Smart 108 / 116 IP
User Guide
# Table of Contents

1. Welcome ............................................................................................................................ 4
2. Introduction ....................................................................................................................... 5
3. Key features ...................................................................................................................... 5
4. System components ........................................................................................................ 6
5. Compatibility ..................................................................................................................... 6
6. Terminology ...................................................................................................................... 6
7. The Smart 108/116 IP unit ................................................................................................ 6
   7.1 LED and button table ........................................................................................................ 7
   7.2 Connector table ............................................................................................................. 7
8. Pre-installation guidelines ............................................................................................... 8
   8.1 Avoiding general rack mounting problems ........................................................................ 8
   8.2 Rack mounting the Smart 108/116 IP .............................................................................. 8
9. Connecting the system .................................................................................................. 10
   9.1 The RICC/ROCs ............................................................................................................. 10
      9.1.1 Connecting a RICC/ROC PS/2 ................................................................................ 11
      9.1.2 Connecting a RICC/ROC USB ................................................................................ 12
      9.1.3 Connecting a RICC SUN ....................................................................................... 12
   9.2 Connecting to the network ........................................................................................... 13
   9.3 Connecting the CAT5 cables ....................................................................................... 13
   9.4 Connecting a KVM console ......................................................................................... 13
   9.5 Connecting the power supply .................................................................................... 13
10. Initial settings - Default IP address ............................................................................. 13
    10.1 Static IP addresses for a number of units .................................................................... 14
11. Logging into the Web interface ................................................................................... 15
    11.1 SSL Certificate notes .................................................................................................. 16
12. Network > Configuration .............................................................................................. 16
    12.1 LAN ............................................................................................................................ 17
    12.2 Centralized Management ......................................................................................... 18
13. Network > SNMP Settings ............................................................................................ 18
    13.1 SNMP Events recorded .............................................................................................. 19
14. Administration > User Settings ................................................................................... 19
    14.1 Adding a user .............................................................................................................. 19
    14.2 Editing a user ............................................................................................................. 20
    14.3 Deleting a user ......................................................................................................... 20
    14.4 Blocking a user ....................................................................................................... 20
15. Administration > Switch Configuration ...................................................................... 20
16. Administration > User Targets .................................................................................... 21
17. Security > Settings ....................................................................................................... 22
18. Security > SSL Certificate ........................................................................................... 23
19. Maintenance > Firmware Upgrade ............................................................................. 23
20. Restore Factory Settings ............................................................................................. 24
21. Saving changes and logging out ................................................................................. 25
22. Starting a remote session ................................................................. 25
  22.1 Sharing a remote session ............................................................. 26
    22.1.1 Private remote session ......................................................... 27
  22.2 Displaying the Toolbar .............................................................. 27
  22.3 Session profile ........................................................................ 27
  22.4 Full screen mode ...................................................................... 28
  22.5 Changing the performance settings ......................................... 28
  22.6 Adjusting the Video settings ..................................................... 29
    22.6.1 Refresh ............................................................................. 30
    22.6.2 Video Adjust ..................................................................... 30
    22.6.3 Advanced ......................................................................... 30
  22.7 Power cycle ............................................................................ 31
  22.8 Keyboard key sequences .......................................................... 31
  22.9 Synchronizing mouse pointers ............................................... 33
    22.9.1 Aligning the mice pointers .............................................. 33
    22.9.2 Calibrating mice pointers .............................................. 33
    22.9.3 Manual mouse synchronization ..................................... 33
  22.10 Switching to a different server/device ...................................... 35
  22.11 Disconnecting the remote session .......................................... 35
23. Troubleshooting - Safe mode ....................................................... 35
  23.1 Entering Safe mode ................................................................ 36
  23.2 Restoring factory defaults ...................................................... 37
  23.3 Restoring the device firmware ................................................ 38
24. Switching between computers ..................................................... 39
  24.1 The keyboard hotkeys ............................................................. 39
25. The OSD ..................................................................................... 39
  25.1 Navigating the OSD ............................................................... 40
  25.2 Selecting a computer .............................................................. 40
  25.3 The OSD settings - F2 ............................................................. 40
    25.3.1 The General settings ....................................................... 41
  25.4 F7 Defaults ........................................................................... 43
  25.5 The Ports settings ................................................................. 43
    25.5.1 Editing the computer name ............................................. 43
    25.5.2 Keyboard (KB) ............................................................... 44
  25.6 The Time settings ................................................................. 44
    25.6.1 Scan (SCN) - Label (LBL) - Time out (T/O) ................. 44
  25.7 Users .................................................................................... 45
  25.8 Security .................................................................................. 46
  25.9 The OSD HELP window – F1 ............................................... 46
  25.10 Scanning computers – F4 ..................................................... 47
  25.11 Tuning – F5 .......................................................................... 47
  25.12 Moving the label – F6 .......................................................... 48
  25.13 DDC – F10 .......................................................................... 48
26. Upgrading the Smart 108/116 IP firmware .................................. 49
  26.1 Obtaining the Update software and latest firmware ............... 49
  26.2 System requirements for the Update software ......................... 49
  26.3 Connecting the Smart 108/116 IP System ............................... 49
  26.4 Connecting the RS232 Download cable .................................. 50
  26.5 Installing the software .......................................................... 50
  26.6 Starting and configuring the Update software ......................... 50
26.7 Verifying the version numbers .................................................................................................. 52
  26.7.1 Smart 108/116 IP Switch version ...................................................................................... 52
  26.7.2 RICC/ROC version ........................................................................................................... 53
26.8 Obtaining new firmware ............................................................................................................ 53
  26.8.1 Updating the firmware ....................................................................................................... 53
26.9 Restoring factory settings ......................................................................................................... 54

27. Update software - Troubleshooting .......................................................................................... 55
  27.1 Communication Error message ............................................................................................. 55
  27.2 Electricity failure .................................................................................................................... 55

28. Technical specifications .............................................................................................................. 56
29. Video resolution and refresh rates .......................................................................................... 57
30. Safety ........................................................................................................................................ 58
31. User guide feedback .................................................................................................................. 58
32. WEEE compliance .................................................................................................................... 58

© 2009 Copyright Minicom Advanced Systems. All rights reserved.
1. Welcome

Thank you for buying the Smart 108/116 IP system. This system is produced by Minicom Advanced Systems Limited.

This document provides installation and operation instructions for Minicom’s Smart 108/116 IP. 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.
Section I

Section I explains how to configure and operate the Smart 108/116 IP system remotely over IP. Section II on page 39, explains how to operate the Smart 16 IP switching system locally through the On Screen Display (OSD).

2. Introduction

The Smart 108/116 IP 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 up to 8 / 16 remote servers from wherever you are, inside or outside the organization. The Smart 108/116 IP is a cost-effective hardware solution, for secure remote KVM access & control of 8 / 16 computers/servers from the BIOS level - independent of the OS. One local analog or one remote digital IP user can access and control 8 / 16 multi-platform (PS/2, SUN, USB) servers.

The Smart 108/116 IP is based on Minicom’s innovative ROC technology in which each computer/ server is directly connected to the switch via ROC dongles using only standard CAT5 cable at a distance of up to 30m/100ft in a star configuration. No external power is needed at the remote ROC.

The Smart 108 IP and the Smart 116 IP are functionally the same. The Smart 108 IP has 8 Server ports and the Smart 116 IP has 16 Server ports.

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.

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

**Multi-user share mode** - Allows up to 5 simultaneous users to share a remote sessions.

**Security** - Supports the highest security standards for encryption (256 bit AES and HTTPS) and authentication for remote user and advanced OSD management with multi-layer security for local user.

**Centralized Management** - Can be controlled by the Minicom’s AccessIT / KVM.net systems for centralized over-IP management of distributed data center locations.
4. System components

The system consists of:

- 1 Smart 108 IP (p/n 0SU70032) or 1 Smart 116 IP (p/n 0SU60005)
- Rack mounting set (p/n 5AC20247)
- 1 RS232 Download cable (p/n 5CB40419)
- ROCS - PS/2, USB. (Ordered separately). CAT5 cables (1.5m provided)

5. Compatibility

The Smart 108/116 IP is compatible with:

- PS/2, SUN and USB computers/servers
- VGA, SVGA, or XGA monitors
- Windows, Linux, UNIX and other major operating systems

6. Terminology

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

<table>
<thead>
<tr>
<th>Term</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target server</td>
<td>The computers/servers that are accessed remotely via the Smart 108/116 IP.</td>
</tr>
<tr>
<td>Client computer</td>
<td>The PC running a remote Smart 108/116 IP session</td>
</tr>
<tr>
<td>Remote session</td>
<td>The process of remotely accessing and controlling Target Servers connected to Smart 108/116 IP from a user workstation</td>
</tr>
</tbody>
</table>

7. The Smart 108/116 IP unit

Figure 1 illustrates the front panel of the Smart 108/116 IP.
7.1 LED and button table

<table>
<thead>
<tr>
<th>LED</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power</td>
<td>Power Indicator</td>
</tr>
<tr>
<td>Remote</td>
<td>Illuminates when remote session is active</td>
</tr>
<tr>
<td>Link</td>
<td>Unit is connected to the network</td>
</tr>
<tr>
<td>Button</td>
<td>Function</td>
</tr>
<tr>
<td>Local</td>
<td>When pressed, Smart 108/116 IP disconnects the Client remote session and</td>
</tr>
<tr>
<td></td>
<td>the local mouse and keyboard become operational. The Remote LED turns off.</td>
</tr>
<tr>
<td>Reset</td>
<td>Press and hold for more than 7 seconds to reset the Smart 108/116 IP</td>
</tr>
</tbody>
</table>

Figure 2 illustrates the rear panel of the Smart 108/116 IP. The Smart 108 IP has 8 Server ports.

7.2 Connector table

<table>
<thead>
<tr>
<th>Connector</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Console KVM</td>
<td>(Optional) Connect a keyboard, video and mouse to operate the Smart</td>
</tr>
<tr>
<td></td>
<td>108/116 IP locally</td>
</tr>
<tr>
<td>Serial</td>
<td>This port is for future Serial functionality</td>
</tr>
<tr>
<td>Flash</td>
<td>To update firmware of the analogue part of the Smart 108/116 IP system</td>
</tr>
<tr>
<td></td>
<td>- OSD, Switch, RICC(s) and RoC(s).</td>
</tr>
<tr>
<td>LAN</td>
<td>Connect to 10/100 Mbit Ethernet. Green LED illuminates when unit is</td>
</tr>
<tr>
<td></td>
<td>connected to a 100 Mbit/sec network. Yellow Led illuminates when unit is</td>
</tr>
<tr>
<td></td>
<td>connected to a 10 Mbit/sec network.</td>
</tr>
<tr>
<td>Server ports</td>
<td>Connect to servers via RICC/ROCs</td>
</tr>
</tbody>
</table>
8. Pre-installation guidelines

- Place cables away from fluorescent lights, air conditioners, and machines that are likely to generate electrical noise
- Place the Smart 108/116 IP on a flat, clean and dry surface
- The Smart 108/116 IP is not intended for connection to exposed outdoor lines
- Ensure that the maximum distance between each computer and the Smart 108/116 IP, does not exceed 10m/33ft for RICCs and 30m/100ft for ROCs.

8.1 Avoiding general rack mounting problems

Elevated operating ambient temperature
The operating ambient temperature of the rack environment may be greater than the room ambient when installing into a closed or multi-unit rack assembly. So install the equipment in an environment compatible with the maximum rated ambient temperature.

Reduced airflow
Install the equipment in a rack in such a way that the amount of airflow required for safe operation is not compromised. Leave a gap of at least 5cm/2” each side of the Smart 108/116 IP.

Mechanical loading
Mount the equipment in the rack in such a way that a hazardous condition is not achieved due to uneven mechanical loading.

Circuit overloading
When connecting the equipment to the supply circuit, consider the effect that overloading of circuits might have on over-current protection and supply wiring. Reliable earthing of rack-mounted equipment should be maintained. Give attention to supply connections other than direct connections to the branch circuit (e.g. use of power strips).

8.2 Rack mounting the Smart 108/116 IP
Rack mount the Smart 108/116 IP using the supplied Rack-mount kit. The brackets can be placed in 2 possible positions, see Figure 3.
Place the brackets towards the front of the unit so that the unit can be mounted front facing, or place the brackets towards the rear of the unit so that the unit can be mounted rear facing. Figure 4 illustrates the bracket connected for rear facing. Screw the bracket to the Smart 108/116 IP using the screws provided.
9. Connecting the system

Figure 5 illustrates the Smart 108/116 IP system overview.

9.1 The RICC/ROCs

Each computer/server is directly connected to the Smart 108/116 IP via the appropriate RoC or RICC using CAT5 cable in a star configuration. No external power is needed at the remote RICC/ROCs. The RICC/ROCs draw their power from the computer’s keyboard port (RICC/ROC PS/2, SUN) or from the USB port (RICC/ROC USB). The figures below illustrate the RoC PS/2 and RoC USB.
9.1.1 Connecting a RICC/ROC PS/2

The connections for RICC/ROC PS/2 are exactly the same. Figure 8 illustrates the RICC PS/2.

You can connect the RICC/ROC PS/2 to a powered on computer, but it must be in the following order:

1. Connect the Mouse connector to the computer’s Mouse port.
2. Connect the Keyboard connector to the computer’s Keyboard port.
3. Connect the Screen connector to the computer’s Video port.

Failure to connect in the above order while the server is running, may lead to the mouse malfunctioning until the server is rebooted.
9.1.2 Connecting a RICC/ROC USB

The RICC/ROC USB supports Windows 98 SE and later, MAC, SUN and SGI, and all modern Linux distributions. The connections for RICC/ROC USB are exactly the same. Figure 9 illustrates the RICC USB and its connections.

To connect the RICC/ROC USB:

1. Connect the Screen connector to the computer’s Video port.
2. Connect the USB connector to the computer’s USB port.

9.1.3 Connecting a RICC SUN

Figure 10 illustrates the RICC SUN and its connections.

To connect the RICC SUN:

1. Connect the Screen connector to the computer’s Video card.
2. Connect the Keyboard connector to the computer’s Keyboard port.
9.2 Connecting to the network
Connect the network cable to the LAN port of the Smart 108/116 IP. This must be done before powering on the Smart 108/116 IP.

9.3 Connecting the CAT5 cables
1. Connect one connector to the RICC/ROCs RJ45 port.
2. Connect the other connector to one of the Smart 108/116 IP’s Computer ports.
3. Follow the above 2 steps for each computer.

9.4 Connecting a KVM console
To operate the system locally, connect a KVM console to the Smart 108/116 IP:
1. Connect the monitor’s connector to the Smart 108/116 IP’s Monitor port.
2. Connect the keyboard’s connector to the Smart 108/116 IP’s Keyboard port.
3. Connect the mouse’s connector to the Smart 108/116 IP’s Mouse port.

9.5 Connecting the power supply
1. Using the Power cord provided, connect the Smart 108/116 IP to a socket outlet with grounding connection. Only use the power cord supplied with the unit.
2. Switch on the Smart 108/116 IP.

10. Initial settings - Default IP address
The following sections provide instructions for setting the IP address for the Smart 108/116 IP unit. See Figure 11 for an overview of the boot-up process.

By default, Smart 108/116 IP 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 Smart 108/116 IP MAC address appears on the underside of the Smart 108/116 IP dialog box. The device number (D.N.) can also be found there.

If no DHCP server is found on the network, Smart 108/116 IP 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 17.
10.1 Static IP addresses for a number of units

Where you want to connect more than 1 Smart 108/116 IP to the same network and there is no DHCP server, or you want to use static IP addresses, do the following:
Connect the Smart 108/116 IP 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

Client computer operating system. - Windows 2000 or higher, with Firefox 3 or Internet Explorer 6.0 or later version. Linux with Firefox 3.

Complete the initial setup via the Web configuration interface:

1. Open your Web browser and type the Smart 108/116 IP system IP address - https://IP address/ - and press Enter. The login page appears, see Figure 12.

![Figure 12 Login page](image)

2. Click the arrow to select Configuration mode. (Clicking the arrow toggles between the option to access a remote session or the configuration pages).

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 13.
11.1 SSL Certificate notes

When first connecting to Smart 108/116 IP’s https configuration page, 2 browser security warnings appear. Click Yes to proceed.

The first warning disappears upon first Smart 108/116 IP 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 Smart 108/116 IP. 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 Smart 108/116 IP dialog box. If the DHCP server is published in the DNS server, you may connect to the Smart 108/116 IP using the device name, as follows:

https://DeviceName

**TCP Port** - Choose any TCP port from port #800 to 65535. (When managed by Centralized Management, the port number can be changed from the management interface if needed).
Notes

Firewall or router security access list must enable inbound communication through the selected TCP ports for the Smart 108/116 IP’s IP address. (Default TCP port is 900, default web interface TCP port is 443).

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

12.1 LAN

Under LAN in Figure 13, is the following:

Enable DHCP – When a DHCP server is active on the same network to which Smart 108/116 IP is connected, DHCP provides automatic IP assignment.

When DHCP is disabled – (Recommended) – You can assign a fixed IP address to the Smart 108/116 IP.

Consult your Network Administrator regarding the use of the DHCP. Note! Where you have access to the server – your configured (or default) Smart 108/116 IP 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 Centralized Management

Minicom’s Centralized Management IP based systems, for secure control of servers and network devices, power and user administration in the data center environment. The Centralized Management systems combine Out-Of-Band, KVM via IP access with modern IT standards and requirements. They are the most comprehensive remote server maintenance solutions available in the market today.

**Enable Centralized Management** - Check this option to allow Smart 108/116 IP to be remotely managed by a Centralized Management system.

**Manager Auto Discovery** – when checked, the Centralized Management system automatically detects the Smart 108/116 IP, if it resides on the same network segment.

**Manager IP Address** – If Smart 108/116 IP resides on a different segment, type the static IP address of the Centralized Management Manager. (We advise typing the static IP address of the Manager even if the Smart 108/116 IP resides on the same network segment as the Manager).

13. Network > SNMP Settings

From the menu click SNMP settings. The following appears.

![Figure 14 SNMP](image)

From this page you can activate or deactivate SNMP logging.

**Enable traps** - Check to enable sending SNMP traps of Smart 108/116 IP events and operation.

**Community** – type the SNMP community.

**SNMP Manager IP** - Enter the SNMP Server IP address.
13.1 SNMP Events recorded
See table in Appendix 1 on page 59 for a list of all events recorded.

14. Administration > User Settings
From the menu click User Settings, Figure 15 appears.

![Figure 15 User Settings](image)

On this page an Administrator creates and edits users.

There are 2 levels of user access:

- Administrator
- User

**Administrator**

An Administrator has unrestricted access to all windows and settings and can change the name and password and Target server permissions of all users.

**User**

A User can access/control Target Servers, but cannot use the advanced mouse settings.

A User has no access to the Web configuration interface.

**14.1 Adding a user**

To add a user:

1. Click **Add** 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 17 on page 22.

2. Select the permission type from the Permission dialog box.

3. Click Apply, the user appears in the list of users.

### 14.2 Editing a user

To edit a user:

1. Select the user from the list.

2. Click Edit. You can now change all the parameters – user name, permission and password.

3. Click Apply, the changes are saved.

### 14.3 Deleting a user

To delete a user:

1. Select the user from the list.

2. Click Delete.

3. Click Apply, the changes are saved.

### 14.4 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.

### 15. Administration > Switch Configuration

Give the servers connected to the Smart 108/116 IP unique names, so that users accessing the system can identify the servers easily.

To do so:

1. From the menu click Switch Configuration. The Switch Configuration window appears, see Figure 16.
2. In the **Server Name** section change the name of the connected servers by selecting the server name and typing a new name. Click **Apply** to save changes.

**Install switch definition file**

In the event that Minicom’s Technical Support updates the Switch Definition file, the file will be available in the Support section of our website - [www.minicom.com](http://www.minicom.com).

1. Download the file onto the Client computer and unzip it.

2. Locate and install the KVM switch definition file. The switch definition file is replaced.

**16. Administration > User Targets**

By default access is allowed to all servers for all user types. You may define the access rights of each user separately.

To do so:

1. From the menu click **User Targets**. The User Targets Configuration window appears, see Figure 17.
2. Select a user from the User drop-down menu.

3. Check the Target servers the user can access (according to his access permissions). To select all Target servers, press Select All.

4. Click Apply, the selection is saved.

5. Repeat the above steps for other users.

17. 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 18.

The Security Settings fields:

**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.

<table>
<thead>
<tr>
<th>Standard security policy</th>
<th>High security policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>6 characters or more</td>
<td>8 characters or more must include at least 1 digit and 1 upper case letter and 1 “special” character as follows !@#$%^*()_-+=[&quot;]':;?{/</td>
</tr>
<tr>
<td>Must not include the user name</td>
<td>Must not include the user name</td>
</tr>
</tbody>
</table>

Check the dialog 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.

18. 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 19.

![Figure 19 Install SSL Certificate page](image)

Certificate File - Browse to locate the cer file.

Private File - Browse to locate the private key file in pem format.

Remove any passwords from the private key file.

Click Save & Restart.

19. Maintenance > Firmware Upgrade

Upgrade the Smart 108/116 IP firmware to take advantage of new features. Download the firmware from the Support section of Minicom’s website – [www.minicom.com](http://www.minicom.com). Save the firmware file on the Client computer.
From the menu select **Firmware Upgrade**. The Firmware Upgrade window appears showing the current firmware version see Figure 20.

![Figure 20 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, the following settings may be erased:
- User settings, server names, mouse and video adjustments. For more information refer to the firmware release notes.
- The network settings remain intact.

### 20. Restore Factory Settings

You can restore the Smart 108/116 IP unit KVM/IP portion to the factory settings. This restores the original Smart 108/116 IP parameters, resetting all the information added by the administrators, including: Network settings*, Servers, Switches, Users, Passwords etc.

(The OSD preserves the server names and other settings. Restore the OSD settings from the OSD, see page 43).

* 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 21.
2. Check the dialog box if you want to preserve Network settings.

3. Click [Restore].

**21. Saving changes and logging out**

To save any configuration changes and restart the Smart 108/116 IP click [Save & Restart]. You must press [Save & Restart] after making changes to the following pages:

- Network>Configuration
- Network>SNMP Settings
- Security>Settings
- Security>SSL Certificate

To exit the Configuration menu and close the session, click [Logout].

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

**22. Starting a remote session**

At a Client computer open the web browser and type the Smart 108/116 IP’s IP address. https://IP address. The Login page appears, see Figure 22. Type your username and password and press Enter. By default, the user name is: **admin** and the password is **access**, (both lower case).

Note! There is a shortcut to the Configuration pages from the login page. Click the arrow [Remote Access] to toggle between the option to access a remote session or the configuration pages.

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.
When using a Firefox browser, install the Minicom Firefox add-on. The screen of the currently selected Target Server with Minicom toolbar appears see Figure 23.

![Figure 23 Remote console window](image)

On the remote console you have the following:

**Server Confirmation label** – This confirms the identity of the current server accessed and disappears by default after 30 seconds, (this period can be adjusted in the OSD – explained in Section II of the guide). It appears again when switching to a different server. The currently accessed server identity can be checked any time by looking at the **Server name** on the Internet Explorer title bar.

### 22.1 Sharing a remote session

When connecting to a Target Server that other users are already connected to, the following message appears.
Up to 5 users can share the same remote session.

22.1.1 Private remote session

When starting a remote session and there are no other logged in users a user can prevent other users from connecting to his session, from the Toolbar – see Exclusive session on page 28.

22.2 Displaying the Toolbar

The Toolbar appears briefly at the top of the screen, see Figure 23. It disappears when the mouse is not over it. To make it reappear, glide the mouse over the top of the screen. To display the Toolbar permanently, click the pinpoint icon on the Toolbar.

22.3 Session profile

You have several remote session display options to choose from. From the Toolbar click / Session Profile. The Session Profile dialog box appears, see Figure 25.

You have the following options:

Local Mouse Pointer – You can change the Client computer mouse pointer to appear as a dot or to not appear at all. Default is a regular shaped mouse cursor.

On connect

Auto Hide – Check this option to hide the Toolbar from the next connection onwards.
**Full Screen** - Check this option to make the remote session screen appear in full screen mode from the next connection onwards. To toggle the full screen mode on and off, press **F11**. (See section 22.4 below).

**Exclusive Session** - When starting a remote session and there are no other logged in users, a user can prevent other users from logging into the session by selecting the Exclusive Session check box.

### 22.4 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 browser window disappears.

To exit full screen mode:

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

**Note**! Full screen mode can also be activated from the Session Profile dialog box, see above.

### About

Click /About to verify the Client, Firmware, KME (Keyboard/Mouse Emulation firmware) and Switch file versions installed on your Smart 108/116 IP.

### 22.5 Changing the performance settings

You can alter the performance settings from the Toolbar.

To alter the settings:

From the Toolbar, click /Performance. The Performance dialog box appears, see Figure 26.
Performance mode

You can choose fixed or adaptive – these are explained below.

Fixed mode

Fixed mode allows you to select the high, medium or low bandwidth option. For example, in a LAN environment, it is best to set the bandwidth setting on High. For VPN and internet environments you may want to alter the settings to increase responsiveness.

Bandwidth - Choose from the following options

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

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

Low - Select Low for high compression and 16 colors.

Adaptive mode

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

Click OK. The chosen setting take effect and the screen of the last accessed Target Server appears.

22.6 Adjusting the Video settings

To change the video settings:

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

- Refresh
- Video Adjust
- Advanced

Each option is explained below.
22.6.1 Refresh
Select Refresh to refresh the Video image. Refresh may be needed when changing the display attributes of a Target Server.

22.6.2 Video Adjust
To adjust the video automatically:
Click **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 where necessary for each Target Server or new screen resolution.

22.6.3 Advanced
Use the Advanced video adjustment options 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:
Click Advanced. The manual controls appear, see Figure 27.
After adjusting the video manually, you can always revert to Auto settings by clicking Auto Video Adjust – explained in section 22.6.2 below.

![Figure 27 Manual Video Adjustments controls](image)

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

**V. 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.

Adjust Phase and Scale to reduce noise level to a minimum.

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

### 22.7 Power cycle

This button 上 is for future Serial power management options.

### 22.8 Keyboard key sequences

Click 下. 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 dialog box appears see Figure 28.

![Figure 28 Special Key Manager dialog box](image.png)
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 dialog box.
3. Click OK. The sequence appears in the Keyboard Key sequence list.

To record a key sequence:
1. From the Special Key Manager dialog box press **Record New**. The Macro dialog box appears see Figure 29.

![Macro dialog box](image)

2. Give the key sequence a name in the Label field.
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 dialog 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**.
22.9 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. The following explains what to do if they are not synchronized.

**Warning**

Before synchronizing mouse pointers adjust the video of the Target Server, (explained above) otherwise mouse synchronization may not work..

22.9.1 Aligning the mice pointers

When accessing the Target Server, the mice may appear at a distance to each other. To align the mouse pointers:

From the Toolbar click / Align. The mice align.

22.9.2 Calibrating mice pointers

A Target Server may have a different mouse pointer speed to the Client computer. Calibrating automatically discovers the mouse speed of the Target Server and aligns the two pointers.

To perform the calibration when the Target Server Operating system is, Windows NT4, 2000 or 98:

From the Toolbar click / Calibrate. Smart 108/116 IP 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 try to eliminate the noise by pressing Auto video adjust and/or adjusting the bars in Manual video adjust, then perform the mouse calibration.

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

22.9.3 Manual mouse synchronization

If the mouse settings on the Target Server were ever changed, or when the Operating system on the Target Server is: Windows XP or later, Linux, Novell, SCO UNIX or SUN Solaris you must synchronize the mouse pointers manually.

To manually synchronize mouse pointers:

1. From the Toolbar click / Mouse Settings. The Mouse Settings dialog box appears see Figure 30.
1. From the drop down menu, select the Target’s Operating system. Instructions and sliders appear.

2. Follow the instructions and set any relevant sliders to the same values as set in the Target’s Mouse Properties window.

3. Click OK to save the settings

2 examples!

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

For Windows 2000. If Mouse Properties were ever changed for the Target – even if they have been returned to their original state - uncheck default \( \square \) Default. Click OK. The mouse pointers should be synchronized.

USB

The USB option in the Mouse Settings dialog box is available for USB to PS/2 adapters, RICC/ROC 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.

22.9.3.1 Advanced – Mouse Emulation

In the Advanced Mouse settings, you can set the type of mouse that you would like Smart 108/116 IP to emulate. We recommend not changing the advanced settings
unless there is erratic mouse behavior (the mouse is making random clicks and jumping arbitrarily around the screen).

Click [Advanced] the Mouse Emulation dialog box appears see Figure 31.

![Figure 31 Mouse Emulation dialog box](image)

Select the mouse connected to the Local Console port on the Smart 108/116 IP, e.g. if the local mouse is a non-Microsoft 2 button mouse, select **Standard Mouse** and uncheck **Microsoft Mouse**.

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

**22.10 Switching to a different server/device**

To connect to a different server/device:

1. From the Toolbar, click ![server](image). A list of connected servers/devices appears.
2. Click the desired server. The screen of the server appears.

**22.11 Disconnecting the remote session**

To disconnect the session, on the Toolbar, click ![exit](image). The Login page appears. You can re-login or close the browser window.

**23. Troubleshooting - Safe mode**

From the Safe mode you can:

**Restore factory defaults** - When you cannot access the system e.g. you have forgotten the Username or Password, restore factory defaults from the Safe mode. (Section 20 on page 24 explained how to restore factory settings from the Web interface).
**Restore the device firmware** – If during a firmware update there is a power failure and you can no longer access the system you can restore the device firmware from the Safe mode.

### 23.1 Entering Safe mode

To enter Safe mode:

1. Press and hold down the **Local** button for 3-4 seconds and at the same time power up the Smart 108/116 IP. The device boots up in Safe mode.

2. Wait until the unit finishes booting (1-2 minutes).

3. You need to know the IP address of the Smart 108/116 IP. The IP address depends on whether there is a DHCP server on the network. If there is, the DHCP server assigns an IP address to the Smart 108/116 IP. If there is no DHCP server, the unit boots with the static IP address 192.168.2.155. See Figure 32 for an overview of this procedure.

![Diagram showing Safe mode procedure]

To access the configuration page of the unit, open Internet Explorer 6.0 or higher and type: `http://IPaddress/config` (*Note: Safe mode is HTTP, not HTTPS*)

Default user: **admin**

Default password: **SAFEmode** (case sensitive)

*Figure 32 Safe mode procedure*
Open Internet Explorer and type the following into the Address dialog box: http://IP address/config. (Do not start the address with https). The Login page appears, see Figure 33.

4. Type username: admin, password: SAFEmode. (Case sensitive). (This username and password works only in Safe mode). A menu appears, see Figure 34.

23.2 Restoring factory defaults

To restore factory defaults:

1. From the menu choose Restore Factory Settings. A warning appears see Figure 35.
2. Click Restore. A further warning appears, see below.

Figure 36 Warning

3. Click OK, the factory defaults are restored. When the process finishes Figure 37 appears.

Figure 37 Reboot

4. Click Reboot to restart the unit.

23.3 Restoring the device firmware

Contact Minicom Technical Support support@minicom.com, to receive the Upgrade firmware required to restore the device firmware. Save the Upgrade firmware on the hard disk of a computer connected to the network.

To restore the device firmware:

1. From the Safe mode menu choose Firmware Upgrade.

2. Locate the Upgrade firmware and click Install, then click Start Upgrade. The firmware upgrades. When the process finishes Figure 38 appears.

Figure 38 Reboot

3. Click Reboot to restart the unit.
Section II

Section II explains how to operate the Smart 108/116 IP Switching system locally (sections 24 and 25) and how to upgrade the Smart 108/116 IP firmware (section 0). Section 27 deals with troubleshooting.

24. Switching between computers

Switch between the connected computers by either:

- Keyboard hotkeys
- The OSD (On Screen Display)

24.1 The keyboard hotkeys

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

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

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

25. The OSD

To display the OSD:

1. Ensure there is no remote user connected. To disconnect the remote user press the **Local** button on the Smart 108/116 IP.

2. Press **Shift** twice. The OSD Main window appears. See Figure 39. Lines with yellow text show active computers. Lines with blue text show inactive computers. The Type column indicates a computer “C” is connected to the port.

![Figure 39 OSD Main window](image)
25.1 Navigating the OSD
To navigate up and down use the Up and Down arrow keys.
To jump from one column to the next (when relevant) use the Tab key.
To exit the OSD or return to a previous window within the OSD press Esc.

25.2 Selecting a computer
To select a computer:
1. Navigate to the desired computer line.
   Or, type the port number of the desired computer.
2. Press Enter. The selected computer is accessed. A Confirmation label appears showing which computer is accessed.

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

25.3 The OSD settings - F2
Press F2. The OSD Settings window appears see Figure 40.

![Figure 40 Settings window](image)

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

With the red line on the word GENERAL, press Enter. The General settings window appears see Figure 41.

![General Settings window](image)

From this window you can do the following:

**25.3.1.1 Security**

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

These levels are as follows:

**25.3.1.2 Administrator (Status A)**

The Administrator can:

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

**25.3.1.3 Supervisor (Status S)**

The Supervisor can:

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

**25.3.1.4 User (Status U)**

There are 6 different Users in the Smart 108/116 IP system. Each User has a Profile set by the Administrator that defines the access level to different computers. There are 3 different access levels - explained on page 45.
25.3.1.5 Activating password protection
By default OSD access is not password protected. Only the Administrator can password-protect the OSD or disable password protection.

To do so:
1. In the General settings window navigate to the Security line.
2. Press the Space bar to toggle between Security On and Off. The password dialog box appears.
3. Type the Administrator’s password (default is “admin”).
4. Press Enter. The new security status is set.

25.3.1.6 Changing the OSD hotkey
By pressing Shift, Shift the OSD appears. You can replace Shift, Shift with any of the following:
- Ctrl, Ctrl
- Ctrl, F11
- Print Screen

To change the hotkey:
1. Navigate to the Hotkey line.
2. Press the Space bar to toggle between options. To display the OSD in future press the new hotkey.

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

To change the Autoskip setting:
1. Navigate to the Autoskip line.
2. Toggle between the options using the Space bar.

25.3.1.8 Serial port
This option is disabled in Smart 108/116 IP. Leave this option on its default setting ON.
25.3.1.9 Changing the Keyboard language

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

1. Navigate to the Keyboard language line.
2. Toggle between the options using the Space bar.

25.3.1.10 Editing the Switch name

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

25.4 F7 Defaults

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

25.5 The Ports settings

In the Settings window navigate to the Ports line and press Enter. The Ports settings window appears see Figure 42.

![Figure 42 Ports Settings window](image)

25.5.1 Editing the computer name

In this window you can edit the computer names with up to 15 characters. (To avoid confusion the names given in the OSD should match the names given in the web configuration).

To erase a character:

Select it and press the Space bar. Blank spaces remain in place of the erased character.
To erase an entire line:
Place the cursor at the beginning of the line. Keep the **Space bar** depressed until the line is erased.

### 25.5.2 Keyboard (KB)

The Smart 108/116 IP operates with Windows, Linux, HP UX, Alpha UNIX SGI, DOS, Novell, MAC-USB or Open VMS.

By default the keyboard mode is set to PS which is suitable for Intel based computers and UNIX servers connected to ROC/RICCs USB.

For systems with UNIX servers connected to ROC/RICCs PS/2 set the KB column as follows:

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

To change the setting:

1. On the desired line, press Tab to jump to the KB column.
2. Toggle between the options using the Space bar.

### 25.6 The Time settings

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

![Figure 43 Time settings window](image)

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

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

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

To set the above periods:

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

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

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

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

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

### 25.7 Users

In the Settings window navigate to the Users line and press Enter. (Note! Users is only enabled if the security status is set to On, see page 42). The Users settings window appears see Figure 44.

![Figure 44 Users settings window](image)

There are 3 different access levels. These are:

- **Y** – Full access to a particular computer.
- **V** – Viewing access only, to a particular computer (No keyboard/mouse functionality)
- N – No access to a particular computer – A TIMEOUT label appears if access is attempted

To give each user the desired access level:

1. Navigate to the desired computer line and User column.
2. Toggle between the options using the Space bar.

### 25.8 Security

In the Settings window navigate to the Security line and press **Enter**. (Note! Security is only enabled if the security status is set to On, see page 42). The Security settings window appears see Figure 45.

![Security settings window](image)

The ‘T’ column on the right hand side stands for Type of access permission.

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

To change a user name or password:

1. Navigate to the desired line and column.
2. Type a new user name / password. User authentication is done solely via the password there is no security significance to the names.

By default the User Profile settings are full access.

### 25.9 The OSD HELP window – F1

To access the HELP window press F1. The HELP window appears see Figure 46.
Please note!

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

25.10 Scanning computers – F4

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

To activate scanning:
1. Press **Shift** twice to open the OSD.
2. Press **F4**. Your screen displays each active computer sequentially, with the Scan label appearing in the top left corner.

To deactivate scanning:
Press **F4**.

25.11 Tuning – F5

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

To adjust the screen image:
1. Navigate to the computer you wish to adjust.
2. Press **F5**. The screen image of the selected computer appears, together with the Image Tuning label.
3. Adjust the image by using the **Right** and **Left** Arrow keys.
4. When the image is satisfactory, press **Esc**.
Note! Picture quality is relative to distance. The further away a remote computer is from the Smart 108/116 IP, the lower the image quality, and the more tuning needed. So place the higher resolution computers closer to the Switch.

**25.12 Moving the label – F6**

Position the Confirmation label anywhere on the screen.

To position the label from the Main window:
1. Navigate to the desired computer using the **Up** and **Down** arrow keys.
2. Press **F6**. The selected screen image and Identification label will appear.
3. Use the arrow keys to move the label to the desired position.
4. Press **Esc** to save and exit.

**25.13 DDC – F10**

Display Data Channel (DDC) is a VESA standard for communication between a monitor and a video adapter.

Input the DDC information of the monitor connected to the Smart 108/116 IP switch into the memories of all connected ROC/RICCs when first installing system.

To input the DDC information:
1. Disconnect the Video cable of all RICCs from the computers. ROCs do not need to be disconnected.
2. Press **Shift** twice to open the OSD.
3. Press **F10**. “Please wait” flashes a few times and disappears. The monitor’s DDC information is sent to all ROC/RICCs.
4. Reconnect the Video cable of all RICCs.

**25.13.1.1 Updating the DDC information**

Update the DDC information in any of the following circumstances:
- When replacing the monitor connected to Smart 108/116 IP Switch
- When adding a new ROC/RICC to the system
- When reconnecting an existing ROC/RICC that was temporarily used in a different system

To update the DDC information, repeat the steps as set out above.
26. Upgrading the Smart 108/116 IP firmware

With the Smart 108/116 IP Switch Update software you can upgrade the firmware for the:

- Switch processors
- RICC/ROCs

The Update software enables you to add new features and fix bugs in a quick and efficient manner. You can also return the OSD to the factory default settings via the Update software. Install the Update software on any computer, even one not part of the Smart 108/116 IP system.

26.1 Obtaining the Update software and latest firmware

The Update software and latest firmware for your system are located on our website at:

http://www.minicom.com/phandle.htm

The firmware can be downloaded in different ways:

**Complete Firmware Package** – This includes the firmware for all Smart switches and RICCS and ROCS.

**Firmware Package for Smart Switch models** - This includes the firmware for all Smart switches.

**Smart CAT5 Switch Firmware** - There are multiple hardware versions of Smart CAT5 Switch units, each with version specific firmware. On the web page find the description and table that identifies your version.

**Firmware Package for RICC and ROC models** – Download a firmware package for RICC and ROC models (see the table on the web page for the Supported RICC/ROC models). Or search for and download the specific RICC/ROC models with the correct firmware version.

26.2 System requirements for the Update software

- Pentium II class computer with 256 MB RAM and 10 MB free Hard Drive space.
- Free Serial port.
- Windows 2000 or later.

26.3 Connecting the Smart 108/116 IP System

To update the firmware the Smart 108/116 IP system must be connected and switched on.
26.4 Connecting the RS232 Download cable

To run the Update software, connect the RS232 Download cable (p/n 5CB40419) to the computer containing the software, and to the Smart 108/116 IP Switch Flash port see Figure 47.

26.5 Installing the software

To install the Update software:

1. Download the software from the Support section of Minicom’s website.
2. Install the software on the computer’s hard drive.

26.6 Starting and configuring the Update software

1. Select Start/Programs/Smart IP Switch Update/Smart IP Switch Update or click the shortcut icon on the Desktop. The Smart IP Switch Update window appears. See the figure below.
The table below explains the functions of the buttons and dialog boxes in the Update window.

<table>
<thead>
<tr>
<th>Button or box</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select All</td>
<td>Selects all RICC/ROCs</td>
</tr>
<tr>
<td>Unselect All</td>
<td>Unselects selected RICC/ROCs</td>
</tr>
<tr>
<td>Start</td>
<td>Starts firmware download</td>
</tr>
<tr>
<td>F/W Version</td>
<td>Displays the firmware version numbers</td>
</tr>
<tr>
<td>H/W Version</td>
<td>Displays the hardware version numbers</td>
</tr>
<tr>
<td>Cancel</td>
<td>Cancels selected function</td>
</tr>
<tr>
<td>System time</td>
<td>System time</td>
</tr>
<tr>
<td>Status:</td>
<td>Displays communication status between the upgrade software and the Smart 108/116 IP. Choose Options/Get Status to refresh the status</td>
</tr>
<tr>
<td>File Name:</td>
<td>Name of Update file</td>
</tr>
</tbody>
</table>

2. To change the Com Port from the Options menu choose Com Port. The Com Port Dialog box appears. See Figure 49.
3. Choose the Com Port the RS232 Serial cable is connected to and click OK.

**26.7 Verifying the version numbers**

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

**26.7.1 Smart 108/116 IP Switch version**

To verify the Smart 108/116 IP Switch version:

1. Select the 108/116 IP Switch check box.

2. Click F/WVersion. The firmware versions of the Translator, Master and OSD appear, see Figure 50.

3. Click H/WVersion. The hardware version of the Translator appears, see Figure 51.
26.7.2 RICC/ROC version

Before you can tick a RICC/ROC, you must unselect the 108/116 IP Switch check box.

To verify the RICC/ROC version number:

1. Check one or more or all of the RICC/ROCs.
2. Click F/W Version. The firmware version number appears.
3. Click H/W Version. The hardware version number appears.

When “Not responding” appears, there is no computer connected, or it is switched off.

26.8 Obtaining new firmware

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

26.8.1 Updating the firmware

Warning!

Never switch off any computer connected to the Smart 108/116 IP system during the updating process.

To update the firmware:

1. Select the option to update Smart 108/116 IP switch or the RICC/ROCs.
2. From the File menu, choose Open. The Open dialog box appears. See Figure 52. The Smart 108/116 IP switch update is a .min file. The RICC/ROC update is a .hex file.
3. Navigate to the folder that contains the firmware update file. You may only see the files that match the file selection mask. When the firmware is contained in a Firmware Package, select the package. The package comes
with a .min extension. The correct firmware is automatically selected according the Switch or RICC/ROCC chosen in step 1 above. The file extension for specific devices is .hex.

4. Open the file.

5. Click Start. The Smart 108/116 IP Switch Update flashes the firmware. On completion the firmware version number appears.

\textbf{Note!} If the status of the device is busy - see the bottom of Figure 48 - the system cannot be upgraded. To free the device choose Options/Advanced/Reset. The device resets and the status is now free. Click Start.

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

\textbf{26.9 Restoring factory settings}

You can restore the OSD to the factory settings from the Update software.

\textbf{Note!} All changes made (passwords, access rights, names etc.) will be removed. To restore the OSD factory settings:

Select Options/Advanced/Set default. The OSD returns to the factory default settings.

(You can also restore the OSD from the OSD (F7), see page 43).
27. Update software - Troubleshooting

This section covers:

- Communication Error message
- Electricity failure

27.1 Communication Error message

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

1. Check that the RS232 Serial cable’s RS232 connector is connected to the Switch’s Flash port.
2. Check that the RS232 Serial cable’s DB9F connector is connected to the laptop’s Serial port.
3. Verify there is no Remote session in progress by pressing the Local button.
4. Restart the update process.

27.2 Electricity failure

When the electricity fails while updating the Smart 108/116 IP firmware, do the following:

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

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

(For electricity failure during a firmware upgrade of the digital part of the Smart 108/116 IP, see page 31).
# 28. Technical specifications

| Operating systems | Target Server  
|                  | DOS, Windows, Novell, Linux, SUN Solaris for PC  
|                  | Client Computer  
|                  | Windows 2000 or higher with Internet Explorer 6.0 and later or Firefox 3.0  
|                  | Linux x86 with Firefox 3.0  
| Resolution       | Target Server  
|                  | Up to 1600 x 1200 @ 85Hz  
|                  | Client Computer  
|                  | Recommended - resolution should be higher than on Target Server  
| Video and mouse synchronization | Both auto and manual modes  
| Security         | 256-bit SSL encryption  
| Connections      | Ethernet – RJ45 – 10/100 Mbit/sec autosensing  
|                  | Serial – RJ45  
|                  | Local KVM connection – Screen HDD15, Keyboard./Mouse – MiniDIN6  
|                  | Flash – RJ11  
|                  | Server – RJ45  
| Weight           | 2.54Kg / 5.6lbs  
| Dimensions (H x D x W) | 44 x 220 x 431 mm / 1.6 x 8.66 x 17"  
| Power input      | 100 – 240 VAC, 0.8 A, 50 / 60 Hz.  
| Operating temperature | 0°C to 40°C / 32°F to 104°F  
| Storage temperature | -40°C to 70°C / -40°F to 158°F  
| Humidity         | 80% non condensing relative humidity  

| Connections     | ROC PS/2  
|                 | VGA - HDD15  
|                 | KM - MiniDin6  
|                 | System - RJ45  
|                 | ROC USB  
|                 | VGA - HDD15  
|                 | KM - USB  
|                 | System - RJ45  
| Power           | From Keyboard port  
| Product weight  | 100g / 0.20lb  
| Shipping weight | 172g / 0.38lb  
| Dimensions      | 65 x 25 x 25mm / 0.21 x 0.08 x 0.08"  
|
## 29. Video resolution and refresh rates

<table>
<thead>
<tr>
<th>Hz →</th>
<th>56</th>
<th>60</th>
<th>65</th>
<th>66</th>
<th>70</th>
<th>72</th>
<th>73</th>
<th>75</th>
<th>76</th>
<th>85</th>
<th>86</th>
</tr>
</thead>
<tbody>
<tr>
<td>640x480</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>720x400</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>800x600</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1024x768</td>
<td>x</td>
<td></td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>1152x864</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1152x900</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>1280x720</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1280x768</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1280x960</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1280x1024</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>1600x1200</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
</tbody>
</table>
30. Safety
This device contains no serviceable parts. Any servicing of the device must be performed by an authorized Minicom technician in a Minicom authorized Service Center.

31. 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).

32. 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.
# Appendix 1: SNMP Events table

The table below lists all events recorded.

<table>
<thead>
<tr>
<th>Event Text</th>
<th>Code</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;System Boot&quot;</td>
<td>1010</td>
<td>Reported upon device boot up.</td>
</tr>
<tr>
<td>&quot;Server Busy ask for disconnect...&quot;</td>
<td>1030</td>
<td>Attempt to connect when another user is already connected. The 2(^{nd}) user has permission for takeover, sent before the 2(^{nd}) user actually takes over the session.</td>
</tr>
<tr>
<td>&quot;User login succeeded&quot;</td>
<td>1040</td>
<td>On every successful user login to the device.</td>
</tr>
<tr>
<td>&quot;Login failed wrong user name or password&quot;</td>
<td>1050</td>
<td>Login failed due to wrong user name or password.</td>
</tr>
<tr>
<td>&quot;Login not succeeded server busy&quot;</td>
<td>1060</td>
<td>Login denied since a user with higher permission is connected (takeover not allowed).</td>
</tr>
<tr>
<td>&quot;Logout&quot;</td>
<td>1070</td>
<td>User Logout (end of remote access session).</td>
</tr>
<tr>
<td>&quot;Disconnected by another user&quot;</td>
<td>1110</td>
<td>Takeover has been successfully performed; the previous user has been disconnected.</td>
</tr>
<tr>
<td>&quot;Hardware Failure&quot;</td>
<td>1200</td>
<td>Device internal hardware failure. Try disconnecting any other attached device and re-boot. If problem persists contact technical support.</td>
</tr>
<tr>
<td>&quot;Hard reset power cycle command&quot;</td>
<td>1220</td>
<td>Power cycle command issued, only relevant when a special power-cycle product is attached to the device (e.g., KBPower).</td>
</tr>
<tr>
<td>&quot;Viewer login&quot;</td>
<td>1230</td>
<td>User connected in view-only mode (while another user is connected in a regular session).</td>
</tr>
<tr>
<td>&quot;Viewer logout&quot;</td>
<td>1240</td>
<td>User connected in view-only mode has disconnected.</td>
</tr>
<tr>
<td>&quot;Global access disabled &quot;</td>
<td>1250</td>
<td>Device has been blocked for access by an administrator; remote access is disabled until the device is unblocked.</td>
</tr>
<tr>
<td>&quot;Block User Account&quot;</td>
<td>1260</td>
<td>User blocked due to too many login attempts failure per policy in configuration.</td>
</tr>
<tr>
<td>Successful User Login</td>
<td>2010</td>
<td>Successful User Login CONF_USER_EVENT_LOGIN_SUCCEEDED</td>
</tr>
<tr>
<td>Login is not successful – wrong user access level.</td>
<td>2020</td>
<td>Login is not successful – wrong user access level. CONF_USER_EVENT_LOGIN_NOT_SUCCEEDED_WRONG_LEVEL</td>
</tr>
<tr>
<td>Wrong user name or password</td>
<td>2030</td>
<td>Wrong user name or password. Login is not successful. CONF_USER_EVENT_LOGIN_NOT_SUCCEEDED_WRONG_USER_NAME_OR_PASSWORD</td>
</tr>
<tr>
<td>Event Text</td>
<td>Code</td>
<td>Comment</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>-------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Login is not successful because server is busy.</td>
<td>2040</td>
<td>Login is not successful because server is busy. CONF_USER_EVENT_LOGIN_NOT_SUCCEEDED_SERVER_BUSY</td>
</tr>
<tr>
<td>DHCP server setting has been changed</td>
<td>2060</td>
<td>DHCP server setting has been changed CONF_DHCP_CHANGED</td>
</tr>
<tr>
<td>Network IP address changed</td>
<td>2070</td>
<td>Network IP address has been changed CONF_IP_CHANGED</td>
</tr>
<tr>
<td>Network Subnet Mask changed</td>
<td>2080</td>
<td>Network Subnet Mask has been changed CONF_SNMASK_CHANGED</td>
</tr>
<tr>
<td>Network Default Gateway changed</td>
<td>2090</td>
<td>Network Default Gateway has been changed CONF_DG_CHANGED</td>
</tr>
<tr>
<td>User Logged out from Config</td>
<td>2100</td>
<td>User Logged out from Config CONF_LOG_OUT</td>
</tr>
<tr>
<td>TCP Port was changed</td>
<td>2110</td>
<td>TCP Port was changed CONF_TCP_PORT_CHANGED</td>
</tr>
<tr>
<td>Remote Access type was changed</td>
<td>2120</td>
<td>Remote Access type was changed CONF_REMOTE_ACCESS_CHANGED</td>
</tr>
<tr>
<td>Security settings changed</td>
<td>2140</td>
<td>CONF_SECURITY_CHANGED</td>
</tr>
<tr>
<td>Restore default factory settings successful</td>
<td>2150</td>
<td>CONF_RESTORE_FACTORY_OK</td>
</tr>
<tr>
<td>Restore default factory settings failed</td>
<td>2160</td>
<td>CONF_RESTORE_FACTORY_FAILED</td>
</tr>
<tr>
<td>Firmware Upgrade successful</td>
<td>2170</td>
<td>CONF_UPGRADE_OK</td>
</tr>
<tr>
<td>Firmware Upgrade failed</td>
<td>2180</td>
<td>CONF_UPGRADE_FAILED</td>
</tr>
</tbody>
</table>