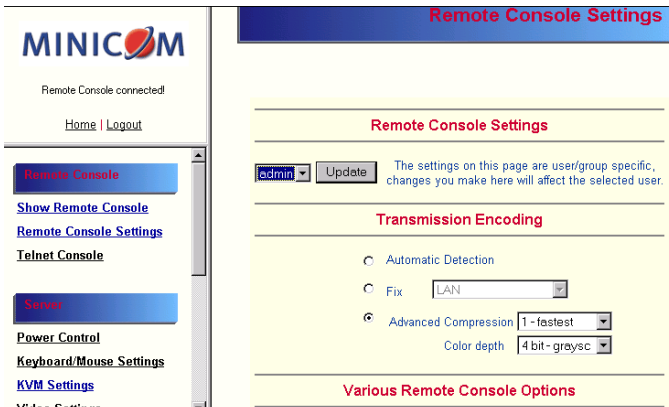
Figure 12 The Remote Console Settings

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.

Fix – Choose the connection method.

Automatic Detection - The encoding and the compression level is determined automatically from the available bandwidth and the current content of the video image.

Normal - Best suited for many parallel users in a LAN environment.

Advanced Compression - For low bandwidth connections. 1 is the lowest and 9 the highest compression rate. The MX 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.

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 the Internet Explorer or the Sun JVM if it is configured this way. Use of the Sun JVM may also be forced (see below).

Sun Microsystems Java Browser Plugin - Uses Sun Microsystems Java Browser Plugin - Sets the administration system's Web browser to use the JVM (Java Virtual Machine) of Sun Microsystems. The JVM 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 11 Mbytes. The JVM provides a stable and identical Java Virtual Machine across different platforms. The Remote Console software is optimized for this JVM version and offers wider range of functionality when run in SUN's JVM.

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

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 23.

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 MX IP recognizes, refer to Appendix B on page 52.

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

21.   Telnet Console

The Telnet Console offers a Java applet for the Telnet protocol to open a connection to MX IP. Its main use is the pass through option for the Serial port 1 see page 35. The Telnet access has to be enabled in the security settings as well, see page 40. It is also possible to connect with a standard Telnet client.

For details regarding the Telnet interface please refer to page 47.

22.   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).

23.   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.

24.   Power Control

The appearance of the power control window depends on the power control option connected to MX IP and on the currently activated setting (discussed on page 37). There are three options available: Power control disabled. Internal power. External power.

Internal power

Once connected enable the internal power option using the Serial settings on page 35.

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 13 these two modes are supported separately. The 2 operation modes are explained in the next section.
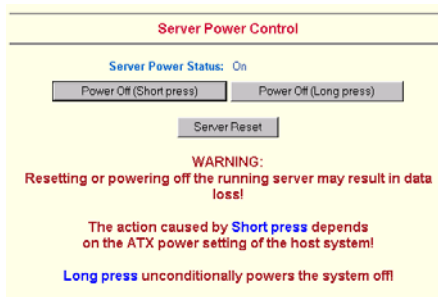
Figure 13 Internal Power Control

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

External power

If the external power option is enabled it will look like Figure 14.
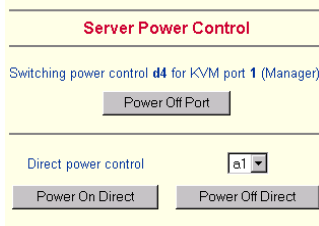
Figure 14 External power control

The upper half is used to switch the power for the KVM port currently active. Use the KVM settings – see page 22 - 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.

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.

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.

25.   Keyboard & Mouse Settings

MX IP supports different keyboard and mouse types.

Click Keyboard & Mouse Settings. The settings appear as in Figure 15.
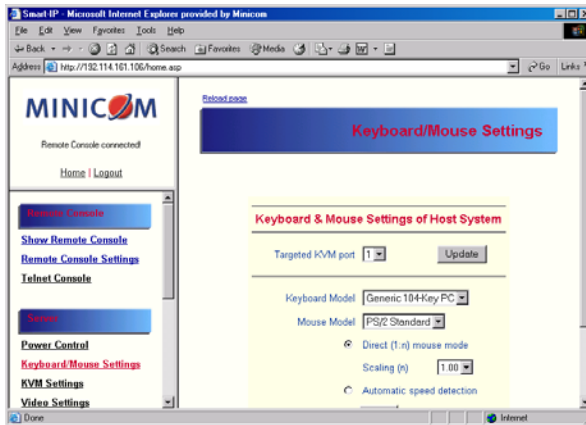
Figure 15 Keyboard & Mouse Settings

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

Targeted KVM port

1. Choose the port to which a KVM switch 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

Mouse Model - Choose the mouse model

Direct (1:n) mouse mode

Use a direct translation of mouse movements between the host and the remote pointer. Fix a scale, which determines the amount the client mouse pointer moves when the host mouse pointer moves by one pixel. This only works when Mouse Acceleration on the local computer is disabled.

Automatic speed detection

When Mouse Acceleration on the local computer is enabled, check Automatic speed detection. We highly recommend disabling the Mouse Acceleration.

G&D Equalizer – **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 MX IP is connected behind such a switch. This option detects the rescaling and compensates for it, so that the mouse synchronization works. Choose auto or a number from the drop down menu.

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.

26. KVM Settings

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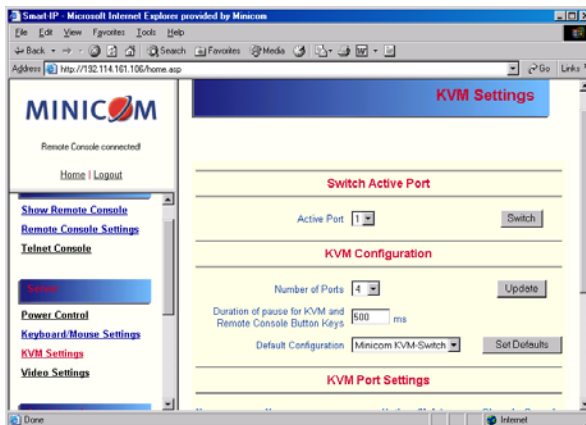
Figure 16 KVM Settings

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 milliseconds , represented by the * symbol in all hotkeys and button keys.

Default configuration

This is explained in the section below.
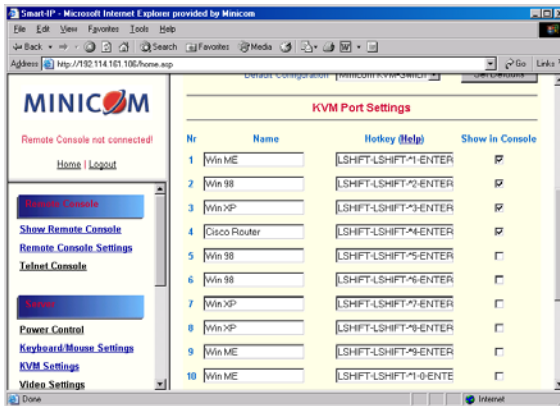
Figure 17 KVM Port Settings

27. 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 52 for a list of key codes.

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

MX IP uses separate mouse synchronization settings - see page 15 - and video-settings - see page 14 - for each port.

Note:

It is still possible to apply KVM 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 19.

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

28. Video Settings

From the MX IP Menu choose Video Settings. The Video settings appear. See Figure 18
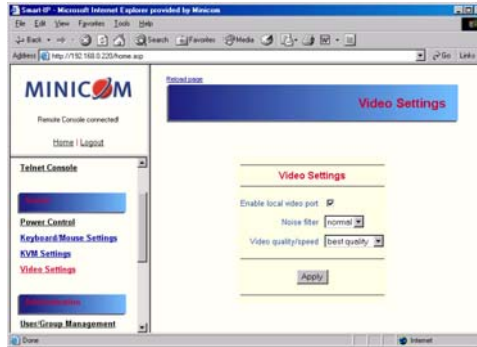
Figure 18 Video Settings

29.   Enable local video port

This option decides if the video output on the front panel of MX IP is active and passing through the incoming signal from the host system.

30.   Noise filter

Define how MX 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.

31.   Video quality/speed

Choose the Video quality/speed, the faster the speed the lower the video quality.

32.   Custom Video Modes

Add video modes to MX IP, which are not recognized using the factory settings, when for example using special modelines 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 19.

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 19 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 MX 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.

33.   User/Group Management

From the MX IP Menu choose User/Group Management. The User/Group Management settings appear. See Figure 20. The user and group management of MX IP is based on configurable users and groups. Each user or group can have different access capabilities.

The MX IP is factory set with a supervisor user called `super' with the password 'smart'. Change the super user password immediately after accessing the MX IP.
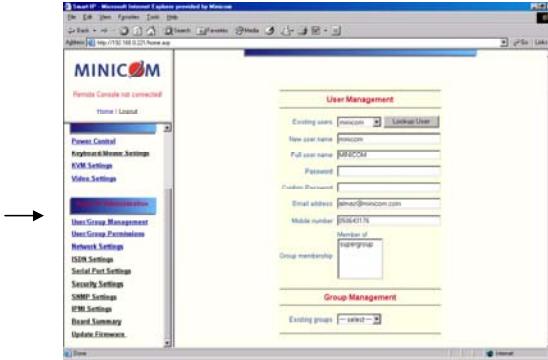
Figure 20 The User/Group Management settings

34.   Existing user

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

35.   New user name

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

36.   Full user name

Write the full name of the new user.

37.   Password / Confirm password

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

38.   Email address /Mobile number

These are optional.

39.   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.

40.   Existing groups

Select an existing group for copying, modification or deletion.

41.   New group name

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

42.   Create User button

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

43.   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.

44.   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.

45.   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.

46.   Group Management

The following headings appear under Group Management.

47.   Create group button

To create a group:

1. Type a name into the New group name box

2. Click the Create group button.

48.   Delete Group button

To delete a group:

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

2. Click the Delete group button.

49.   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.

50.   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.

51.   User/Group Permissions

From the MX IP Menu choose User/Group Permissions. The User/Group Permissions settings appear. See Figure 21.
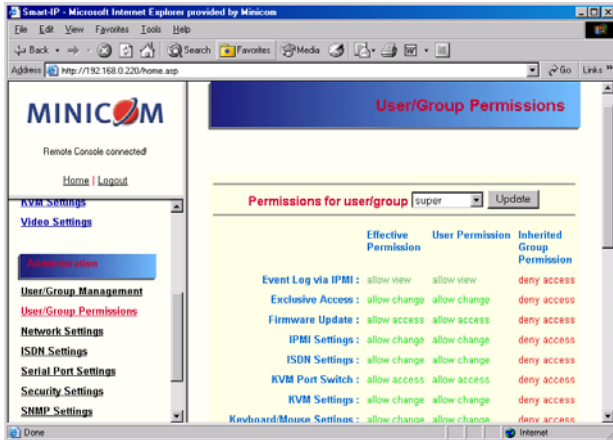
Figure 21 User/Group Permissions

Each user or group has a set of access rights to the MX 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.

Group setting – Use the access rights inherited from the group(s), the user belongs to.

3. Select the desired permission.

4. To add the right, click **Add**.

    To remove the right, check the Delete Entry box.

5. Click **Apply**.

52.   Network Settings

From the MX IP Menu choose Network Settings. The Network Settings appear. See Figure 22.

Figure 22 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 MX IP using its pre-configured IP settings.

Warning! Changing the network settings of MX IP may result in losing the connection. If you remotely change the settings ensure that all values will give you access to the MX 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, MX 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 MX IP to your local sub-net, complete the corresponding configuration of your DHCP server.

BOOTP - When selected, MX 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 MX 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 MX 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. MX 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 MX IP's Remote Console server and HTTPS server are listening. If empty the default value is used.

HTTP port

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

Telnet port

Port number at which MX IP's Telnet server is listening. If empty the default value is used.

Bandwidth limitation

The maximum network traffic generated through the MX IP Ethernet device.

Disable Setup Protocol

Exclude the MX IP from the setup protocol.

53. Dynamic DNS

Minicom provides a Dynamic DNS service. See Figure 23.
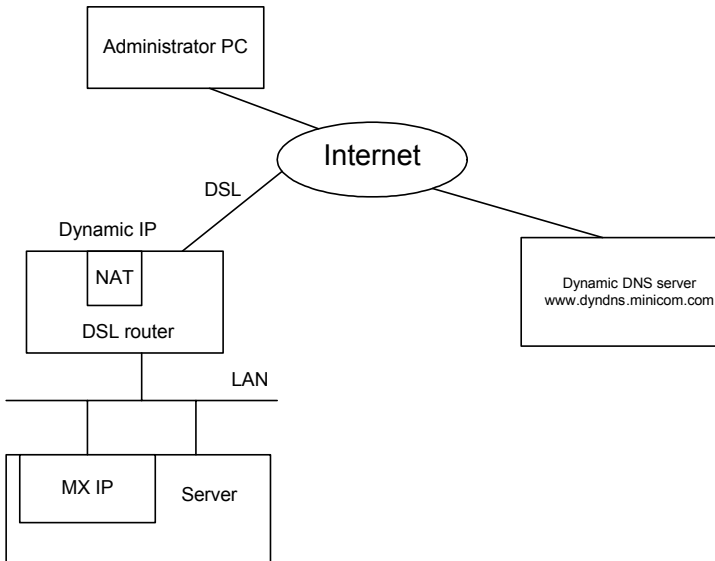
Figure 23 Dynamic DNS scenario

MX 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, MX 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 MX 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 MX IP.

To enable the Dynamic DNS:

1. Ensure the MX IP LAN interface is properly configured.

2. From the MX IP menu choose Network Settings / Dynamic DNS. The Dynamic DNS Settings appear. See Figure 24.

Figure 24 Dynamic DNS Settings

3. Check the Enable Dynamic DNS box.

4. Change the settings as desired.

Dynamic DNS server - Enter the server name where MX IP registers itself in regular intervals. If left blank the default will be used.

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

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

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

MX IP has its own independent real time clock. Ensure the time setting is correct by configuring a timeserver see page 23.

MX 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.

54.   Serial Port Settings

From the MX IP Menu choose Serial Port Settings. The Serial Port Settings appear. See Figure 25.
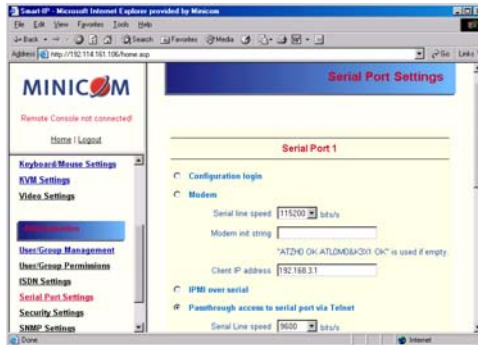
Figure 25 Serial Port Settings

In the MX 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 - MX 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 MX IP. The MX 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 MX 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 MX IP via a modem. When you dial into the MX IP the client computer will receive a Client IP address from the MX IP. Open the Web browser and type modem server IP address to login to the MX 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 MX 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 MX 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 44 for more information.

Passthrough… - 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 39) or a standard telnet client to connect to MX IP. For more information, see page 47.

External Power Option – When the **External Power Option** is the Sentry Power Tower 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 26 External Power Option for Serial port 1 window

Serial Port 2

This port provides the power control options, see page 19. Choose a suitable setting and fill in additional required options. MX 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 27 Button Press Durations box

External Power Option

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

SPC 800/1600 - Using the Avocent™ SPC, switch power for more than one system connected to MX 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.

Intelligent Power Module - External module option to switch power of a single system by putting it in the power supply line of the controlled system.

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

ePowerSwitch-Slave – This switch is cascadable to up to 4 power sockets with 8 ports. MX IP must be connected to the first socket of the cascade via a serial connection.

Spectrum Control Inc. - Smart Start Jr. – Check the box if this option is connected.

55.   Security Settings

From the MX IP Menu choose Security Settings. The Security Settings appears. See Figure 28.
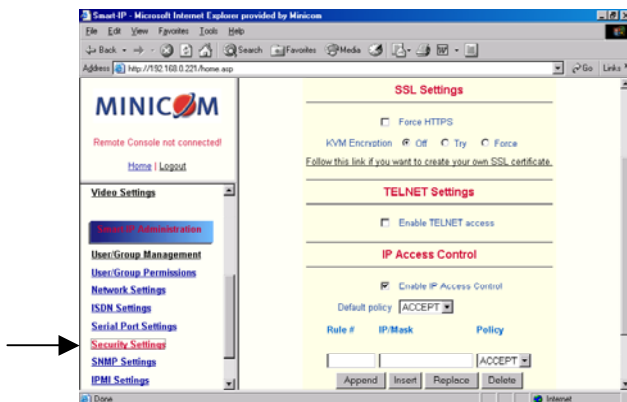
Figure 28 Security Settings

SSL settings

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

Disable SSLv2 ciphers – disables SSLv2 ciphers. Only version 3 or higher is enabled.

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

MX IP uses the SSL (Secure Socket Layer) protocol for any encrypted network traffic between itself and a connected client. When connecting, MX IP reveals its identity to a client using a cryptographic certificate. This is the same for all MX 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. MX 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 MX IP SSL certificate:

1. From the Security Settings page choose **Create your own SSL certificate**. The window appears as in Figure 29.

Figure 29 CSR

2. Fill in the fields:

Common name - Network name of MX 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 MX IP belongs.

Organization/Locality/City/State/Province - Organization to which MX 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 MX 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 MX IP. The certificate uploads.

Important! If you destroy the CSR on MX 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 5).

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 - Enter the IP/Mask and set the policy. Then press Append .

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

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.

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

56.   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 MX IP)

- Server's power state

- The following actions can be initiated via SNMP:

- Reset server

- Power on/off server

- Reset MX IP

The following events are reported by MX IP via SNMP:

- Login trial at MX IP failed

- Login trial at MX IP succeeded

- Denying access to a particular action.

- Server was reset.

- Server was powered on/off

From the MX IP Menu choose SNMP settings. The SNMP Settings appear. See Figure 30.
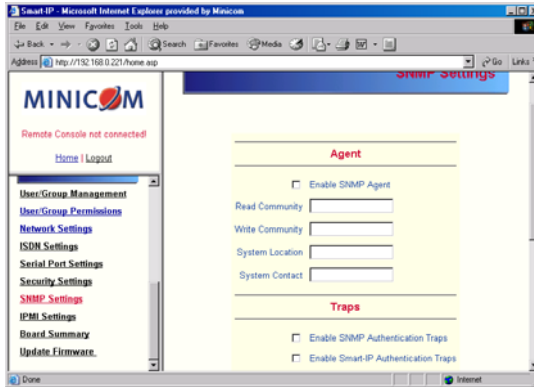
Figure 30 SNMP settings

You can change the following parameters:

Enable SNMP Agent - When checked, MX 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 MX 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 MX 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 MX IP via SNMP using a wrong SNMP community.

Enable MX 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, MX 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.

57. The MX IP SNMP MIB

Click the link to access the MX IP SNMP MIB file. With it, an SNMP client can communicate with MX IP.

58. IPMI Settings

The MX 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 MX IP Menu choose IPMI Settings. The IPMI Settings appears. See Figure 31.

Figure 31 IPMI Settings
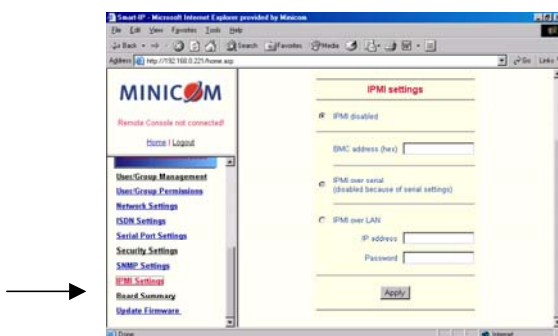
IPMI disabled - Disables IPMI. Status via IPMI and Event Log via IPMI are not available and the power on/off and reset functions won't use IPMI.

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 MX 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.

59.   LDAP Settings

You can keep authentication information in a central LDAP directory.

From the MX IP Menu choose LDAP Settings. The LDAP Settings appears. See Figure 32.

Figure 32 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 MX IP.

60. Maintenance

From the MX IP Menu choose Maintenance. The MX IP Maintenance window appears.

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

61. 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 33.

Figure 33 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 MX IP's power supply won't be interrupted during the update process, as this may cause damage.

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

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

62. Data file for support

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

63. 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 MX IP therefore the graphics should be accessible on the Network. Define Primary and secondary DNS in the Network settings if needed.

64. Access via Telnet

Connect via a standard Telnet client using MX 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 35 - according to the requirements of the device.

Connect to MX IP in the usual way required by the Telnet client, e.g. in a UNIX shell: telnet 192.168.0.220 – (The IP address has been replaced by the one that is actually assigned to MX 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.

65.   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.

Frequently Asked Questions

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

A: Ensure the MX IP mouse settings match the mouse model. Also see page 15

Q 2: Bad video quality or grainy picture

A: Use the brightness and contrast settings - see page 14. 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 I try to open the Remote Console applet loading fails with Bad Magic Number Exception.

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

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

A: Check if the network connection is working (ping the IP address of MX IP). If not, check network hardware. Is MX IP powered on? Check if the IP address of MX 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, MX 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'. This can be done in the Remote Console settings.

Q 8: In the browser the MX 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 MX 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.

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.

Appendix A: MX IP Video modes

The MX 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
1280x1024	75

Appendix B: Key codes

Figure 1 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 MX 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 1 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

Key	Key code	Alternative
Psc	PRINTSCREEN	
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: The OSD functions

The Phantom MX IP system can be controlled and monitored through On-Screen-Displays (OSD) on the MX IP and UPM Manager screens. The OSD contains a number of different windows that are accessed using Hot-keys. Each window has its own special function.

Displaying the OSD

To display the OSD:

Press **Shift**, **Shift**. The Select Computer window appears. See Figure 2.

Pressing keyboard hotkeys

Note! For all keyboard hotkey sequences mentioned in this guide – press the first key, release and then press the next key.

Note! When the MX IP or UPM are not connected to a local computer, the OSD appears automatically.
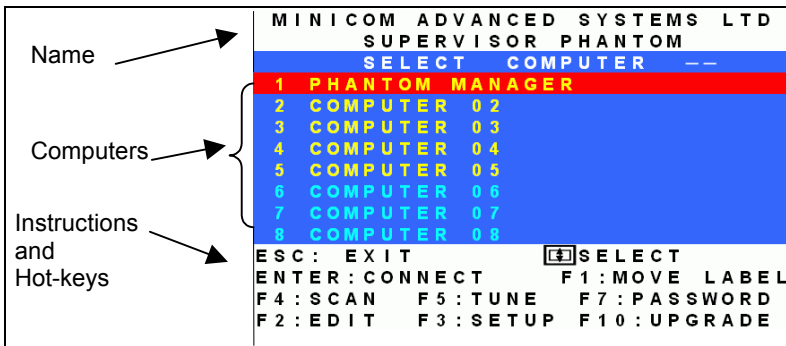

Figure 2 The Select Computer window

The OSD is divided into three sections. These are:

- Name
- Computers
- Instructions and Hot-key guide

The Computers section

The Computers section displays the computers in groups of eight.

Navigate between the groups with the **Page Up** and **Page Down** Arrow keys.

In this section you select computers - discussed below.

Line Color codes

Each computer line can be one of three colors as follows:

Yellow	Connected and switched on computer.
Black	Connected and switched on computer currently being accessed by the other Manager. This is subject to a Timeout period. Meaning that after a 60 second (default) period of non-use the line turns to yellow.
Blue	Unconnected or switched off computer.

Selecting a Computer

To select a computer:

1. Navigate to the desired computer with the **Up** and **Down** Arrow keys.

Or

Type the computer number. It will appear in the "SELECT COMPUTER" line. See Figure 2.

2. Press **Enter**. The selected computer's screen replaces the Manager's screen. A Confirmation label appears showing which computer is accessed. See Figure 3.

Figure 3 The Confirmation label

Control and monitor the computer from the Manager KVM position. Note! After 60 seconds of non-use the keyboard and mouse are disabled and a Timeout label appears. See Figure 4.

Figure 4 The Timeout label

To re-enter the system press **Esc**.

When trying to select a black colored computer line, (computer currently accessed by the other Manager) you can view the screen but not gain control. Also a "**BUSY**" label appears. However, once the other Manager's Timeout period activates the "**BUSY**" label is replaced by a "**FREE**" label and you can gain control. To gain control press **Esc**.

To return to the OSD after accessing a computer:

Press **Shift**, **Shift**.

To return to the Manager computer screen:

Press **Shift**, **Esc**.

To return to the previously accessed computer screen:

Press **Shift**, **Tab**.

The hotkey functions

The OSD hotkey functions are briefly outlined in the table below, and are explained in detail further on.

Hotkey	Function
F1	Move label identifying the current selected computer to anywhere on the screen
F2	Opens Edit window to edit text – change computer names etc.
F3	Opens Setup window to set parameters – scan times etc.
F4	Activate scan
F5	Image tuning
F6	Autoskip – during a scan skip inactive computers
F7	Opens Password window to activate password protection
F8	Keyboard language
F9	Change the display hotkey
F10	Firmware upgrade/ Numbering software access mode
F11	Load defaults
F12	Auto-numbering

Move Label - F1

Position the Confirmation label – Figure 3 above – anywhere on the screen.

To position the label:

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

2. Press **F1**. 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.

Edit Mode window - F2

You can edit text in the Name and Computers sections. This is done in the **Edit Mode** window.

To display the **Edit Mode** window:

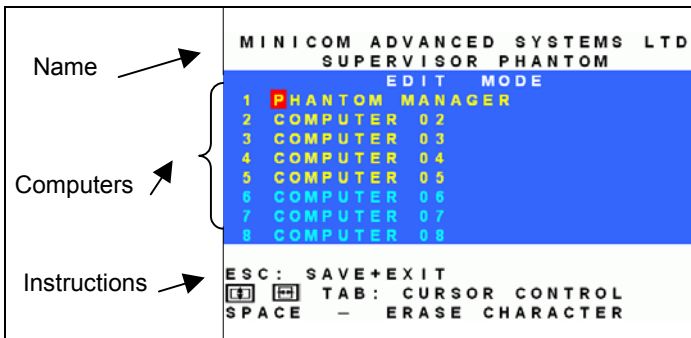Press **F2**. The Edit Mode window with instructions appears, see Figure 5.

Figure 5 The Edit Mode window

Navigating between sections

To navigate between the Name and Station sections, use the **Up** and **Down** Arrow keys.

Editing options

The editing options below apply to all OSD windows in which you can edit characters.

You can either overwrite or erase a character.

To overwrite a character:

1. Navigate to it using the Arrow keys.

2. Type the new character.

To erase a character:

1. Navigate to it using the Arrow keys.

2. Press the Spacebar. The character disappears. A blank space replaces the erased character.

To erase a sequence of characters:

1. Navigate to the first character in the sequence.

2. Press and hold the Spacebar down until you erase the sequence.

Saving changes

To save all editing changes and return to the Select Computer window:

Press **Esc**.

Editing the Name section

You can substitute the text in the Name section with up to 30 characters in each of the two lines. A space constitutes a character.

Editing the Computers section

The numbering at the start of each line is unalterable.

You can substitute the text that appears after the number with up to 20 characters per line.

Editing a group of lines

You can edit a group of lines with the same data change.

To edit a group of lines:

1. Navigate to the first line you want to change.

2. Type the desired change.

3. Press **End**, **End**. The rest of the column downwards takes on the same change.

The Setup window - F3

You set parameters, and configure settings, in the Setup window.

To display the Setup window:

Press **F3**. The Setup window with the relevant instructions and hotkeys appears. See Figure 6.

Figure 6 The Setup window

The **Setup** window contains 7 columns, as follows:

Column	Function
Numbers	Computer numbers in groups of 8
SCN	Scanning time period
DSP	Confirmation label display time
KB	Keyboard setting, either PS or Unix
MS	Mouse type
OUT	Timeout period
1-6	Security profiles

The SCN (Scan) column

The SCN column shows the length of time in seconds that a remote computer's screen will appear on the Management screen during scanning.

The DSP (Display) column

The DSP column shows the length of time in seconds that the remote computer's Confirmation label appears on the Management screen.

Changing the SCN and DSP time spans

The **SCN** and **DSP** time spans are preset to 030 seconds. You can adjust these times to suit your needs.

To change the time span:

1. Navigate with the **Tab** or **Right** and **Left** Arrow keys to the time span you want to change.

2. Type the desired time span using the numbers above the keyboard letters.

3. Press **Esc**.

When typing over a group of three digits, the cursor automatically reverts to the first digit once you edit the third digit.

Changing the time span of a group of computers

You can change the time spans of the **SCN** and **DSP** columns from a particular computer downwards.

To change the time span:

1. Navigate to the time span of the first computer you wish to change.

2. Type the desired change.

3. Press **End, End**. The remainder of the column takes on the same change.

4. Press **Esc**.

Removing a computer from the scanning sequence

To remove a computer from the scanning sequence:

1. Type 000 in the **SCN** column.

2. Press **Esc**.

Constantly displaying the Confirmation label

To constantly display the computer Confirmation label:

1. Type 999 in the **DSP** column.

2. Press **Esc**.

The KB column

The **KB** column shows the keyboard mapping settings. Set the **KB** mapping for each computer according to its operating system.

The default **KB** mode is **PS**, which is the standard keyboard mapping for Windows and Linux based operating systems.

For a UNIX operating system using a standard PS/2 keyboard, set the KB mapping as follows:

-   **U1** for HP UX and SGI

-   **U2** for Alpha UNIX and Open VMS

To change the **KB** column from **PS** to **U1** or **U2**:

1. Navigate to the **KB** field by using the Tab or Arrow keys.

2. Press the Spacebar. The display interchanges between **PS**, **U1** and **U2**. Find the desired setting.

3. Press **Esc**.

The MS column

The Phantom system automatically detects the mouse types, and configures the system accordingly.

Timeout period

The Management keyboard, mouse and screen are automatically disabled after a preset time of non-use. This Timeout period is set in the OUT column of the Setup window (F3).

By default the OUT column is 060, meaning the Time Out function is set to 60 seconds.

To change the Timeout period:

1. From the Select Computer window press **F3**. The Setup window appears.

2. Navigate with the Tab or Arrow keys to the OUT column of the desired computer.

3. Type the desired time span (minimum 030 seconds maximum 998 seconds).

(For the rest of the column downwards to take on the same change press **End**, **End**.)

4. Press **Esc**.

When Timeout activates, the keyboard and mouse are disabled, and a 'Timeout' label appears. See Figure 7.

<div align="center">

T I M E O U T
Figure 7 The TIMEOUT label

</div>

To re-enter the system:

Press **Esc**.

Scanning Computers – F4

You scan computers from the Select Computer window.

To start scanning:

Press **F4**. During scanning a Confirmation label appears, showing which **Remote** computer is presently displayed. See Figure 8.

Figure 8 The Scan Confirmation label

Note! The scan will skip any active computer set to 000 in the **SCN** column.

To stop scanning press **F4**.

Image tuning - F5

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

To adjust the screen image:

1. Navigate to the remote computer you wish to adjust.

2. Press **F5**. The screen image of the selected computer appears, together with the Image Tuning IN label. See Figure 9.

Figure 9 The Image Tuning IN label

3. Adjust the image by pressing the **Right** or **Left** Arrow keys.

4. When the image is satisfactory, press **F5** again, the Image Tuning OUT label appears. See Figure 10

Figure 10 The Image Tuning OUT label

5. Adjust the image by pressing the **Right** or **Left** Arrow keys. When the image is satisfactory, press **Esc**.

Note! Picture quality is relative to distance. The further away a remote computer is from the Manager position, the lower the image quality, and the more tuning needed. So place the higher resolution computers closer to the manager unit.

Skipping out unconnected or switched off computers - F6

When navigating through the list of computers, you can skip out the unconnected or switched off computers. You do this with Autoskip. By default, Autoskip is activated.

To activate or deactivate Autoskip:

In the Setup window (F3), press **F6**. The F6 Autoskip in the hotkey section of the OSD changes from ON to OFF

When Autoskip is inactive and the computer being scanned is switched off, then the **Manager** screen appears dark.

Changing the keyboard language - F8

You can change the keyboard language from US English (QWERTY) **US** to German (QWERTZ) **DE** or French (AZERTI) **FR**.

To change the Language:

1.   In the Setup window (F3), press **F8** until you reach the desired language.

2.   Press **Esc**.

Changing the OSD display hotkey – F9

The default hotkey to display the OSD, is **Shift**, **Shift**. You can replace this hotkey with any of the following:

- Ctrl, Ctrl

- Ctrl, F11

- Print Screen

With a choice of 4 different hotkeys, you can operate up to 4 OSDs from 1 KVM position. Each OSD needs a different display hotkey. This is useful for cascading systems of for example, the Supervisor MU, Supervisor Pro, and Phantom.

To change the hotkey:

1.   In the Setup window (F3), press **F9**. The hotkey changes from **Shift, Shift** to **Ctrl, Ctrl**. Continue pressing until you reach the required hotkey.

2.   Press **Esc**. The new hotkey is set. From now on, use the new hotkey to display the OSD.

Exiting the OSD

When the OSD is displayed press **Esc** to exit the OSD and remain switched to the current computer.

Reverting to the default OSD settings - F11

The Administrator can reset all editing and configurations done in the different OSD windows, to the default factory settings.

Warning! This feature will erase all settings including computer names, passwords.

To revert to the default OSD settings:

1. From the Management OSD Select Computer window press F7. The Password box appears. See Figure 11.

Figure 11 The Enter Password box

2. Type the default password "admin". (You can change this password when customizing the system).

3. Press **Enter**. The Password window appears. See Figure 12.
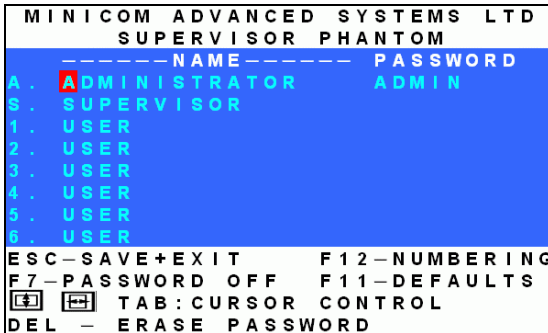
Figure 12 The Password window

4. Press **F11**.

5. Press 'Y' to confirm. The OSD reverts to the default settings.

Auto numbering – F12

Auto numbering gives each Phantom Specter a sequential ID number. Auto numbering can be done through the Management OSD.

For Auto numbering to work properly **ALL** connected computers **MUST** be switched on

To perform Auto numbering:

1. From the OSD Select computer window press **F7**. The Enter Password box appears. See Figure 2.

Figure 13 The Enter Password box

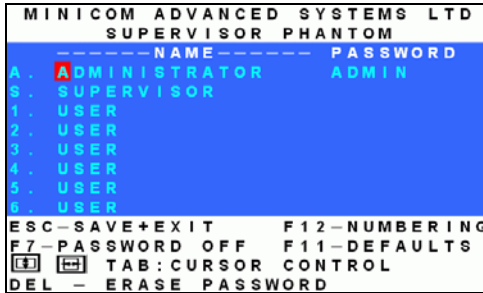2. Type the Administrators password (default password is ADMIN) and press **Enter**. The Password window appears.

Figure 14 The Password window

3. Press **F12** to activate Auto numbering. A Confirmation label appears.

4. Press **Y** to confirm. The process activates. Wait until the process is complete.

5. Press **Esc** to save and return to the Select Computer window. The Remote computers appear on the OSD.

Password protecting the OSD

The Management 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) - Highest

The Administrator can:

- Set and modify all Passwords and security profiles

- Fully access any computer

- Use all OSD functions

Supervisor (Status S) - Middle

The Supervisor can:

- Fully access any computer

- Access the following OSD functions only – **F1** Moving the Confirmation label. **F4** Scan and **F5** Tune.

User (Status U) – Lowest

There are 6 different Users in the Phantom 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 – A TIMEOUT label appears if access is attempted

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

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

Enabling password protection

By default, password protection is disabled.

To enable password protection:

1. From the Management OSD Select Computer window press **F7**. The Password box appears. See Figure 15.

Figure 15 The Enter Password box

2. Type the default password "admin". (You can change this password when customizing the security system).

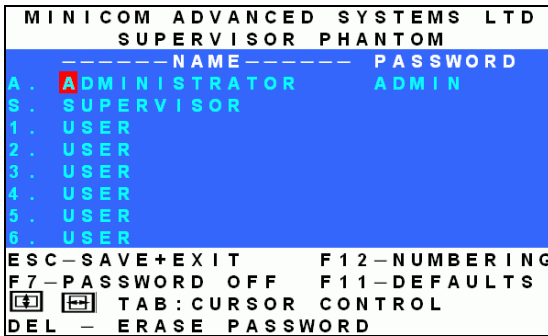3. Press **Enter**. The Password window appears. See Figure 16.

Figure 16 The Password window

4. Press **F7**. The Confirmation label appears. The password indication in the hotkey section of the OSD changes to **PASSWORD ON**.

5. Press 'Y' to confirm. Password protection is now enabled.

6. Press **Esc**.

Disabling password protection

To disable the password protection:

1. Enter the OSD Select Computer window with the Administrator's password.

2. Press **F7**. The Password window appears.

3. Press **F7** again to disable Password protection. The Confirmation label appears. The password indication in the hotkey section of the OSD changes to **PASSWORD OFF**.

4. Press 'Y' to confirm. Password protection is now disabled.

5. Press **Esc**.

Setting up a password

The Administrator sets up passwords for each User Profile in the Password window. He can also edit the names to give each Profile a more identifiable name.
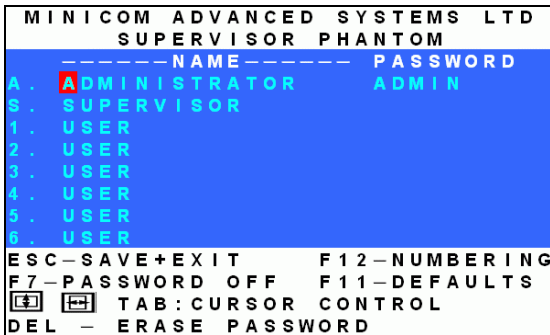
Figure 17 The Password window

To set up a password:

1. From the OSD Select Computer window press **F7**. The Enter Password box appears.

2. Type the Administrator's password.

3. Press **Enter**. The Password window appears. See Figure 17.. The first row marked **A** is for the Administrator name and password and the second row marked **S** is for the Supervisor name and password.

Note! Password characters are not case sensitive, and a space can be a password character. A space will appear as an asterix.

To set up a password:

1. Navigate to the desired line number.

2. Type:

> (i). Identifiable name in the **Name** column.

> (ii). Password in the **Password** column – between 1 and 8 characters.

3. Press **Esc**.

Changing a password

The Administrator can change any name or password from the **Password** window.

To change a name or password:

1. Navigate to the desired line number.

2. Delete the text by pressing **Delete**.

3. Type the desired change.

4. Press **Esc**.

Setting the User profiles access level

Set the 6 User profiles access levels from the OSD Setup window (**F3**). See Figure 18. The 6 User Profiles correspond to the 6 Users in the Password window see Figure 17 above.

Figure 18 The Setup window

To set the User Profiles access levels:

1. Navigate to the desired User Profile and computer.

2. Change the desired access level by pressing the Spacebar.

3. Repeat steps 1 and 2 for each User Profile and computer.

4. Press **Esc** to save the changes. When a User accesses the system with their password they see the access levels for each computer displayed on the OSD. See Figure 19.

Figure 19 User access levels

Accessing the OSD using a password

Once password protection is enabled, you can only access the OSD by entering the appropriate password.

The default Administrator's password is "ADMIN". The passwords of the other two security statuses are set by the Administrator.

To access the OSD:

1. Press **Shift**, **Shift**. The **Enter Password** box appears. See Figure 20.

Figure 20 The Enter Password box

2. Type in the appropriate password.

3. Press **Enter**.

Timeout

When password protection is activated you can automatically disable the Management keyboard, mouse and screen after a preset time of non-use. You set the Timeout period in the OUT column of the Setup window (F3).

By default the OUT column is set to 999, which means that the Time Out function is disabled.

To set Timeout:

1. From the Select Computer window press **F3**. The Setup window appears.

2. Navigate with the Tab or Arrow keys to the OUT column of the desired computer.

3. Type the desired time span (minimum 030 seconds maximum 998 seconds).

(For the rest of the column downwards to take on the same change press **End**, **End**.)

4. Press **Esc**.

When Timeout activates the keyboard and mouse are disabled and the monitor blacks out with a 'Timeout' label.

Figure 21 The TIMEOUT label

To re-enter the system:

Press **Shift, Shift**.

Type the password and press **Enter**. You re-enter the system.

Numbering newly added Specters or renumbering existing Specters

When the Phantom MX IP system was first installed, ID numbers were assigned with the auto-numbering process. Auto numbering gives each Phantom Specter a sequential number according to its physical location in the daisy chain.

When adding a Specter to the system give it an ID number by performing the Auto numbering process (either through the OSD, or through the Phantom Numbering software discussed below).

Alternatively, when adding a Specter or to renumber existing Specters, you can number them according to their physical location or by manually choosing the numbers you desire.

Renumbering is done using Phantom Numbering software. The software is on the Marketing & Documentation CD.

Connect the Phantom MX IP System

To number the Specters the Phantom 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 Phantom Manager (MX IP or UPM). See the respective Installation Guides.

RS232 Serial cable system requirements

- Pentium 166 or higher computer
- 16Mb RAM
- Windows 98, NT4 (SP6), 2000, ME or XP
- Free Serial port

Running the Phantom Numbering software

To use the Numbering software, the OSD must be in the Numbering mode.

1. Press **Shift**, **Shift** to display the OSD.

2. Press **F10** to enter the Numbering mode. The Firmware Upgrade label appears. See Figure 22.

Figure 22 The Firmware Upgrade label

Start the Marketing & Documentation CD and choose Phantom Utilities Softpack. The Phantom Softpack window appears.

The Numbering Software can be installed onto the computer or operated directly from the CD. To install the software choose **Install Phantom Numbering Software**.

To run the software:

Select **Run Phantom Numbering Software**. The Phantom Numbering window appears. See Figure 23.
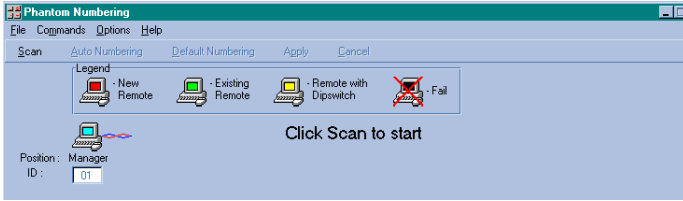

Figure 23 The Phantom Numbering window

Selecting a Com port

1. From the **Options** menu, select **Com por**t. The Com port no. box appears.

2. Choose the Com port to which the RS232 Serial cable is connected.

3. Click **OK**.

Legend

The color-coded computer icons are explained in the table below.

Icon	Meaning
	Manager. The ID number is fixed at 01.
	New Specter. Has no ID number at present.
	Existing Specter. Has an ID number.
	Remote with dipswitches - not relevant to the Phantom MX IP system
	Failure to number

Scanning the system

In the toolbar, click **Scan**. This maps out the computers connected to the system. When finished the window appears as in Figure 24.
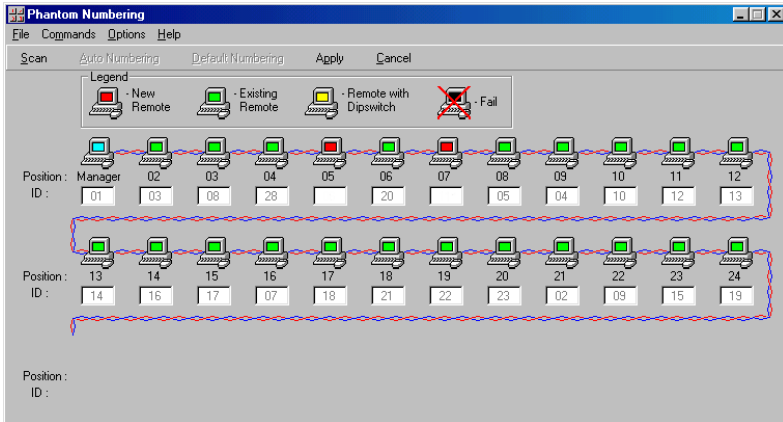
Figure 24 After scanning

Position and ID

The **Position** shows the physical location of the computer in the daisy chain. The **ID** is the ID number given to each Specter.

In Figure 24, the blank ID boxes indicate that no ID number has yet been assigned.

Auto numbering

Auto numbering fills in any blank ID number boxes with the first available free ID number.

To perform Auto numbering:

1. In the toolbar, click **Auto Numbering**. All blank boxes are filled in.

2. Click **Apply**. The process activates. When finished new ID numbers are assigned to the Specters. The icons change to green.

Default numbering

Default numbering assigns ID numbers according to the physical location of each Specter.

To perform Default numbering:

1. In the toolbar, click **Default Numbering**.

2. Click **Apply**. The process activates. When finished the ID numbers are assigned according to the physical position of the units.

Manual numbering

Manual numbering involves selecting an ID number box and assigning a number from the Drop-down numbers list. See Figure 25. Only numbers that have not been assigned are available.

Note! Numbering a Specter **00** removes it from the system

To perform Manual numbering:

1. Select an ID number box and choose a number.

2. Click **Apply**. The process activates, and the ID number assigns.
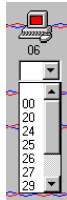

Figure 25 The Drop-down menu

Using 00 or blank ID numbers

You may want to swap ID numbers between Specters, or give a Specter the ID number of another Specter. To do this, renumber a Specter to either 00 or blank. The previous ID number now becomes available to assign to another Specter.

Cancel

After making changes to ID numbers using the Auto, Default or Manual numbering, but BEFORE clicking **Apply**, you can revert to the position as it was before the changes.

To do so:

Click **Cancel**.

Restore

After making changes to ID numbers using the Auto, Default or Manual numbering, and AFTER clicking **Apply**, you can revert to the position as it was before the changes.

To do so:

From the **Options** menu, select **Restore**.

Note! **Restore** is only available BEFORE the new scan is activated.

Communication Error

If a Communication Error box appears when trying to scan the system – see Figure 26. Check the following:

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

- The Com Port settings in **Options**/**Com Port** are set correctly.

- The Firmware Upgrade label (F10) appears on the screen. See Figure 26.
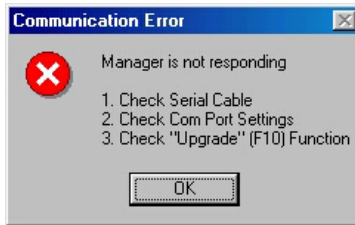

Figure 26 Communication Error

Fail icons

When after a carrying out a numbering procedure, Fail icons appear – see Figure 27. Wait 30 seconds and repeat the numbering procedure.
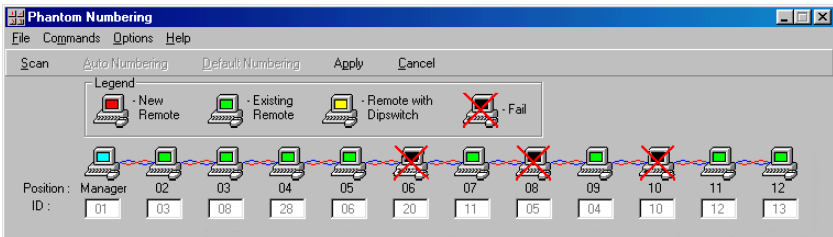

Figure 27 Fail icons

Upgrading the Phantom firmware

With the Phantom Update software program you can upgrade the firmware for the:

- OSD

- Both Managers (MX IP & UPM)

- Specters

Phantom Update enables you to add new features and fix bugs in a quick and efficient manner.

You can install Phantom Update on the Manager computer or any other computer, even one not part of the Phantom system.

The Phantom Update software and firmware is on the Marketing & Documentation CD.

To obtain latest firmware for your system refer to http://www.minicom.com/phandl.htm.

System requirements for the Phantom Update software

- Pentium 100 or higher with 16 MB RAM and 10 MB free Hard Drive space.

- Free Serial port.

- Windows 95, 98, 2000, ME, XP or Windows NT 4.0 SP (service pack) 3 or later.

Connect the Phantom system

To update the firmware the Phantom 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 Phantom Manager (MX IP or UPM). See the respective Installation Guides.

Installing the software

To install the Phantom Update software:

1. Insert the Marketing & Documentation CD. The CD menu runs automatically.

2. Choose Phantom Utilities Softpack.

3. Either run the Phantom Update software straight from the CD or install it on the computer's hard drive and run it from there.

Starting and configuring Phantom Update

1. Start the Phantom Update software. The Phantom Update window appears. See Figure 28.

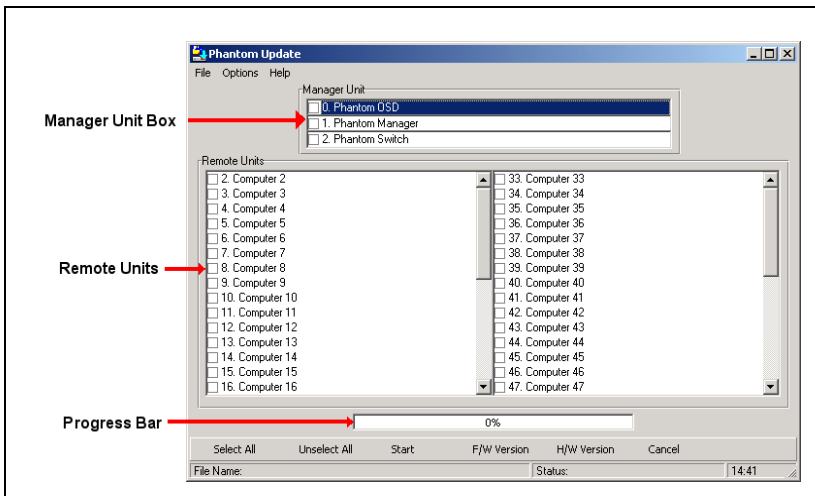**Figure 28 The Phantom Update window**

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

Button or Box	Function
Select All	Selects all remote computers
Unselect All	Unselects selected remote computers
Start	Starts firmware download
F/W Version	Displays the firmware version number

Button or Box	Function
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 29.

Figure 29 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.

Displaying the maximum number of Remote units

Select the maximum number of Remote units to display in the Phantom Update window. By default 64 Remote units are displayed.

1. From the **Options** menu choose **Remotes**. The Remotes box appears see Figure 30.

2. Select the maximum number of Remote units in your Phantom system.

3. Click **OK**.

Figure 30 The Remotes box

The F10 Upgrade hotkey

Whenever you use Phantom Update, you must first activate the Firmware Upgrade mode on the Phantom Manager OSD.

To activate the Firmware Upgrade mode:

1. Display the Manager OSD window. The default Display hotkey is **Shift**, **Shift**.

2. Press **F10**. The Firmware Upgrade mode activates. The Firmware Upgrade label appears. See Figure 22.

Figure 31 The Firmware Upgrade label

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 Phantom Update program.

2. Activate the Firmware Upgrade mode on the Manager OSD.

3. In the **Manager Unit** box, check the OSD option. See Figure 32 below.

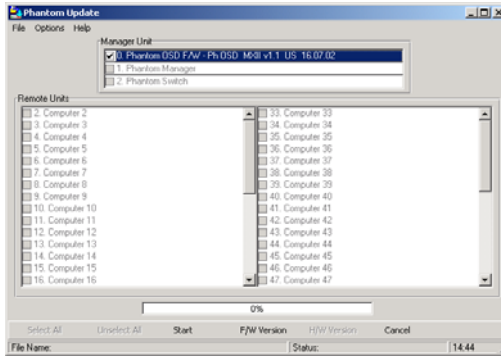4. Click F/W Version . The version number appears in the **Manager** box.

Figure 32 The OSD Manager option

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

The Phantom Manager version number

To verify the Phantom Manager version number:

1. Open the Phantom Update program.

2. Activate the Firmware Upgrade mode on the Manager OSD.

3. In the **Manager Unit** box, check the **Phantom Manager** option**.**

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

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

The Phantom MX IP Switch version number

To verify the Switch version number:

1. Open the Phantom Update program.

2. Activate the Firmware Upgrade mode on the Manager OSD.

3. In the **Manager Unit** box, check the **Phantom Switch** option.

4. Click F/W Version . The version number appears in the **Manager Unit** box.

Verifying the Remote version number

Before you can check a remote computer, you must uncheck the **Manager Unit** box options.

To verify the Remote version number:

1. Open the Phantom Update program.

2. Activate the Firmware Upgrade mode on the Manager OSD.

3. Check one or more or all of the remote computers.

4. Click F/W Version . The firmware version number appears after the computer number.

5. Click H/W Version . The hardware version number appears after the computer 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 http://www.minicom.com/phandl.htm.

Updating the firmware

Warning!

Never switch off any computer connected to the Phantom system during the updating process.

To update the firmware:

1. Open the Phantom Update program.

2. Activate the **Firmware Upgrade mode** on the Manager OSD.

3. In the Phantom Update window, check the appropriate option in the **Manager Unit** box or the desired remote computer or computers.

4. From the **File** menu, choose **Open**. The **Open** box appears. See Figure 33.

5. Navigate to the folder that contains the firmware update file. You may only see the files that match the file selection mask.
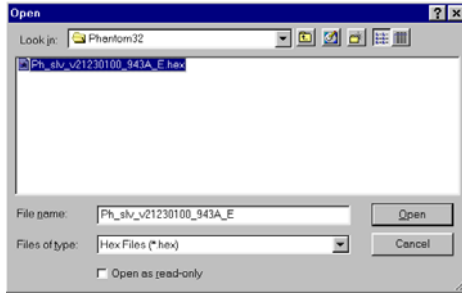
Figure 33 The Mask for a Remote computer

6. Open the file.

7. Click **Start**. The Phantom Update flashes the firmware. On completion an **Upgrade Successful** message appears.

8. 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.

Note! When you update the Manager firmware the OSD display hotkey reverts to Shift, **Shift**.

Wrong firmware

When the firmware you are trying to flash is incompatible with the Phantom units a **Not Compatible** message appears stating that some or all units are not compatible with the selected firmware.
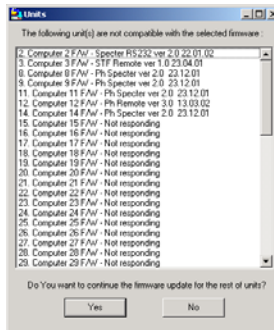

Figure 34 The Not Compatible message

In this case go to http://www.minicom.com/phandl.htm for information on how to correctly identify Phantom units.

All new Phantom units are protected from being updated with the wrong firmware. If you attempt to flash them with incompatible firmware, an **Upgrade Denied** message appears and the Phantom unit continues to function in the

Reset

Reset the software for the Phantom Manager or Specter units 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 Manager or Specter units

To reset the Manager or Specter units:

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

    For the Specters, check one or more Specters in the **Remote 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 Manager'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 from page 79, and make sure the Firmware Upgrade mode is activated.

Electricity failure

When the electricity fails while updating the Phantom firmware, do the following:

If the electricity fails during the firmware update of the Manager, a **Communication Error** message appears. The Phantom Manager enters the Upgrade mode automatically without displaying the Firmware Upgrade label. 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 Specter units a **Not Responding** or **Upgrade Error** message appears. Restart the upgrade from the beginning.

Should the update fail to work go to http://www.minicom.com/phandl.htm and download the Technical memos that explain the firmware restoration techniques

Phantom Specter USB SUN Combo keys

The SUN keyboard consists of a special keypad to perform special functions in the SUN Operating System environment. A PS/2 keyboard connected to the Phantom Manager does not have a corresponding keypad, so the Phantom USB emulates these 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**