

Smart IP Access

User Guide



Supported by:

Rackit[®]
Technology Corporation

Rackit® Technology Corporation
274 Madison Avenue, New York, NY 10016
Tel: (212) 679-0050 • Fax: (212) 679-0040
1 . 8 0 0 . 6 3 6 . 3 4 3 4
www.RackitTechnology.com

International HQ

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

North American HQ

Linden, New Jersey
Tel: + 1 908 4862100
info.usa@minicom.com

European HQ

Dübendorf, Switzerland
Tel: + 41 1 823 8000
info.europe@minicom.com

Italy

Rome
Tel: + 39 06 8209 7902
info.italy@minicom.com

www.minicom.com

Customer support - support@minicom.com

Table of Contents

Welcome	3
1. Introduction.....	4
2. Key Features	4
3. System components	4
4. The Smart IP Access unit	5
5. Pre-installation guidelines.....	6
6. Terminology.....	7
7. Client computer Operating System	7
Connecting the system.....	8
Initial Settings.....	11
8. Default IP address.....	11
9. Logging into the Web interface	11
10. Network	13
11. Configuration	13
12. Saving changes.....	14
13. SNMP settings.....	14
14. Administration.....	15
15. User Settings.....	15
16. Switch configuration	17
17. Serial Settings	18
18. Security	19
19. Installing SSL certificates.....	20
20. Event Log	21
Maintenance	22
21. Set System Time	22
22. Firmware Upgrade.....	22
23. Restore Factory Settings	23
24. Log Out	23
Configuring Serial devices	24
25. Serial Device Interface	24
26. Setting Up the RS232 port for Serial device.....	24
27. Initiating Serial device emulation	24
Operating the system	25
28. Remote operational flow	25

29. Operating through a local KVM console.....	25
30. Getting Started	25
31. Full screen mode.....	26
32. The Toolbar elements.....	27
33. Reset.....	35
34. Troubleshooting – restoring factory defaults	35
Technical Specifications	37
Video Resolution and Refresh Rates	38

© 2005 Copyright Minicom Advanced Systems. All rights reserved.

Welcome

The Smart IP Access system is produced by Minicom Advanced Systems Limited.

This document provides installation and operation instructions for Minicom's Smart IP Access. 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.

1. Introduction

The Smart IP Access extends your KVM (keyboard, video, 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 Smart IP Access 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 or to a KVM switch to access multiple servers, over TCP/IP communication.

2. Key Features

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

Low bandwidth requirement. Provides a unique ability to utilize a standard 56Kbps analog modem connection, while allowing adaptive and configurable bandwidth consumption when accessed via LAN.

Compatible with all major operating systems. Supports many hardware and software configurations for the remote client and the target server computers, as well as the KVM switch in use.

Web-based Access - Browser access to a target server, from any location via secured standard IP connection.

SNMP - SNMP traps for monitoring Smart IP Access events and operation.

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

3. System components

The Smart IP Access system consists of:

- 1 Smart IP Access
- 3 in 1 CPU cable
- 1 RS232 Cross cable
- Rack-Mount kit
- This User Guide + Quick Installation Guide

The RS232 Cross cable connects the Smart IP Access to Serial manageable devices such as Power Management units, Routers, etc.

RS232 Cross cable option

Smart IP Access has two RS232 RJ45 connectors. You can purchase another RS232 Cross cable to connect a second Serial device. P/N 5CB00566

4. The Smart IP Access unit

Figure 1 illustrates the front panel of the Smart IP Access.

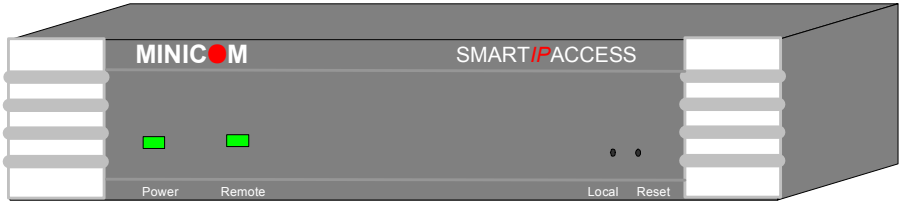


Figure 1 Smart IP Access front panel

The table below lists the LEDs, buttons and functions.

LED/Button	Function
Power	Power Indicator
Remote	Illuminates when remote session is active
Local	When pressed, Smart IP Access disconnects the Client computer's link to the Target Server, and the Local Mouse and Keyboard become operational.
Reset	Restarts the Smart IP Access unit

The figure below illustrates the rear panel of the Smart IP Access.

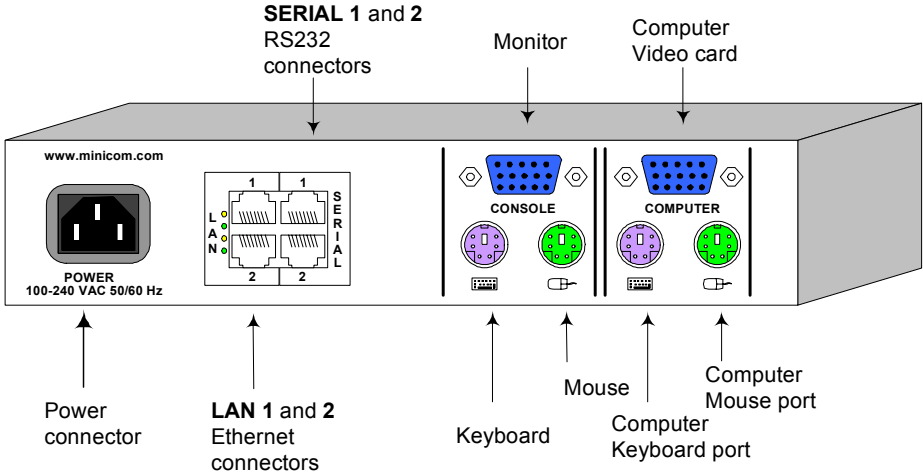


Figure 2 Smart IP Access rear panel

The table below lists the rear connectors and functions.

Connector	Function
Computer KVM	Connect a computer or KVM switch
Console KVM	Connect a keyboard, video and mouse to operate the Smart IP Access locally
Serial 1 and 2 RS232	Connect to an RS232 device
LAN 1 and 2	Connect to 10/100 Mbit Ethernet

5. Pre-installation guidelines

Place cables away from fluorescent lights, air conditioners, and machines that are likely to generate electrical noise.

6. Terminology

Below are some phrases and their meanings used throughout this guide.

Phrase	Meaning
Target Server	The computers/servers that are accessed remotely via the Smart IP Access.
Client computer	The PC running a remote Smart IP Access session
Smart IP Access Toolbar Menu	Toolbar Menu displayed at the User station Internet explorer once the Smart IP Access client component is installed, facilitating control and adjustments of Smart IP Access operations.
Target Server Pointer	Mouse pointer of the Target Server.
Smart IP Access Pointer	Semi-transparent mouse pointer created by Smart IP Access on the User station, providing better responsiveness.
Remote Session	The process of accessing and controlling Target Servers connected to Smart IP Access from a User station

7. Client computer Operating System

Any Microsoft Windows PC with Internet Explorer 5.0 or above. The support of 128 bit encryption is required if a secured connection is selected.

Connecting the system

Connect the Target Server / KVM switch to the Smart IP Access as follows:

1. Connect one end of the 3 in 1 CPU cable to the **Computer** ports of the Smart IP Access.
2. Connect the other end of the 3 in 1 CPU cable to the KVM ports of the Target Server / KVM switch.
3. To operate the KVM switches and Servers locally, connect a keyboard, mouse and monitor to the IP Access's Local Console connectors.
4. Connect Smart IP Access to the network by attaching one of the LAN ports to an Ethernet port on your Network. IP Access has two LAN interfaces – see **Initial Settings**
5. Connect the power cord.

Figure 3 and Figure 4 illustrate the connections to a computer and KVM switch respectively, with the optional KVM console.

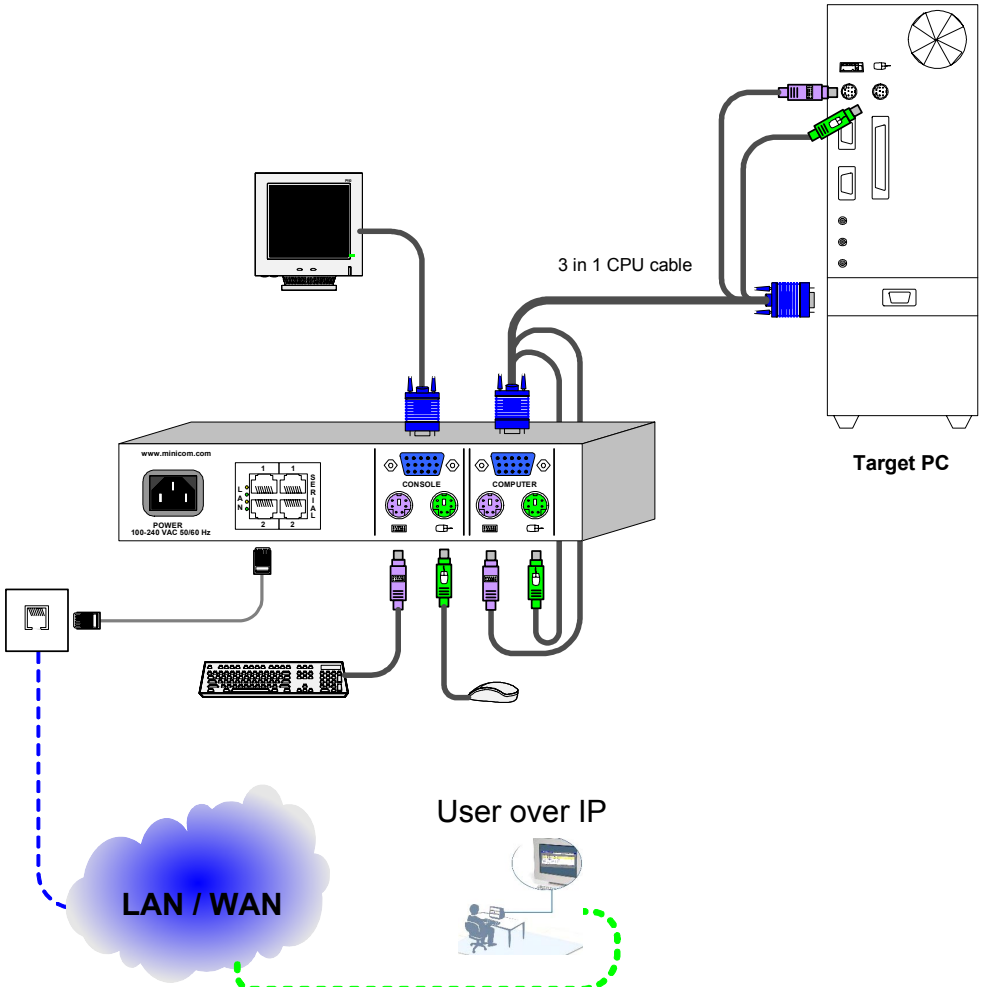


Figure 3 Smart IP Access connections to a computer

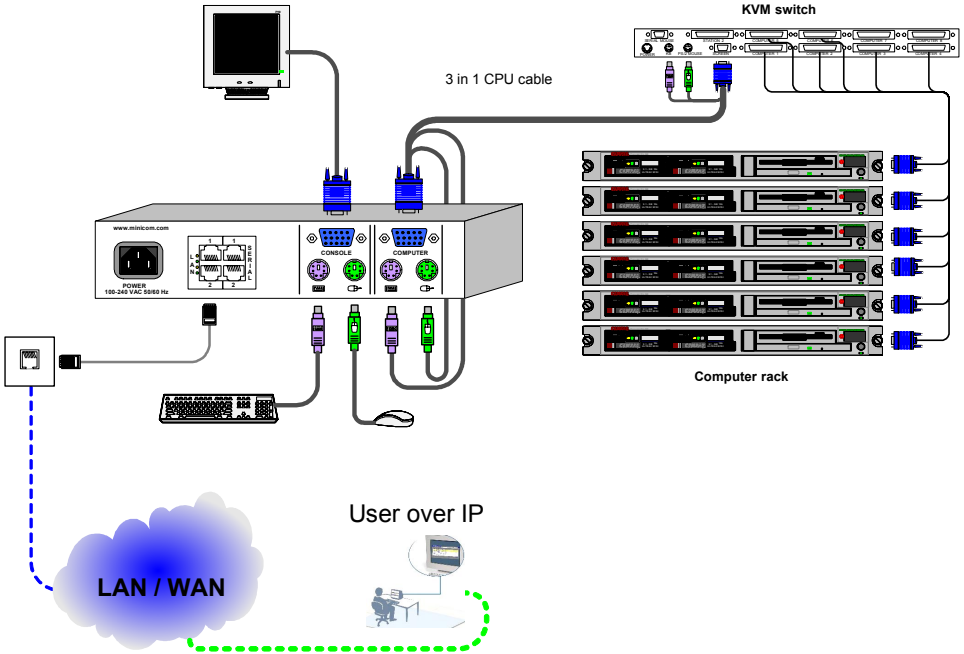


Figure 4 Smart IP Access connections to a KVM switch

Initial Settings

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

8. Default IP address

Smart IP Access has two available Ethernet Adapters, **LAN 1 and LAN 2**:

- By default, **LAN 1** boots with an automatically assigned IP address if a DHCP (Dynamic Host Configuration Protocol) server exists. The MAC address appears on a label on the underside of the IP Access box. Also on the label is the 6-digit device number (D.N.). The default device name is the letter 'D' followed by the device number
- **LAN 2** boots with the default IP configuration:

IP Address - 192.168.0.155

Subnet mask - 255.255.255.0

You can use the default Smart IP Access IP address if your computer resides on the same subnet where Smart IP Access is installed, or you can connect a Crossover LAN connector cable to the Smart IP Access on one end, and to the Ethernet adapter of your computer at the other end.

9. Logging into the Web interface

To complete the initial setup via the Web configuration interface:

1. Open your Web browser (Internet Explorer version 5.0 or higher)
2. Type the IP address of the Smart IP Access system in the address field (i.e. <https://192.168.0.155/config>) and press **Enter**. The login page appears, see Figure 5

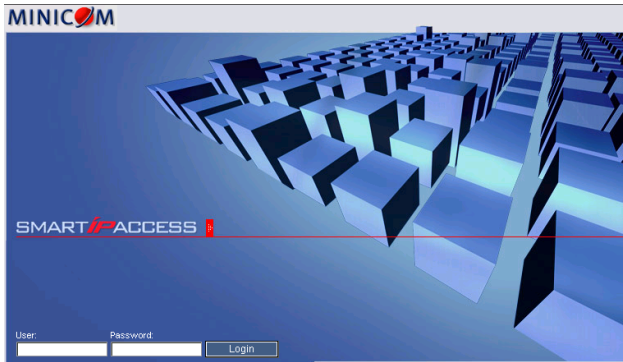


Figure 5 The Login page

3. Type the Administrator user name and password. By default, the user name is: **admin** and the password is **access** (both lower case).
4. Press **Enter**. The Web interface appears. See Figure 6.
5. Bookmark the page for easy reference.

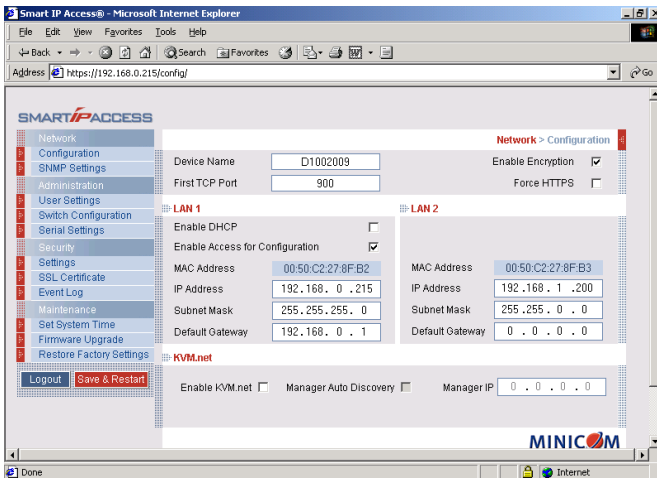


Figure 6 Smart IP Access Web interface

SSL Certificate notes

Upon first connection to Smart IP Access's https configuration web page, 2 browser security warnings appear. Click **Yes** to proceed.

The first warning disappears upon first Smart IP Access client installation, once Minicom's root certificate is installed.

The second warning can be avoided by adding a line to your window's 'hosts' file (typically at \winnt\system32\drivers\etc\hosts – edit with Notepad)

The line format should be: *any-IP any-name.kvm.net*

Example:

10.0.0.200 IPAccess.kvm.net

From now on, you can browse to Smart IP Access by typing (or book-marking) [https:// IPAccess.kvm.net](https://IPAccess.kvm.net). Minicom dedicates the kvm.net domain to this usage. You can use any device name except for **www.kvm.net** that is reserved by Minicom.

10. Network

The Smart IP Access Web interface opens at the Network configuration page. See Figure 6 above.

11. Configuration

Consult your Network Administrator for the network settings.

Device name - Type the name you wish to designate to your Smart IP Access machine. 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 IP Access box.

First TCP Port - Choose 3 consecutive ports, and type in the first port number of the series.

Note

Firewall or router security access list must enable inbound communication through the selected TCP ports for the Smart IP Access's IP address.

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

Enable Encryption - Enable Encryption if you wish to operate in a secure connection (recommended).

If enabled, the Internet Explorer at the Client computer must support 128 bit Encryption.

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

LAN 1

Enable DHCP – Check to enable the use of DHCP.

When checked, enables the Dynamic Host Configuration Protocol, which provides automatic IP assignment for Smart IP Access, if a DHCP server is active on the same network where Smart IP Access is connected.

When unchecked – (Recommended) - Allows you to assign a fixed IP address to the Smart IP Access unit.

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

Enable Access for Configuration - Click to enable access to the configuration menu from the **LAN 1**. If disabled, a remote session can only be performed via **LAN 1** and the Web configuration menu can only be accessed from **LAN 2**. This may be useful when dedicating **LAN 2** to LAN access only, to enhance security.

Enter the **IP Address**, **Subnet Mask**, and **Default Gateway** for **LAN 1** and **2**, as given by your Network Administrator. You can obtain an IP address dynamically if DHCP server is enabled.

KVM.net

KVM.net is a centralized IP based system for secure control of servers, 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 Smart IP Access unit to be remotely managed by Minicom’s **KVM.net** system.

Manager Auto Discovery – when checked, **KVM.net** automatically detects Smart IP Access, if it resides on the same network segment.

Manager IP – If Smart IP Access resides on a different segment, type a static IP address of the Smart IP Access **KVM.net**.

12. Saving changes

Click **Save & Restart** to save any configuration changes and restart the IP Access system.

13. SNMP settings

From the menu click SNMP settings. The following appears.

SNMP:

Enable traps:

Community:

SNMP Manager IP:

Figure 7 SNMP settings

From this page you can activate or deactivate SNMP logging.

Enable traps - Check to enable SNMP traps of Smart IP Access events and operation.

Community – type the SNMP community

SNMP Manager IP - Enter the SNMP Server IP address

To save changes, click **Save & Restart**.

14. Administration

In this section of the Web interface you set user permissions, switch configuration and serial settings as explained below.

15. User Settings

From the menu click User Settings, the following appears.

SMART IP ACCESS Administration > User Profile

User: Password: Block:

Permission: Administrator Confirm Password:

Add **Edit** **Delete** **Apply** **Cancel**

User Name	Permission	Status
1. admin	Administrator	

Logout **Save & Restart**

MINICOM

Figure 8 User Settings

There are 3 levels of access. Each level has its own name and password.

- Administrator
- User
- View only

Administrator

An Administrator has unrestricted access to all windows and settings and can “take over” any active session. An Administrator can change the name and password of all users.

User

A User has no access to the Web configuration interface. When accessing a Target Server a User cannot use the following:

- Advanced mouse settings
- Power – Hard Reset, Power Management

View only

You can access any Target Server and view the screen. You have no keyboard and mouse control. Only the Connect/Disconnect and Servers options appear in the menu. A “view only” indicator appears on the viewer’s local mouse pointer. A “view only” indicator appears on the viewer’s local mouse pointer.

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 9 Busy remote session options

Choose to take over or view only or cancel.



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. See section 18 on page 19 for the user name and password parameters.
2. Select the permission type from the **Permission** box.
3. Click , the user appears in the list of users.



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.

Deleting a user

To delete a user:

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

Block

Check **Block** to block access to a user. The user's name and password remain stored. Uncheck **Block** to allow the user access.

16. Switch configuration

Input the brand and model of the KVM switch connecting the IP Access to the Target Servers. From the menu choose **Switch Configuration**. The KVM settings appear, see Figure 10.

You can change the selected KVM switch at run time without reconnecting.

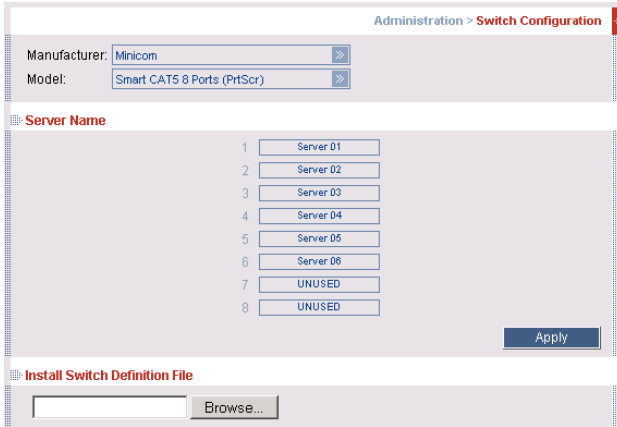


Figure 10 Switch configuration

1. Choose the manufacturer and model of the connected KVM switch. The number of possible connected servers appears in the **Server Name** section.
2. Change the name of the connected servers by selecting the server and typing a new name. Click **Apply** to save changes. **Note!** Server names left as **UNUSED** cannot be accessed.

Install switch definition file

Where the KVM switch type is not listed in the manufacturer/model drop-down lists, contact Minicom to request an updated Switch Definition file with the desired KVM switch listed.

1. Load the file onto the Client computer.
2. Locate and install the KVM switch definition file.
3. Click **Save & Restart**.

17. Serial Settings

From the menu click **Serial Settings**, the **Serial Settings** page appears, see Figure 11. Here you configure the RS232 settings that support Serial devices.

Serial Port 1

Device Name:

Baud Rate: Data Bits:

Parity: Stop Bits:

Show:

Serial Port 2

Device Name:

Baud Rate: Data Bits:

Parity: Stop Bits:

Show:




Figure 11 Serial Settings

For both Serial ports (where relevant), type in a device name and choose the correct device parameters.

Show

Check **Show** to make the device appear in the list of servers/devices that can be accessed. Where there is no device connected to the particular Serial port uncheck **Show**.

18. Security

From the **Security** section if the menu click **Settings**, the **Security Settings** page appears, see Figure 12.

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

Standard Security Password	High security Password
Any 6 characters	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

Remote Deactivation – Check the box to allow remote deactivation by the administrator. When checked, a **Disable Access** key appears in Smart IP Access toolbar panel. You can reactivate access to Smart IP Access via Smart IP Access configuration menu from **LAN 2** only.

Idle Timeout – Select the Timeout inactivity period after which the user is disconnected from the system. Timeout can also be disabled.

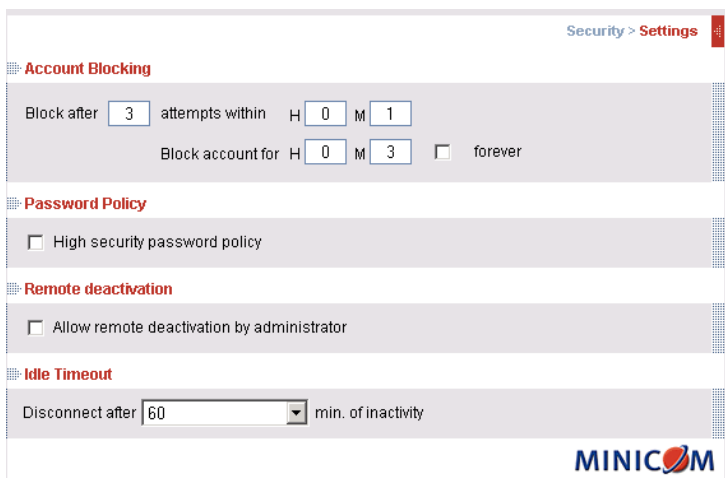


Figure 12 The Security Settings

19. Installing SSL certificates

From the menu, select **SSL Certificate**, the SSL Certificate page appears, see Figure 13.

Security > SSL Certificate

Install SSL Certificate

Certificate File: Browse...

Private File: Browse...

Key Password:

Figure 13 The SSL Certificate page

You can replace the current Smart IP Access's SSL certificate.

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**.

20. Event Log

From the menu select **Event Log**. The Event Log page appears, see Figure 14. Here you can view the device log, recording various events: security alerts, system alerts, configuration changes, and user activity.

Maintenance > Device Log

Device Log

Date	Action	User	Severity	Details
Wed, 23 Mar 2005 16:58:52	(2010) Config: User login succeeded	admin		PeerIP = 192.168.0.148
Wed, 23 Mar 2005 16:58:52	(2010) Config: User login succeeded	admin		PeerIP = 192.168.0.148
Wed, 23 Mar 2005 12:16:04	(2010) Config: User login succeeded	admin		PeerIP = 192.168.0.148
Wed, 23 Mar 2005 12:16:04	(2010) Config: User login succeeded	admin		PeerIP = 192.168.0.148
Wed, 23 Mar 2005	(2010) Config: User login succeeded	admin		PeerIP = 192.168.0.148

Figure 14 Event log

Maintenance

In the maintenance section you set the following parameters.

21. Set System Time

From the menu select **Set System Time**. The Time Settings page appears see Figure 15. Set a date and time for Smart IP Access.

Maintenance > Set system time

Time settings

Date: D: M: Y:

Time: H: M: S:

MINICOM

Figure 15 The Time Settings

22. Firmware Upgrade

Upgrade the Smart IP Access firmware to take advantage of new features. You can receive firmware updates by email or download them from the Minicom Web site. Save the firmware file on the computer from which the web configuration interface is launched.

From the menu select **Firmware Upgrade**. The Firmware Upgrade page appears see Figure 16.

Firmware Upgrade

Upload File:

Figure 16 The Firmware Upgrade page

1. Locate and install the firmware file.
2. Click **Start Upgrade**. The upgrade starts. On completion, click **Reboot** to return to the main menu.

Note

When KVM.net Manager is selected, all firmware upgrades are launched from the KVM.net Manager.

Note!

Firmware upgrade erases all User settings, KVM switch setting, mouse and video adjustments and RS232 settings. The units network settings remain intact.

23. Restore Factory Settings

From the menu select **Restore Factory Settings**. The Restore Factory Settings page appears see Figure 17.

Click **Restore** to restore the original Smart IP Access parameters, resetting all the information added by user: Network settings, Servers, Switches, Users, Passwords etc.

Warning! Once reset the data cannot be retrieved.

Note: When KVM.net is managing IP Access the data can be retrieved.

Restore factory settings

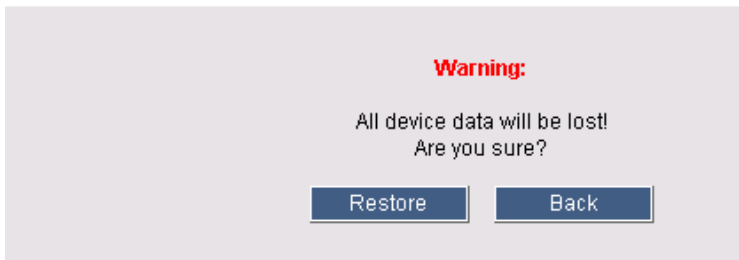


Figure 17 Restore factory settings

24. Log Out

Click **Logout** to exit the configuration menu and close the session. Note that only one Administrator can log into the configuration area at a time. An idle timeout of 30 minutes terminates the session.

Configuring Serial devices

25. Serial Device Interface

A Power Management device provides the means to turn on and off, Target Servers connected to it. It has a number of individually (relay) controlled AC power receptacles. It may also allow you to monitor current, voltage, power, temperature, and other capabilities.

Smart IP Access can control most Power Management devices via its Serial Port. Setup and control is performed at the Client computer, and is granted to Administrators only.

Smart IP Access can control Power Management devices with a Serial interface.

26. Setting Up the RS232 port for Serial device

To set up the RS232 port:

1. From a Client computer, connect to Smart IP Access as an Administrator.
2. Select **Settings/Serial Devices**.
3. Set the Serial link parameters as defined for the Serial Device.
4. Connect a Serial cable to Smart IP Access Serial port and to the Serial device.

27. Initiating Serial device emulation

To initiate Serial device emulation:

1. Connect to Smart IP Access as an Administrator.
2. Select **Reset/Serial Device**. A "Serial emulation window" opens. You may interact with a serial device, as if you were connected directly to the device itself via its serial connection (refer to the Power Management unit documentation for activities that may be performed with the specific Power Management unit).
3. When finished close the Serial Device window.

Operating the system

There are various remote operating options as follows:

28. Remote operational flow

The Smart IP Access receives Mouse and Keyboard commands from the Client computer. Smart IP Access transmits these commands to the KVM Mouse and Keyboard ports - as if physical devices were directly attached.

The desktop video images are received by Smart IP Access, captured, processed, and transmitted back to the Client computer to reflect the activity done at the Client computer.

During remote operations the Remote LED on the Smart IP Access illuminates and the 3 LEDs on the Local keyboard flash to indicate that a user is connected remotely.

29. Operating through a local KVM console

Where you need regular KVM functionality, the Smart IP Access provides a pass-through connection. Connect a mouse, keyboard and monitor to the Smart IP Access's **Console** connectors and operate the connected servers locally.

30. Getting Started

At a Client computer open Internet Explorer (5.0 and above) and input the Smart IP Access's IP address in the Address Bar. For example: <http://192.168.0.115>.

Note

This part of the Installation requires ActiveX controls to be downloaded to the Client computer. The user must be logged-on with full administrative rights.

The Smart IP Access window appears see Figure 18.

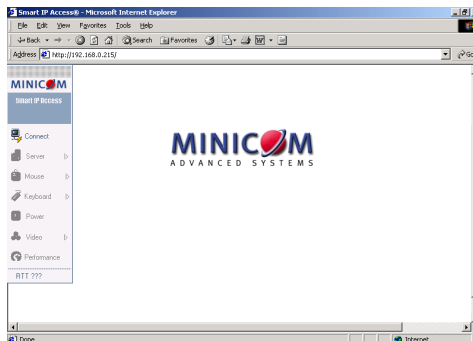



Figure 18 The Smart IP Access window

To start a remote session:

1. Click  **Connect**. The Login box appears.
2. Type in the user name and password. By default, the user name is: **admin** and the password is **access**, (both lower case).

The screen of the Target Server connected directly to Smart IP Access, or the currently selected server on the KVM switch appears. The server number appears on the Toolbar, see Figure 19.

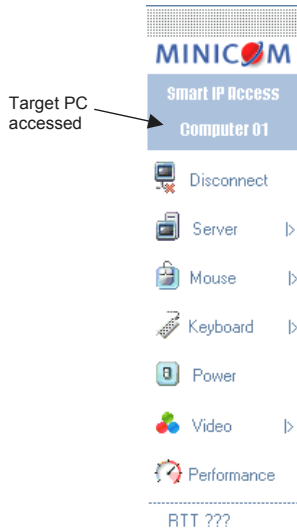


Figure 19 The Toolbar

toggling the Toolbar on and off

The Toolbar can be dragged and dropped to anywhere on the screen.

To hide the Toolbar either

Double-click the Smart IP Access System tray Icon 

Or

Press **F9**.

To make the Toolbar reappear repeat the above actions.

31. 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.

Note! You can press **F9** to hide the Smart IP Access Toolbar. See page 26.

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.


32. The Toolbar elements



Click the Minicom logo to verify the Firmware, KME (Keyboard/Mouse Emulation firmware) and Switch Configuration File versions installed on your Smart IP Access.

Connect/Disconnect



Click  to connect to the system. (When connected, the icon changes to **Disconnect**. For a secured connection, a Lock symbol appears over the icon.). The Login box appears see Figure 20. You can alter the bandwidth setting from the login box to high or low.

High-Bandwidth

For optimal performance while working in a LAN, select High-Bandwidth. This will adjust the performance as follow: Low-Compression and high color (16bit).

Low-Bandwidth

For optimal performance when using a Dialup connection, select Low-Bandwidth. This will adjust the performance as follow: High-Compression and 16 colors.

Keep Current

(Default) will use the last configured setting. The default Bandwidth characteristics, are those used in the last connection.

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

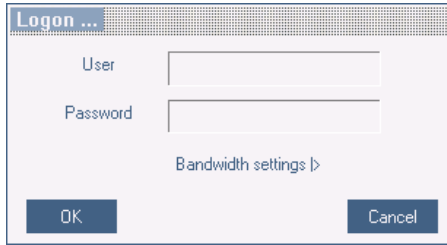



Figure 20 The Login box

Server

Click  **Server** to display a list of currently connected servers and Serial devices. Select a Target Server. The Target Server is accessed. Switch to another server by clicking the desired server in the Server list.

Mouse

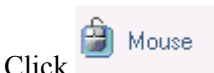
When working at the Client computer, two mouse pointers appear: The Client computer's is larger than the Target Server's.


The two pointers appear whenever your mouse pointer is inside the screen area of the Target Server. A Target Server may have a different mouse pointer speed to the Client computer. You need to synchronize them.

Warning

Before synchronizing Mouse pointers adjust the Video of the Target Server, otherwise mouse synchronization may not work. See below to adjust the video.

Video Adjustment and Mouse Pointer Synchronization, should be performed only once per Target Server.



Click  **Mouse**. Options appear to align calibrate or configure the Client and Target Server mice manually.

Synchronizing mouse pointers

Windows NT4, 2000, or 98,

When the Operating system on the Target Server is, Windows NT4, 2000 or 98, select **Mouse / Calibrate**. **Calibrate** automatically discovers the mouse speed of the Target Server and aligns the two pointers. Smart IP Access saves this alignment so calibration is only needed once per Target Server.

If the Video Noise Level is above zero, calibration may not work. Go to Video Adjustment and eliminate the noise, then perform Mouse Calibrate.

Note! For Win NT4, if the mouse settings on the Target Server were ever adjusted, you must synchronize mouse pointers manually, as explained below.

Windows XP, Windows 2003 Server, Linux, Novell, SCO UNIX, SUN Solaris

When the Operating system on the Target Server is, Windows XP, Windows 2003 Server, Linux, Novell, SCO UNIX or SUN Solaris you must synchronize the mouse pointers manually.

To synchronize mouse pointers:

1. Select **Mouse / Manual Settings**. The **Mouse Settings** box appears see Figure 21.

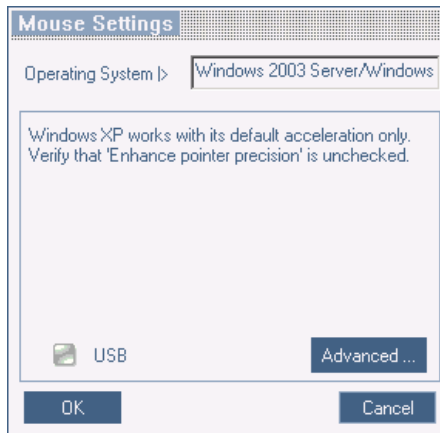



Figure 21 The Mouse Settings box

2. Select the Target Server's Operating System and click OK. Instructions and sliders appear.
3. Follow the instructions and set any relevant sliders to the same values as set in the Target Server's Mouse Properties window.

2 examples!

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

For NT4

If Mouse Properties were ever changed for the Target Server – even if they have been returned to their original state - uncheck default -  .

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

USB – This option is available for RICC and X-RICC USB and Phantom Specter USB and for unsupported operating systems and SUN Solaris. Use this option if you are sure of the custom acceleration algorithm you are using, or have been informed so by customer support.

Align / Control + M Hotkey

You only need to perform calibration once for the Target Server and only after the video adjustments. When accessing the Target Server, the mice may appear at a distance to each other.

To re-synchronize the Mouse pointers:

Select **Align** or press **Ctrl+M** simultaneously. The mice re-synchronize.

Advanced – Mouse Emulation

In the Advanced Mouse settings, you can set the type of mouse that you would like Smart IP Access to emulate. We recommended not changing the advanced settings unless there is erratic mouse behavior (the mouse is making random clicks and jumping arbitrarily around the screen).


Click  the Mouse Emulation box appears see Figure 22.




Figure 22 Mouse Emulation box

Select the mouse connected to the Local Console port on the Smart IP Access, e.g. if the local mouse is a non-Microsoft 2 button mouse, select **Standard Mouse** and uncheck **Microsoft Mouse**.

Switch Acceleration - In some KVM switch brands (for example G&D, Rittal), the switch accelerates the mouse on top of the acceleration provided by the operating system. If necessary, check this option to compensate (decelerate) the switch acceleration and achieve full synchronization.

Max Rate - this defines the maximum mouse report rate. For Sun Solaris the default value is 20 in order to support older Sun versions.

Keyboard

Click  **Keyboard**. 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 keyboard sequences:

1. Click **Add/Remove**. The Special Key Manager box appears see Figure 23.

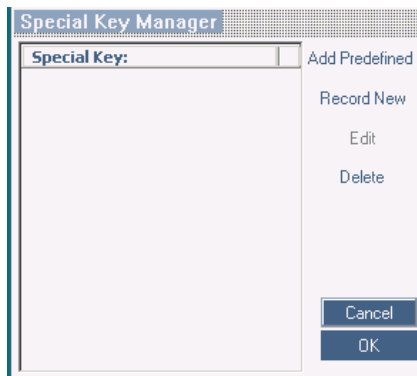


Figure 23 The Special Key Manager box

2. Add a predefined sequence from the list provided; record a new sequence or edit an existing one.
3. To Record or Edit a Key Sequence, press **Record New**. The Add Special Key box appears see Figure 24.

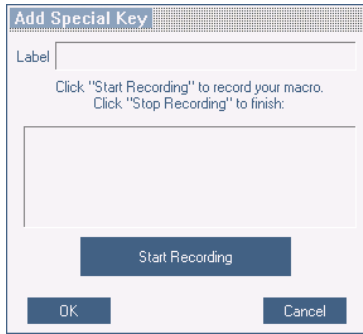


Figure 24 The Add Special Key box


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

Editing a key sequence

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**.

Power

To send a hard reset through KB-Power™ to the Target Server click  Power . A prompt appears before the Reset activates. See also section 33 page 35.

Video

Click  the following appear in a menu:

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.

Auto Adjust – Click to automatically detect the Target screen’s resolution and adjust the video accordingly. Target Servers generally require video adjustments. Perform the procedure once for each Target Server and Windows Resolution.

To adjust the video:

Select **Auto Adjust**. The process is completed in a few seconds. During the process, an indicator bar shows the progress. If the process runs more than 3 times, this indicates an abnormal noise level. Check the video cable and verify that no dynamic video application is running on the Target Server’s desktop.

During Auto Adjustment, the background freezes.

We recommend opening Windows Explorer (or similar) in the background and in full-screen DOS/CLI mode, perform a manual video adjustment.

Note!

Each Target Server needs its own video adjustment.

Manual Video Adjustment

Manual Adjust – Click to open a slider bar to adjust the Target Server video manually.

Use the manual video adjustment option for fine-tuning after auto adjustment or for adapting to a noisy environment or a non-standard VGA signal.

To adjust the video manually:

1. Select Video / Manual Adjust. The Video Adjustments controls appear see Figure 25. 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.

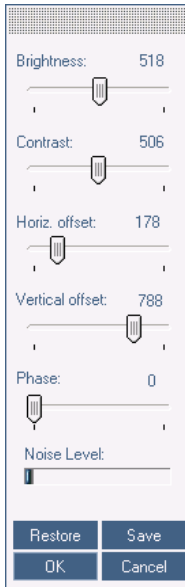


Figure 25 The Video Adjustments controls

Video Adjustment controls

Move the sliders to change the displayed image. Click in the area of the sliders for fine-tuning.

Brightness / Contrast - use the scales to adjust the brightness and contrast of the displayed image.

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

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

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

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

RTT

RTT – Round-trip-time is the time it takes, (in milliseconds) for a packet to travel from the Client computer to the Smart IP Access and back. (RTT measurement is ICMP based, similar to the 'Ping'. Note that if Ping is blocked, the RTT will show a Timed Out value).

33. Reset

Hard Reset

KB-Power™ and KB-Power IPMI™ offer a power control over remote electronics devices through a remote session.

Select Power to send a Power Cycle command to the remote electronic device. (Such as the Target Server)

Only a user with administrative privileges can initiate a Hard Reset command.

Power Management Console

The Power Management Console can be accessed when the Power Management Console is activated. Only users with Administrative privileges can access it.

34. Troubleshooting – restoring factory defaults

Section 23 on page 23 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 Smart IP Access unit.

To restore factory defaults:

1. Switch on the unit.
2. Within 3 seconds of switching on, press the Reset and Local buttons simultaneously.
3. Release the Reset button. The Remote LED illuminates.
4. Release and re-press Local Button. The Remote LED turns off.
5. Wait 2 minutes until the unit finishes booting.
6. Login to the lower network interface (**LAN 2**) to the default IP address of the unit: <http://192.168.0.155/config>. The Login box appears see Figure 26.



The image shows a login interface with a yellow background. It contains two input fields: one labeled 'User:' and one labeled 'Password:'. Below these fields is a prominent orange button with the text 'Login' in white.

Figure 26 The login box

7. Type username: **admin** , password: **SAFEmode**. (Case sensitive). This username and password works only after the reset procedure described above. A menu appears.
8. From the menu choose **Restore Factory Settings**. A warning appears see Figure 27.



Figure 27 Warning

9. Select Restore. The factory defaults are restored. When the process finishes Figure 28 appears.



Figure 28 Reboot

10. Click **Reboot** to restart the unit.

Technical Specifications

Operating systems	<p>Target Server Win 3.1, 9X, 2000, XP, NT4, 2003 Server, Dos, Novell 3.12 – 6, Linux</p> <p>Client Computer Windows computer with IE 5.5 or higher and ActiveX</p>
Resolution	<p>Target Server Up to 1600x1200 @85Hz</p> <p>Client Computer Recommended - resolution should be higher than on Target Server</p>
Video and mouse synchronization	Both auto and manual modes
Connections	<p>Ethernet – 2 X RJ45 – 10/100 Mbit/sec autosensing</p> <p>Serial – 2 X RJ45</p> <p>Local KVM connection – Screen HDD15, Keyboard./Mouse – MiniDIN6</p> <p>Computer / switch connection – Screen HDD15, Keyboard./Mouse – MiniDIN6 3 in 1 cable 1.8m</p>
Weight	1.204kg/ 2.65lbs
Dimensions (H x D x W)	44 X 230 X 215mm / 1.7 x 9 x 8.5in
Power supply	Internal Switching 85 – 265 VAC 50 / 60 Hz
Operating temperature	0°C to 40°C / 32° to 104°F
Storage temperature	-40°C to 70°C/-40°F to 158°F
Humidity	80% non condensing relative humidity

Video Resolution and Refresh Rates

	56Hz	60Hz	66Hz	70Hz	72Hz	73Hz	75Hz	85Hz
VESA 640x480		x			x		x	x
VESA 800x600	x	x			x		x	x
VESA 720x400				x				x
VESA 820x464						x		
VESA 1024x768		x		x			x	x
VESA 1152x960							x	
VESA 1280x860		x						x
VESA 1280x1024		x					x	x
VESA 1600x1200		x	x	x			x	x



©Copyright Minicom Advanced Systems

