

PX

User Guide



www.minicom.com

International HQ

Jerusalem, Israel
Tel: + 972 2 535 9666
minicom@minicom.com

North American HQ

Linden, NJ, USA
Tel: + 1 908 486 2100
info.usa@minicom.com

European HQ

Dübendorf, Switzerland
Tel: + 41 44 823 8000
info.europe@minicom.com

Technical support - support@minicom.com

Table of Contents

1. Welcome	3
2. Introduction	4
3. Key features	4
4. System components	4
5. Connecting the PX to a rack	4
6. Connecting the PX	6
7. Terminology	8
8. Client computer operating system	8
9. Initial settings	8
10. Default IP address	8
10.1 Static IP addresses for a number of units.....	8
11. Logging into the Web interface	9
11.1 SSL Certificate notes.....	10
12. Network > Configuration	10
12.1 LAN 1.....	10
12.2 KVM.net.....	11
13. Administration > User Settings	11
13.1 Adding a user.....	12
13.2 Editing a user.....	13
13.3 Deleting a user.....	13
13.4 Blocking a user.....	13
14. Security > Settings	13
15. Security > SSL Certificate	14
16. Maintenance > Firmware Upgrade	15
17. Restore Factory Settings	15
18. Saving changes and logging out	16
19. Starting a remote session	16
19.1 Taking over a busy remote session.....	17
19.2 Moving or hiding the Toolbar.....	17
19.3 Server name.....	18
19.4 Changing the performance settings.....	18
19.5 Adjusting the Video settings.....	19
19.5.1 Refresh.....	19
19.5.2 Manual Video Adjust.....	19
19.5.3 Auto Video Adjust.....	20
19.6 Power cycle.....	21
19.7 Keyboard key sequences.....	21
19.8 Synchronizing mouse pointers.....	22
19.8.1 Manual mice synchronization.....	23
19.9 Minicom logo menu features.....	24
19.10 Full screen mode.....	26
19.11 Disconnecting the remote session.....	26
20. Troubleshooting	27

20.1 - Restoring factory defaults..... 27

20.2 Booting the PX in safe mode..... 27

21. Technical specifications..... 28

22. Video resolution and refresh rates..... 29

23. Safety..... 29

24. User guide feedback..... 29

25. WEEE Compliance..... 29

© 2007 Copyright Minicom Advanced Systems. All rights reserved.

1. Welcome

Thank you for buying the PX system. This system is produced by Minicom Advanced Systems Limited.

This document provides installation and operation instructions for Minicom's PX. It is intended for system administrators and network managers, and assumes that readers have a general understanding of networks, hardware and software.

Technical precautions

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

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

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

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

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

Trademarks

All trademarks and registered trademarks are the property of their respective owners.

2. Introduction

The PX extends your KVM (keyboard, video and mouse) from any computer or server over TCP/IP via LAN, WAN or Internet connection. Now you can control, monitor and manage your servers from wherever you are, inside or outside the organization. The PX is a cost-effective hardware solution, for secure remote KVM access & control of a computer/server from the BIOS level - independent of the OS. It is designed to connect to a single computer over TCP/IP communication.

3. Key features

BIOS level control to any server's brand and model, regardless of the server condition and network connectivity, covering the entire spectrum of crash scenarios.

Compatible with all major operating systems. Supports many hardware and software configurations for the remote client and the Target server computer.

Web-based control - Browser control to a Target server, from any location via secured standard IP connection.

Multi-user view mode - Allows simultaneous users to view remote sessions. Remote control can be intuitively handed between users with appropriate permissions.

Virtual media - Mount virtually any removable mass storage devices connected to the Client computer onto the Target server.

4. System components

The PX system consists of:

- 1 PX
- 1 USB/Video cable (p/n 5CB00599)
- Rack-mounting brackets
- Optional power adapter, ordered separately

5. Connecting the PX to a rack

The PX comes with a versatile bracket in two sections see Figure 1. The bracket can be connected to the PX and then mounted on a rack in many different ways.

- Connect to the left or right side of the rack
- Connect the PX to the bracket at different angles
- Connect to different horizontal positions on the rack

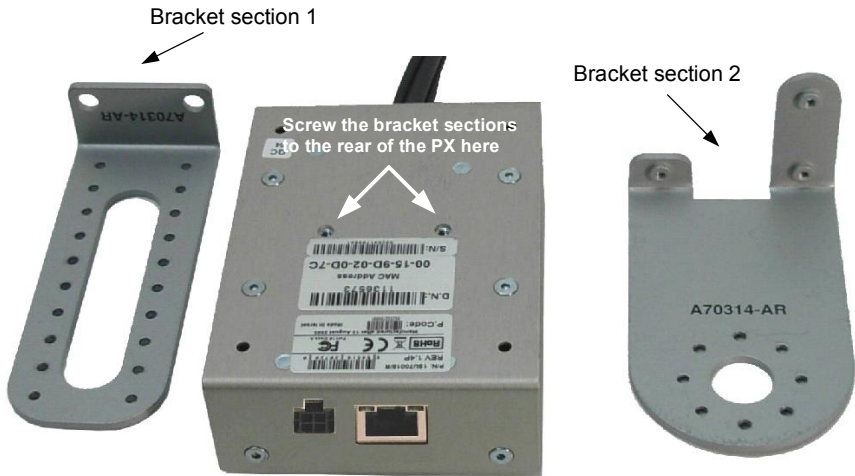


Figure 1 Rear of PX plus bracket sections

Use the screws provided to connect the bracket sections. There are 2 different types of screws. Connect the 2 parts of the brackets together with the 3 longer round headed screws. See Figure 2.

Connect section 2 of the bracket to the rear of the PX with the 2 shorter flat headed screws. **Note!** The screws fit snugly into the side of the bracket section 2 that is indented.

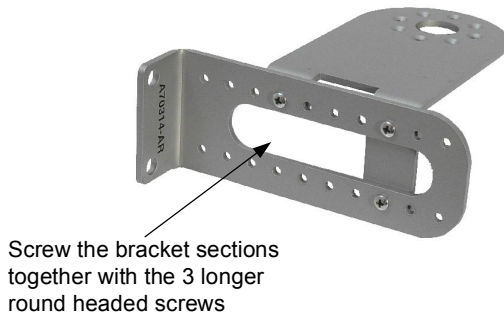


Figure 2 Connecting the bracket sections together

The figure below illustrates a possible application of the bracket.

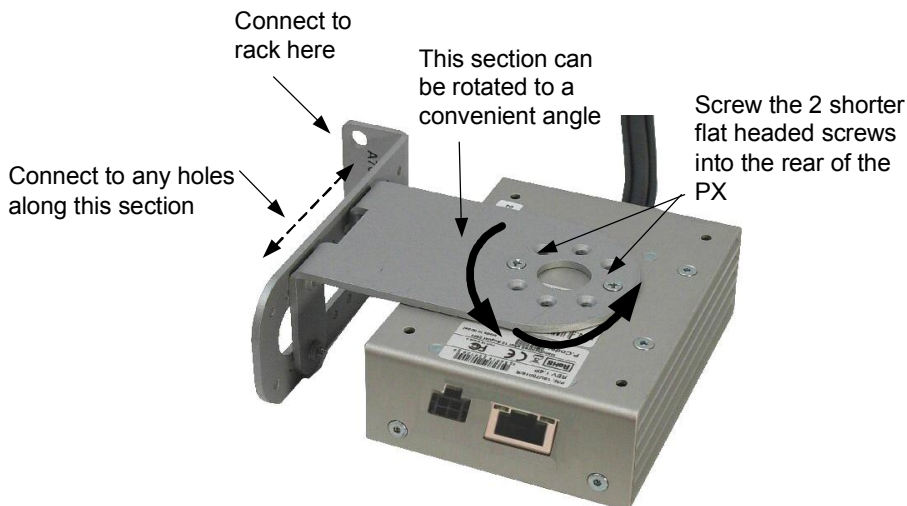


Figure 3 Bracket application

6. Connecting the PX

Where your network switch supports PoE (Power Over Ethernet), PXs can receive power via the network cable. Alternatively PXs can receive power from the optional power adapter.

To connect the PX:

1. Connect the 26 pin connector of the supplied USB/Video cable to the 26 pin port of the PX.
1. Connect the USB and Video connectors of the USB/Video cable to the relevant ports of the Target server. See Figure 4 below.
2. Connect a network cable to the RJ45 port of the PX and to your PoE enabled network switch.
3. Where relevant connect the power adapter to the PX power port.

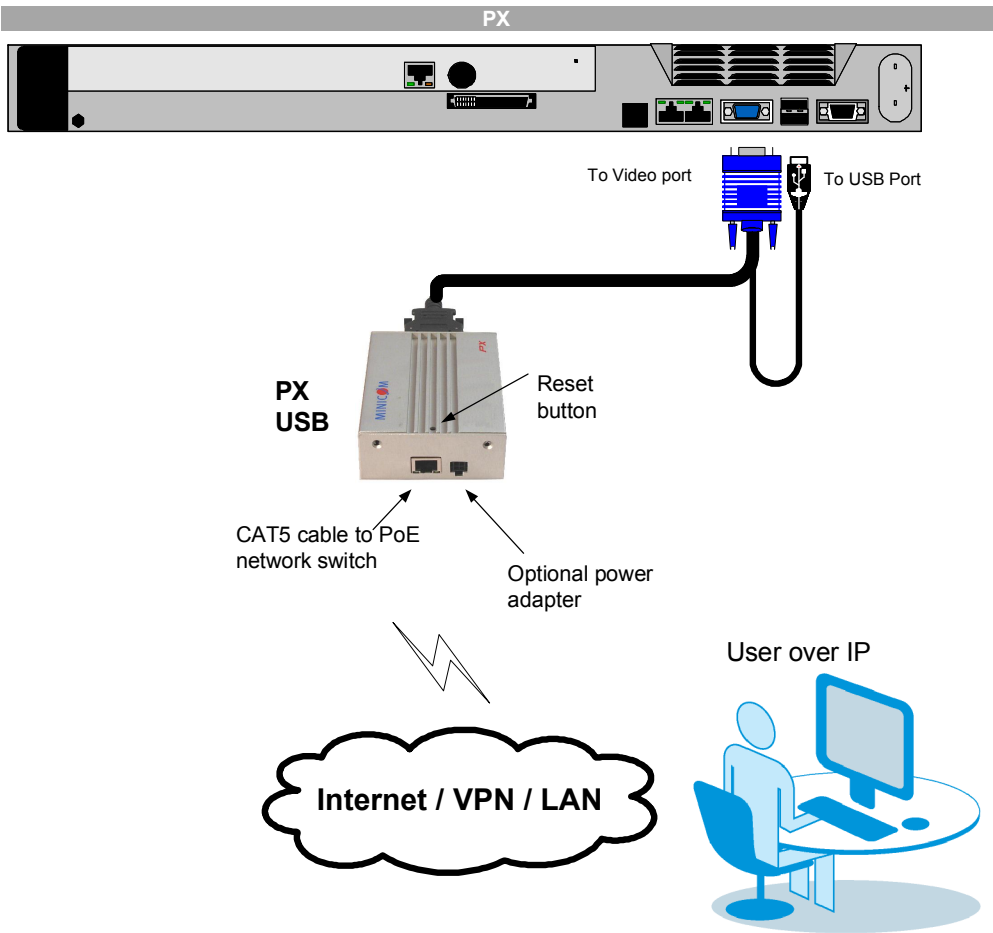


Figure 4 PX connections

PX LEDs

The PX has 2 green LEDs by the RJ45 connector. One shows the PX is connected to PoE network switch and the other shows that the Target server connected to this particular PX is being accessed.

7. Terminology

Below are some terms and their meanings used in this guide.

Term	Meaning
Target server	The computer/server accessed remotely via the PX.
Client computer	The PC running a remote session
Remote Session	The process of accessing and controlling Target Servers connected to PX from a User workstation

8. Client computer operating system

Windows 2000 or higher, with Internet Explorer 6.0 or later version. For Windows Vista a user must have administrative rights to Windows Vista and must run Internet Explorer as an administrator.

128 bit encryption support is required.

9. Initial settings

The following sections provide instructions for setting the IP address for the PX unit.

10. Default IP address

By default, PX boots with an automatically assigned IP address from a DHCP (Dynamic Host Configuration Protocol) server on the network. The DHCP server provides a valid IP address, gateway address and subnet mask.

To identify the IP address, the PX MAC address appears on the underside of the PX box. The device number (D.N.) can also be found there.

If no DHCP server is found on the network, PX boots with the static IP address: 192.168.0.155.

Note! If a DHCP server later becomes available, the unit picks up the IP settings from DHCP server. To keep the static IP address, disable DHCP – explained in section 12.1 on page 10.

10.1 Static IP addresses for a number of units

Where you want to connect more than 1 PX to the same network and there is no DHCP server, or you want to use static IP addresses, do the following:

Connect the PX units one at a time and change the static IP address of each unit before connecting the next unit.

11. Logging into the Web interface

Complete the initial setup via the Web configuration interface:

1. Open your Web browser (Internet Explorer version 6.0 or higher).
2. Type the PX system IP address - `https://IP address/config` - and press **Enter**. The login page appears, see Figure 5.

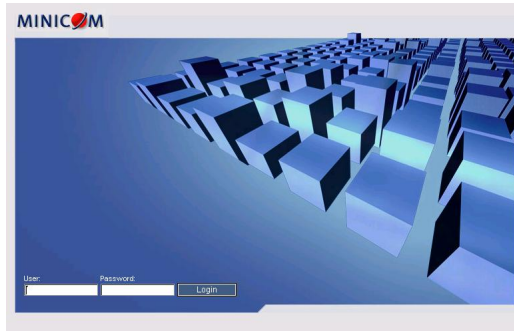


Figure 5 Login page

3. Type the default Administrator user name - **admin** - and password - **access** - (both lower case).
4. Press **Enter**. The Web interface opens at the Network Configuration page. See Figure 6.
5. Bookmark the page for easy reference.

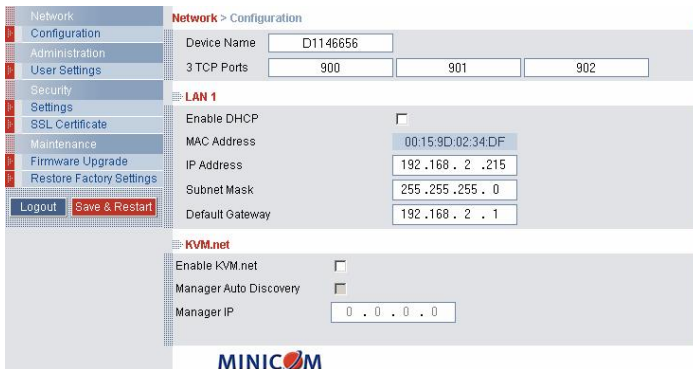


Figure 6 PX Web interface

11.1 SSL Certificate notes

When first connecting to PX's https configuration page, 2 browser security warnings appear. Click **Yes** to proceed.

The first warning disappears upon first PX client installation, when Minicom's root certificate is installed.

12. Network > Configuration

Consult your Network Administrator for the network settings.

Device name - Type a name for the PX. Default device name consists of the letter 'D' followed by the 6-digit device number (D.N.) found on the silver label on the underside of the PX box.

3 TCP Ports - Choose any 3 TCP ports. When the PX is a standalone system the ports do not have to be consecutive. When part of the KVM.net system, the ports must be the consecutive default ports of 900, 901 and 902. These default ports are suitable for the majority of installations.

Note

Firewall or router security access list must enable inbound communication through the selected TCP ports and port 443 for the PX's IP address.

For Client computer access from a secured LAN, the selected ports should be open for outbound communication.

12.1 LAN 1

Under LAN 1 in Figure 6, is the following:

Enable DHCP – When a DHCP server is active on the same network to which PX is connected, DHCP provides automatic IP assignment.

When DHCP is disabled – (Recommended) – You can assign a fixed IP address to the PX.

Consult your Network Administrator regarding the use of the DHCP. **Note!** Where you have access to the server – your configured (or default) PX device name will appear on the DHCP server's interface, making it easy to locate.

When DHCP is disabled, enter the **IP Address**, **Subnet Mask**, and **Default Gateway** for **LAN 1**, as given by your Network Administrator.

12.2 KVM.net

KVM.net is a centralized IP based system for secure control of servers and network devices, power and user administration in the data center environment.

KVM.net combines Out-Of-Band, KVM via IP access with modern IT standards and requirements. It is the most comprehensive remote server maintenance solution available in the market today.

Enable KVM.net - Check this option to allow the PX unit to be remotely managed by Minicom's **KVM.net** system. When managed by KVM.net, only Network Configuration and Restore Factory Settings are available from the PX configuration page. All other settings are managed from the KVM.net.

Manager Auto Discovery – when checked, **KVM.net** automatically detects a PX unit, if it resides on the same network segment.

Manager IP – If the PX unit resides on a different segment, type the static IP address of the KVM.net Manager. (We advise typing the static IP address of the KVM.net Manager even if the PX resides on the same network segment as the KVM.net Manager).

Note! Before assigning the PX to KVM.net, ensure that the PX is configured to 3 consecutive TCP ports 900, 901, 902.

13. Administration > User Settings

From the menu click **User Settings**, Figure 7 appears.

Administration > User Settings

User: Password: Block:

Permission: Administrator Confirm Password:

User Name	Permission	Status
1. alex	User	
2. ephraim	Administrator	
3. test1	User	
4. avishay	Administrator	
5. admin	Administrator	

MINICOM

Figure 7 User Settings

On this page an Administrator creates and edits users.

There are 3 levels of user access:

- Administrator
- User
- View only

Administrator

An Administrator has unrestricted access to all windows and settings and can “take over” any active session (explained in section 19.1 on page 17). An Administrator can change the name and password of all users.

User


A User can access/control the Target Server, but has no access to the Web configuration interface.

View only

View only can view the screen of any Target Server without keyboard and mouse control. A “view only” indicator appears on the viewer’s local mouse pointer.


13.1 Adding a user

To add a user:

1. Click  and type a name and a password. The password must be at least 6 characters – letters or numbers, and must not include the user name, even if other characters are added.



Note! The following “special” characters: &, <, >, ”, {, } cannot be used for either the user name or password.

Depending on the security level chosen the user name and password parameters are different. See section 14 on page 13.

2. Select the permission type from the **Permission** box.
3. Click , the user appears in the list of users.



13.2 Editing a user

To edit a user:

1. Select the user from the list.
2. Click . You can now change all the parameters – user name, permission and password.
3. Click , the changes are saved.

13.3 Deleting a user

To delete a user:

1. Select the user from the list.
2. Click .
3. Click , the changes are saved.

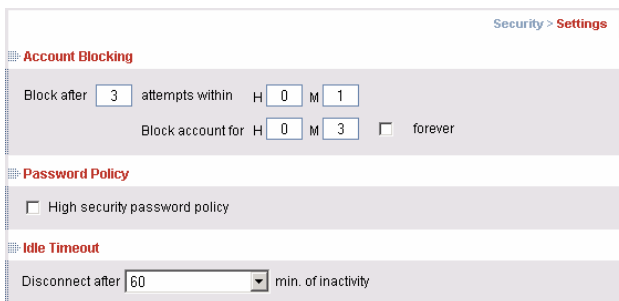
13.4 Blocking a user

An alternative to deleting a user is blocking a user. This means that the user's name and password is stored, but the user is unable to access the system. Check **Block** to block a user. Uncheck **Block** to allow the user access.

14. Security > Settings

Configure the security features, such as Account Blocking, Password Policy and Idle Timeout, as explained below.

From the **Security** section click **Settings**, the **Security Settings** appear, see Figure 8.



The screenshot shows the 'Security > Settings' interface. It contains three main sections:

- Account Blocking:**
 - 'Block after' is set to 3 attempts within H 0 M 1.
 - 'Block account for' is set to H 0 M 3, with an unchecked 'forever' checkbox.
- Password Policy:**
 - The 'High security password policy' checkbox is unchecked.
- Idle Timeout:**
 - 'Disconnect after' is set to 60 min. of inactivity.

Figure 8 Security Settings

The security Settings elements:

Account Blocking – decide on the number of attempts to login with a wrong username or password after which there is a time lock or a total block.

Password Policy – You have the option of a standard or high security level of password. The table below shows the parameters of the 2 options.

Standard security policy	High security policy
6 characters or more	8 characters or more must include at least 1 digit and 1 upper case letter and 1 "special" character as follows !@#%*^*()_+=[]:;?/
Must not include the user name	Must not include the user name

Check the box to enable the high security password policy. Unchecked, the standard security policy applies.

Idle Timeout – Select the Timeout inactivity period after which the user is disconnected from the system. Choose **No Timeout** to disable Timeout.

15. Security > SSL Certificate

You can install an SSL certificate.

To do so:

From the menu, select **SSL Certificate**, the install SSL Certificate page appears, see Figure 9.

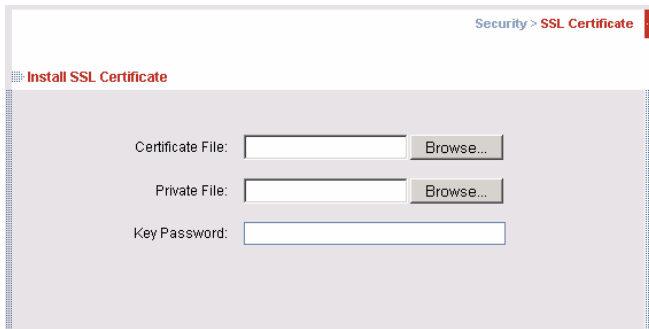


Figure 9 Install SSL Certificate page

Certificate File - Browse to locate the **cer** file.

Private File - Browse to locate the **private key** file.

Key Password - Type the “private key” password.

Click **Save & Restart**.

16. Maintenance > Firmware Upgrade

Upgrade the PX firmware to take advantage of new features. Download the firmware from Minicom's website. Save the firmware file on the Client computer.

From the menu select **Firmware Upgrade**. The Firmware Upgrade appears see Figure 10.

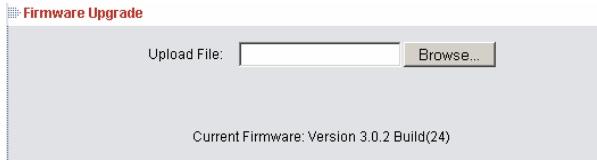


Figure 10 Firmware Upgrade

1. Locate and upload the firmware file.
2. Verify the current and uploaded version of the firmware.
3. Click **Start Upgrade**. The upgrade starts. On completion, click **Reboot**. The unit reboots. After about 30 seconds the Login page appears.

Note!

Depending on the type of firmware upgrade, user settings and mouse and video adjustments may be erased. For more information refer to the firmware release notes.

The network settings remain intact.

17. Restore Factory Settings

You can restore the PX unit to the factory settings. This restores the original PX parameters, resetting all the information added by the administrators, including: Network settings*, Users, Passwords etc.

* You have the option to preserve Network settings – explained below.

Warning! Once reset the data cannot be retrieved.

To restore factory settings:

1. From the menu select **Restore Factory Settings**. Restore Factory Settings appears see Figure 11.

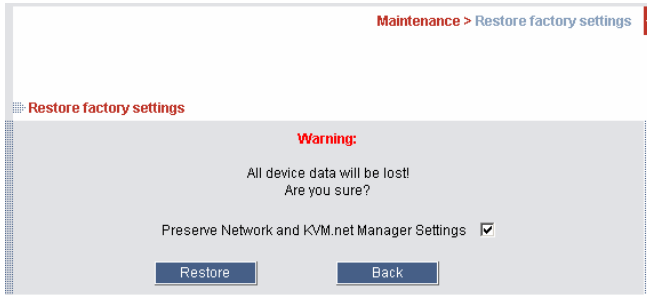




Figure 11 Restore factory settings

2. Check the box if you want to preserve Network settings.
3. Click .

18. Saving changes and logging out

To save any configuration changes and restart the PX, click .

To exit the Configuration menu and close the session, click .

Only one Administrator can log into the Configuration area at a time. An idle timeout of 30 minutes terminates the session.

19. Starting a remote session

At a Client computer open Internet Explorer (6.0 and above) and type the PX's IP address. `https://IP address`. The Login page appears. Type your username and password and press Enter. By default, the user name is: **admin** and the password is **access**, (both lower case).

On first connection install the Minicom certificate and ActiveX control. You must login as an Administrator to your computer to install the ActiveX control. Once the ActiveX control is installed, all types of users can login.

The screen of the Target Server connected directly to PX, or the currently selected server on the KVM switch with PX toolbar appears, see Figure 12.

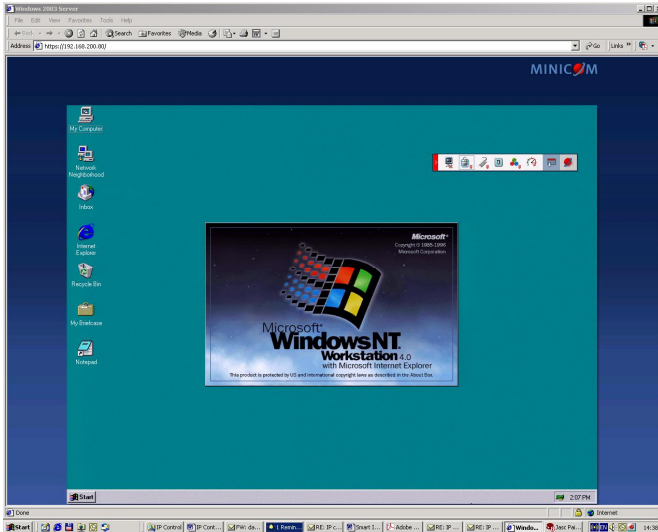


Figure 12 Remote session window

19.1 Taking over a busy remote session

When connecting to a busy Target Server an Administrator has the option to take over the Target Server. A User only has this option when the current session is run by another User, but not by an Administrator. The following message appears




Figure 13 Busy remote session options

Choose to Take Over or View Only or Cancel.

19.2 Moving or hiding the Toolbar

The Toolbar can be dragged and dropped to anywhere on the screen, by clicking

and dragging the logo .

To hide the Toolbar, either:

Double-click the PX System tray Icon .

Or

Press **F9**.

To display the Toolbar repeat the above actions. See also page 25.

To minimize the Toolbar:



Click the arrow . Click again to maximize the Toolbar.

19.3 Server name

When the PX is in standalone mode, the server name is always:Server1. If the PX is managed by KVM.net, the server name as assigned via the KVM.net can be seen in the IE title bar and in the ActiveX toolbar.

Also the server name appears from the Toolbar by clicking , or right-clicking



19.4 Changing the performance settings

You can alter the bandwidth settings from the Toolbar.

To alter the settings:

From the Toolbar, click . The Settings.. box appears, see Figure 14.

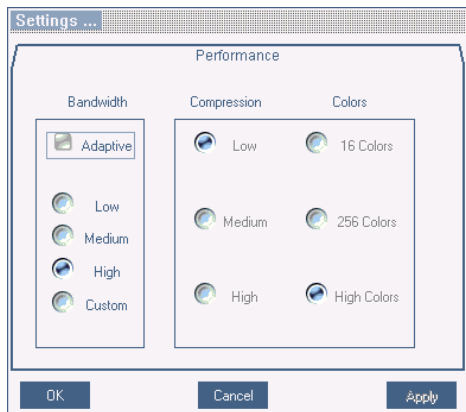


Figure 14 Settings.. box

Bandwidth

Choose from the following options

Adaptive – automatically adapts to the best compression and colors according to the network conditions.

Low - Select Low for high compression and 16 colors.

Medium - Select medium for medium compression and 256 colors. Medium is recommended when using a standard internet connection.

High - For optimal performance when working on a LAN, select High. This gives a low compression and high colors (16bit).

Custom – You can choose your own compression and color levels.

Click **OK**. The screen of the Target Server appears.

19.5 Adjusting the Video settings

To change the video settings:

From the Toolbar, click . You have the following options:

- Refresh
- Manual Video Adjust
- Auto Video Adjust

Each option is explained below.

19.5.1 Refresh

Select **Refresh** or press **Ctrl+R** to refresh the Video image. Refresh may be needed when changing the display attributes of a Target Server.

19.5.2 Manual Video Adjust

Use the manual video adjustment for fine-tuning the Target Server video settings after auto adjustment or for adapting to a noisy environment or a non-standard VGA signal or when in full-screen DOS/CLI mode.

To adjust the video manually:

Click **Manual Video Adjust**. The manual controls appear, see Figure 15. Also a red frame appears around the screen. This represents the screen area according to the Server's screen resolution. Perform the adjustments inside and relative to this frame.

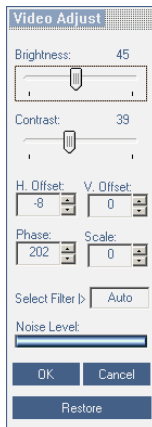


Figure 15 Manual Video Adjustments controls

Brightness / Contrast - use the scales to adjust the brightness and contrast of the displayed image. Move the sliders to change the displayed image. Click in the area of the sliders for fine-tuning.

For the following controls choose the appropriate measurement.

H. (Horizontal) Offset - defines the starting position of each line on the displayed image.

V. (Vertical) Offset - defines the vertical starting position of the displayed image.

Phase - defines the point at which each pixel is sampled.

Scale – defines the scale resolution of the session image.

Select Filter - defines the filter of the input video from the server. A higher filter reduces the noise level but makes the image heavier.

Noise Level - represents the Video "noise" when a static screen is displayed.


19.5.3 Auto Video Adjust

To adjust the video automatically:


Click **Auto Video Adjust**. The process takes a few seconds. If the process runs for more than 3 times, there is an abnormal noise level. Check the video cable and verify that no dynamic video application is running on the Target Server's desktop.

Perform the procedure every time you change the refresh rate or screen resolution.

19.6 Power cycle

The Power menu displayed when clicking the Power cycle icon  is not currently relevant to the PX.

19.7 Keyboard key sequences

Click . A list of defined keyboard sequences appears. When clicked, these transmit directly to the Target Server, and will not affect the Client computer.

For example, select **Ctrl-Alt-Del** to send this three key sequence to the Target Server to initiate its Shutdown/Login process.

To add a keyboard sequence:

Click **Add/Remove**. The Special Key Manager box appears see Figure 16.

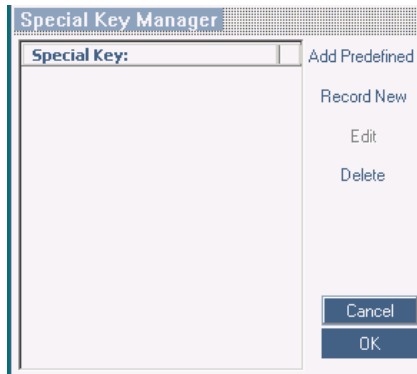


Figure 16 Special Key Manager box

To add a predefined sequence:

1. Click Add Predefined. A list of sequences appears.
2. Select the desired sequence and click OK. The sequence appears in the Special Key Manager box.
3. Click OK. The sequence appears in the Keyboard Key sequence list.

To record a key sequence:

1. From the Special Key Manager box press **Record New**. The Add Special Key box appears see Figure 19.

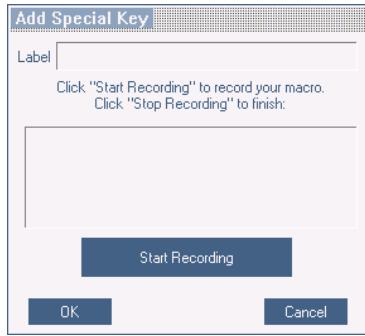


Figure 17 Add Special Key box

2. Give the key sequence a name in the Label box.
3. Click **Start Recording**.
4. Press the desired keys. The keys appear in the area provided.
5. Click **Stop Recording**.
6. Click **OK**.

To edit a key sequence:

1. From the Special Key Manager box select the desired key.
2. Click **Edit**.
3. Click **Start Recording**
4. Press the desired keys. The keys appear in the area provided.
5. Click **Stop Recording**.
6. Click **OK**.

19.8 Synchronizing mouse pointers

When working at the Client computer, two mouse pointers appear: The Client computer's is on top of the Target Server's. The mouse pointers should be synchronized.

Note! If the mouse settings on the Target Server were ever changed, you must synchronize mouse pointers manually, as explained below.

19.8.1 Manual mice synchronization

1. From the Toolbar click  / **Manual Settings**. The **Mouse Settings (USB)** box appears, see Figure 18.



Figure 18 Mouse Settings (USB) box

Absolute Mouse position

If the Operating system on the Target Server is, Windows ME or higher, then Absolute Mouse position should be selected (default).

Relative Mouse position

If the Operating system on the Target Server is, Windows 98 or Linux, Novell, UNIX or SUN, then select Relative Mouse position, the Operating System menu appears see Figure 19.



Figure 19 Mouse Settings (USB) box

1. From the drop down menu, select the Target Server's Operating system and click OK. Instructions and sliders appear.
2. Follow the instructions and set any relevant sliders to the same values as set in the Target Server's Mouse Properties window.

Note! Absolute Mouse Position works best for Windows XP, 2003 Server and Vista. However it is possible to use Relative Mouse Position and follow the instructions.

2 examples!

For Windows XP. Go to the Mouse settings on the Target Server and uncheck Enhance pointer precision.

For Linux. If Mouse Properties were ever changed for the Target Server – even if they have been returned to their original state - uncheck default Default by adjusting the Acceleration or Threshold slider.


Click **OK**. The mouse pointers should be synchronized.

Apple Macintosh Mouse

If the Target Server is a MAC computer, select Apple Macintosh Mouse.

19.9 Minicom logo menu features



Right click the Minicom logo , a menu appears. From this menu you have the following features:

Disconnect – You can disconnect the session by clicking Disconnect.

About - Click About to verify the Client, Firmware and KME (Keyboard/Mouse Emulation firmware) versions – KME is not always available when the USB cable is connected to the PX. Switch file version is not relevant to the PX.

Local Settings – Click Local settings, the Client Configuration box appears, see Figure 20

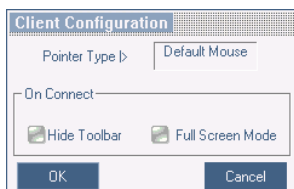


Figure 20 Client Configuration box

Pointer type – From the Drop-down menu you can change the Client computer mouse pointer to appear as a dot or to not appear at all.

Hide Toolbar – Check this option to hide the Toolbar from the next reconnection onwards. To toggle the Toolbar on and off, press **F9**. See above page 17.

Full Screen Mode - Check this option to make the remote session screen appear in full screen mode from the next reconnection onwards. To toggle the full screen mode on and off, press **F11**. Also see section 19.10 below.

Configuration – click Configuration to access the configuration pages of the PX. This saves having to exit the remote session and login to the configuration site.

Virtual Media – With Virtual Media you can mount virtually onto the Target server, removable mass storage devices connected to the Client computer.

This includes:

- Floppy drive
- CD-ROM
- DVD-ROM
- ISO Image of CD/DVD
- USB Flash Drives (Disk on key tokens)
- Miscellaneous USB memory sticks/cards identified by the operating system as removable mass storage devices

1. Click Virtual Media, the Virtual Media dialog box appears, see Figure 21. All connected mass storage devices appear in the Local Drives section.

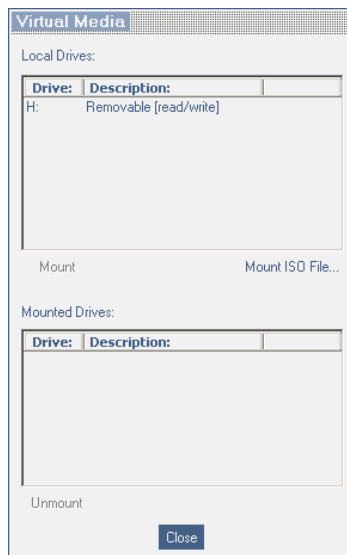


Figure 21 Virtual Media

2. Select the device to be mounted and click **Mount**. A Remote Device Warning appears, see below.

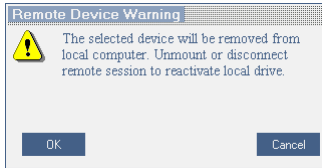


Figure 22 Remote Device Warning

3. Click **OK**. The device mounts onto the Target Server and appears as a removable or CD/DVD drive of the Target Server. It also appears in the Mounted drives section in Figure 21. Once mounted, you can use the device during the remote session as if it is connected to the Target Server.

Mounting an ISO file

To mount an ISO file, click Mount ISO File, locate the file and mount it.

19.10 Full screen mode

Work on the Target Server as if you are working on a local computer, with full screen mode.

To work in full screen mode:


1. Ensure that the Client computer has the same screen resolution as the Target Server.
2. Press **F11**. The Internet Explorer window disappears, leaving the Internet Explorer menu bar at the top.
3. Right click the Internet Explorer menu bar and check Auto-Hide. The Internet Explorer menu bar disappears. You are in full screen mode.

To exit full screen mode:

Press **F11**. Or place the mouse at the top of the window to display the Internet Explorer toolbar and click the Restore button.

Note! Full screen mode can also be activated from the Toolbar menu, see page 25.

19.11 Disconnecting the remote session

To disconnect the session, on the Toolbar, click . The Login box appears. You can re-login or close the browser window.

20. Troubleshooting

This section explains how to:

- Restore factory defaults from the PX unit
- Boot up in safe mode (when password is forgotten)

20.1 - Restoring factory defaults

Section 17 on page 15 explained how to restore factory settings from the Web interface. When you cannot access the system e.g. you have forgotten the Username or Password, you can restore factory defaults from the PX unit.

To restore a PX USB to the factory default settings, the PX USB must be connected to the PoE switch and a powered on computer.

To restore factory defaults:

Press the PX USB's Reset button (see Figure 4) for a few seconds. The Power LED blinks once and the PX USB reboots with the factory default settings.

20.2 Booting the PX in safe mode

If the administrator password is forgotten, you can boot the PX in safe mode and reconfigure the password.

1. Disconnect the network cable from the PX USB.
2. Press and hold the Reset button and re-connect the PX USB to the PoE switch.
3. Continue pressing the Reset button for 3 - 5 sec after re-connecting.
4. Release the Reset button. If a DHCP server is available, PX USB picks up an IP address from it. If there is no DHCP server, PX USB boots with static IP 192.168.2.155.
5. Type <http://192.168.2.155/config> (HTTP and not HTTPS), or type the IP address received from the DHCP server.
6. Login with user name **admin** and password **SAFEmode** (case sensitive).
7. Restore PX USB default settings from the safe mode or perform a firmware upgrade if PX USB fails to boot with its normal firmware.

Contact Minicom Technical Support for special firmware for upgrading PX USB from the safe mode.

21. Technical specifications

Operating systems	<p>Host Computer Windows 98, ME and higher, Novell, Linux and SUN Solaris</p> <p>Client Computer Windows: 2000, XP, 2003 Server or Vista. With IE 6.0 or 7.0.</p>
Resolution	<p>Host Computer Up to 1600x1200 @85Hz</p> <p>Client Computer Recommended resolution should be higher than resolution on local computer</p>
Video and Mouse Synchronization	Both auto and manual modes
Connections	<p>Ethernet - RJ45 - 10/100 Mbit/sec autosensing</p> <p>26 pin connector for Video and USB (keyboard, mouse and virtual media) cable</p>
Product dimensions HxDxW	33 x 80 x 105mm / 1.2 x 3.15 x 4.13 in
Product weight	0.3kg / 0.66 lbs
Shipping dimensions HxDxW	105 x 150 x 230mm / 4.1 x 5.9 x 9.0 in
Shipping weight	0.7kg / 1.54 lbs
Power supply	PoE 4.5W or external power supply 12V, 1000mA
Operating temp.	0°C to 40°C / 32°F to 104°F

22. Video resolution and refresh rates

Hz →	56	60	65	66	70	72	73	75	76	85	86
640x480		x		x	x	x		x		x	
720x400					x					x	
800x600	x	x				x		x		x	x
1024x768		x			x	x	x	x	x	x	
1152x864								x			
1152x900				x					x		
1280x720		x									
1280x768		x						x			
1280x960		x								x	
1280x1024		x				x		x	x	x	
1600x1200		x	x		x			x		x	

23. Safety

The device must only be opened by an authorized Minicom technician.

24. User guide feedback

Your feedback is very important to help us improve our documentation. Please email any comments to: ug.comments@minicom.com

Please include the following information: Guide name, part number and version number (as appears on the front cover).

25. WEEE Compliance

WEEE Information for Minicom Customers and Recyclers

Under the Waste Electrical and Electronic Equipment (WEEE) Directive and implementing regulations, when customers buy new electrical and electronic equipment from Minicom they are entitled to:

- Send old equipment for recycling on a one-for-one, like-for-like basis (this varies depending on the country)
- Send the new equipment back for recycling when this ultimately becomes waste

Instructions to both customers and recyclers/treatment facilities wishing to obtain disassembly information are provided in our website www.minicom.com.

Regional Offices

Germany

Kiel

Tel: + 49 431 668 7933

info.germany@minicom.com

France

Vincennes

Tel: + 33 1 49 57 00 00

info.france@minicom.com

Italy

Rome

Tel: + 39 06 8209 7902

info.italy@minicom.com

England

Camberley

Tel: + 44 (0) 1276 25053

info.uk@minicom.com

www.minicom.com



