

# IP Control User Guide



[www.minicom.com](http://www.minicom.com)

## International HQ

Jerusalem, Israel  
Tel: + 972 2 535 9666  
[minicom@minicom.com](mailto:minicom@minicom.com)

## North American HQ

Linden, NJ, USA  
Tel: + 1 908 486 2100  
[info.usa@minicom.com](mailto:info.usa@minicom.com)

Technical Support – [support@minicom.com](mailto:support@minicom.com)



## Legal Notice

This manual and the software described in it are furnished under license, and may be used or copied only in accordance with the terms of such license. The content of this manual is provided for informational use only, and is subject to change without notice. It should not in and of itself be construed as a commitment by Minicom Advanced Systems Limited, which assumes no responsibility of liability for any errors or inaccuracies that may appear in this book.

The software that accompanies this manual is licensed for use by the Licensee only, in strict accordance with the software license agreement, which the Licensee should read carefully before commencing use of the software. Except as permitted by the license, no part of this publication may be reproduced, stored in retrieval system, or transmitted in any form of by any means, electronic, mechanical, recording, or otherwise, without the prior written permission of Minicom Advanced Systems Limited.

# About this Document

This document provides installation and operation instructions for the IP Control system, produced by Minicom Advanced Systems Limited. It is intended for system administrators and network managers.



## Chapters and Their Contents

---

<b>1</b>	<b>Introduction</b>	Provides an introduction to the document, IP Control product overview, features and benefits of IP Control, client computer operating system requirements, technical precautions, trademarks, and terminology used in the document. It also describes how to safely handle the device, provide feedback on the user guide, and WEEE Information for Minicom Customers and Recyclers.	Pg. 9
<b>2</b>	<b>Installation</b>	Lists IP Control system components, describes the functionalities of the IP Control elements, and provides instructions for rack mounting the unit and connecting the system.	Pg. 10
<b>3</b>	<b>Configuring the Network</b>	Provides instructions for logging into the Web configuration interface, configuring the device ID, IP address, and Centralized Management settings, enabling and configuring SNMP, adding, editing, removing, and blocking system Users, configuring the KVM switch, Serial port, security settings, and the system date and time. It also provides instructions for installing an SSL certificate, upgrading firmware, restoring factory settings, and saving changes and logging out.	Pg. 19
<b>4</b>	<b>Conducting a Remote Session</b>	Describes how to start a remote session, set the session profile, full screen mode, view system information, adjust video settings, power manage target servers, manage keyboard sequences, synchronize mouse pointers, switch to a different server or device, and disconnect the remote session.	Pg. 39
<b>5</b>	<b>Troubleshooting – Safe Mode</b>	Describes how to enter Safe mode, restore factory defaults, and restore device firmware.	Pg. 59
<b>6</b>	<b>Technical Specifications</b>	Lists and describes IP Control specifications.	Pg. 63
<b>7</b>	<b>Video Resolution and Refresh Rates</b>	Lists video resolutions and refresh rates.	Pg. 63

---

## Style Conventions

Convention	Used for
Verdana	Regular text.
<b>Arial Bold</b>	Names of menus, commands, buttons, and other elements of the user interface.
<i>Arial Italics</i>	Special terms, the first time they appear.
Monospace	Text entered by the user.
	<b>Notes</b> , which offer an additional explanation or a hint on how to overcome a common problem.
	<b>Warnings</b> , which indicate potentially damaging user operations and explain how to avoid them.

# Table of Contents

<b>TABLE OF FIGURES .....</b>	<b>VII</b>
<b>1 INTRODUCTION .....</b>	<b>9</b>
1.1 PRODUCT OVERVIEW .....	9
1.1.1 Features and Benefits .....	9
1.2 TERMINOLOGY .....	9
1.3 CLIENT COMPUTER OPERATING SYSTEM.....	10
1.4 TECHNICAL PRECAUTIONS.....	10
1.5 SAFETY .....	10
1.6 USER GUIDE FEEDBACK .....	10
1.7 TRADEMARKS .....	11
1.8 WEEE COMPLIANCE .....	11
<b>2 INSTALLATION .....</b>	<b>12</b>
2.1 OVERVIEW .....	12
2.2 SYSTEM COMPONENTS.....	12
2.2.1 The IP Control Unit.....	12
2.3 MOUNTING THE IP CONTROL UNIT.....	14
2.3.1 Rack Mounting Safety Considerations.....	14
2.3.2 Mounting the Unit .....	15
2.4 CONNECTING THE SYSTEM .....	16
<b>3 CONFIGURING THE NETWORK .....</b>	<b>19</b>
3.1 BOOT-UP PROCESS .....	19
Assigning Static IP Addresses for a Number of Units .....	20
3.2 LOGGING ONTO THE WEB CONFIGURATION INTERFACE .....	20
3.2.1 Web Configuration Interface Tabs.....	22
3.2.2 Web Configuration Toolbar Buttons.....	23
3.3 CONFIGURING THE NETWORK SETTINGS .....	23

---

3.3.1	Configuring Device ID Settings .....	23
3.3.2	Configuring the Device IP Address .....	24
3.3.3	Configuring Centralized Management Settings .....	24
3.4	CONFIGURING NETWORK SNMP SETTINGS .....	25
3.5	CONFIGURING USER SETTINGS .....	25
3.5.1	Adding a User .....	26
3.5.2	Deleting User(s) .....	27
3.5.3	Blocking a User .....	28
3.5.4	Editing User Information .....	28
3.6	CONFIGURING THE KVM SWITCH .....	29
3.6.1	Installing the Switch Definition File .....	30
3.7	CONFIGURING THE SERIAL PORT SETTINGS .....	31
3.7.1	Assigning Serial Port .....	31
3.8	CONFIGURING THE SECURITY SETTINGS .....	32
3.9	CONFIGURING THE SYSTEM DATE AND TIME .....	33
3.10	PERFORMING ADDITIONAL CONFIGURATION OPERATIONS .....	33
3.10.1	Installing an SSL Certificate .....	34
3.10.2	Upgrading Firmware .....	34
3.10.3	Restoring Factory Settings .....	36
3.11	RELOADING A PAGE .....	36
3.12	SAVING CHANGES AND LOGGING OUT .....	37
<b>4</b>	<b>CONDUCTING A REMOTE SESSION .....</b>	<b>39</b>
4.1	STARTING A REMOTE SESSION .....	39
4.1.1	Remote Session Toolbar Buttons .....	41
4.2	SHARING A REMOTE SESSION .....	41
4.2.1	Exclusive Session .....	42
4.3	DISPLAYING THE TOOLBAR .....	42
4.4	SETTING THE SESSION PROFILE .....	42
4.4.1	Full Screen Mode .....	43
4.5	VERIFYING REMOTE PRESENCE SOLUTIONS INFORMATION .....	44
4.6	CHANGING THE VIDEO PERFORMANCE SETTINGS .....	45

4.7	ADJUSTING THE VIDEO .....	46
4.7.1	Refreshing the Video Image.....	46
4.7.2	Automatically Adjusting the Video Image.....	47
4.7.3	Manually Adjusting Video Settings .....	47
4.8	POWER MANAGING THE TARGET SERVERS .....	49
4.9	MANAGING KEYBOARD SEQUENCES.....	49
4.9.1	Adding a Keyboard Sequence.....	50
4.9.2	Recording a New Custom Key .....	51
4.9.3	Editing a Key Sequence.....	52
4.9.4	Deleting Key Sequence(s) .....	52
4.10	SYNCHRONIZING MOUSE POINTERS .....	53
4.10.1	Manually Synchronizing the Mouse.....	53
	The USB Option.....	55
	Advanced Mouse Emulation .....	56
4.10.2	Aligning the Mouse Pointers .....	56
4.10.3	Calibrating Mouse Pointers .....	57
4.11	SWITCHING TO A DIFFERENT SERVER/DEVICE .....	57
4.12	DISCONNECTING THE REMOTE SESSION .....	58
<b>5</b>	<b>TROUBLESHOOTING – SAFE MODE.....</b>	<b>59</b>
5.1	ENTERING SAFE MODE .....	59
5.2	RESTORING FACTORY DEFAULTS .....	61
5.3	RESTORING THE DEVICE FIRMWARE .....	61
<b>6</b>	<b>TECHNICAL SPECIFICATIONS .....</b>	<b>63</b>
<b>7</b>	<b>VIDEO RESOLUTION AND REFRESH RATES .....</b>	<b>64</b>

## Table of Figures

Figure 1 – IP Control Unit Front Panel.....	13
Figure 2 – IP Control Unit Back Panel .....	13
Figure 3 – IP Control Unit Connected to a Rack.....	14
Figure 4 – IP Control Unit Connected to a Tabletop.....	14
Figure 5 – Holes for Rack/Tabletop Mounting .....	15
Figure 6 – Connecting the L-shaped Bracket to Unit .....	16
Figure 7 – IP Control Connections to a Computer .....	17
Figure 8 – IP Control Connections to a KVM Switch.....	18
Figure 9 – Boot-Up Process.....	20
Figure 10 – Web Page .....	21
Figure 11 – Logon Page.....	21
Figure 12 – Network Configuration – Device Tab .....	22
Figure 13 – SNMP Settings.....	25
Figure 14 – Users Page .....	26
Figure 15 – Add User Page.....	26
Figure 16 – Delete User Confirmation .....	27
Figure 17 – Edit User Page.....	28
Figure 18 – KVM Switch Configuration Page.....	29
Figure 19 – Servers of Selected KVM Switch .....	30
Figure 20 – Serial Port Page.....	31
Figure 21 – Security Page.....	32
Figure 22 – Date and Time Page .....	33
Figure 23 – SSL Certificate Page.....	34
Figure 24 – Device Version Upgrade Page .....	35
Figure 25 – Reboot Confirmation Page.....	35
Figure 26 – Restore Factory Settings Page .....	36
Figure 27 – Device Reboot Confirmation Message.....	37
Figure 28 – Save Succeeded Message .....	37
Figure 29 – Device Rebooting Progress Box.....	38
Figure 30 – Logon Page after Rebooting.....	38
Figure 31 – Logon Page.....	40
Figure 32 – Remote Session Page .....	40
Figure 33 – Shared Remote Session .....	42
Figure 34 – Session Profile Dialog Box .....	43
Figure 35 – Remote Presence Solutions Information .....	44
Figure 36 – Performance Settings .....	46
Figure 37 – Video Adjust Progress.....	47
Figure 38 – Manual Video Adjustments Controls.....	48
Figure 39 – Power Menu .....	49

## Table of Figures

---

Figure 40 – Special Key Manager .....	50
Figure 41 – Add a Predefined Key Dialog Box .....	51
Figure 42 – Record Macro Box.....	52
Figure 43 – Delete Key(s) Confirmation Box .....	53
Figure 44 – Relative Mouse Settings.....	54
Figure 45 – Windows 7 Mouse Properties .....	55
Figure 46 – Mouse Emulation Box .....	56
Figure 47 – Safe Mode Procedure .....	59
Figure 48 – Login Page.....	60
Figure 49 – Safe Mode Menu.....	60
Figure 50 – Warning .....	61
Figure 51 – Additional Warning .....	61
Figure 52 – Reboot.....	61
Figure 53 – Update Succeeded .....	62

---

# 1 Introduction

Congratulations on adding IP Control to your remote access tools.

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

## 1.1 Product Overview

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

### 1.1.1 Features and Benefits

IP Control has the following features and benefits:

- **BIOS level control** to any server's brand and model, regardless of the server condition and network connectivity. Covers the entire spectrum of crash scenarios.
- **Compatible** with all major operating systems. Supports many hardware and software configurations for the remote client and target server computers, as well as the KVM switch in use.
- **Web-based control** – Browser based control of a target server from any location, via a secured standard IP connection.
- **Multi-user share mode** – Allows up to five simultaneous users to share a remote session.

## 1.2 Terminology

The following table describes terms used in this guide.

## Introduction

---

### Client Computer Operating System

Term	Definition
Target server	The computer/server that is accessed remotely via IP Control
Client computer	The PC running a remote IP Control session
Remote session	The process of accessing and controlling target servers connected to IP Control from a user workstation

## 1.3 Client Computer Operating System

The client computer operating system must be one of the following:

- Windows 2000 or later, with Firefox 3 or Internet Explorer 32-bit 7.0 or later version
- Linux with Firefox 3; 128-bit encryption support is required

## 1.4 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.

## 1.5 Safety

The device must only be opened by an authorized Minicom technician. Disconnect the device from the power source and all cables from the device before service operation!

## 1.6 User Guide Feedback

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

Please include the following information:

- Guide name
- Part number
- Version number (on the front cover)

## 1.7 Trademarks

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

## 1.8 WEEE Compliance

This section provides 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 back the new equipment for recycling when it ultimately becomes waste

Instructions for both customers and recyclers / treatment facilities wishing to obtain disassembly information are provided in our website [www.minicom.com](http://www.minicom.com).

## 2 Installation

### 2.1 Overview

Install the IP Control system as follows:

1. Remove the IP Control system from the package, and check that all components are present and in good working condition.
2. Mount the IP Control unit in a rack or under a tabletop.
3. Make all hardware connections between the power source, IP Control, target devices, and Ethernet, and the optional modem connection.
4. Power on the IP Control unit.

### 2.2 System Components

Before installing the IP Control system, verify that you have all the components on the following list, as well as any other items required for installation.

The IP Control system consists of:

- One IP Control unit (p/n 1SU70017)
- One KVM cable (p/n 5CB00565)
- One RS232 cable (p/n 5CB00566)
- One universal power adapter (p/n 5PSB0005)
- A rack mounting kit (p/n 5AC00297)

#### 2.2.1 The IP Control Unit

The IP Control Unit back and front panels are illustrated in Figure 1 and Figure 2.

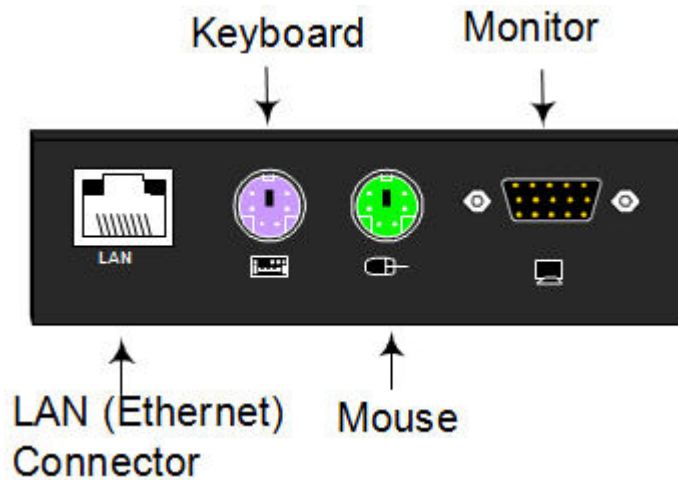


Figure 1 – IP Control Unit Front Panel

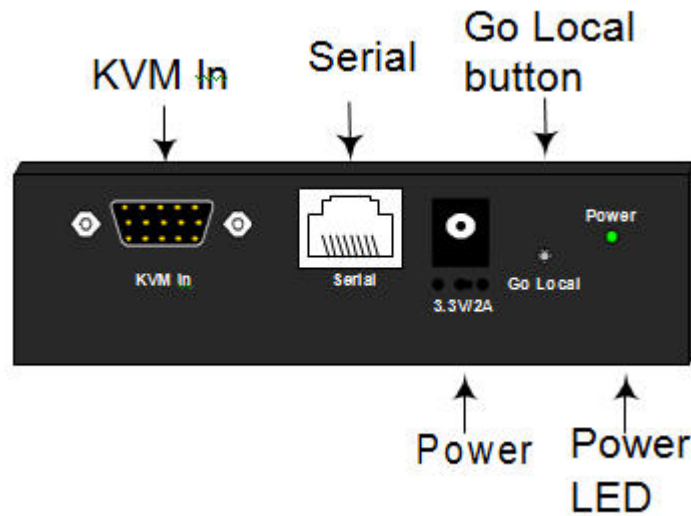


Figure 2 – IP Control Unit Back Panel

The following table describes the functionality of the elements of the IP Control back and front panels.

Element	Functionality
<b>LAN (Ethernet) Connector</b>	For connecting the IP Control unit to the 10/100 Mbit Ethernet port on the Network switch via a cable.
<b>Keyboard, Mouse, and Monitor ports</b>	For optional local access to the connected computer, a keyboard, mouse, and monitor can be connected to the KVM ports on the front panel of the IP Control unit.
<b>KVM In</b>	For connecting the IP control unit to the server (computer) or KVM switch via a 1 to 3 CPU cable.

## Installation

---

### Mounting the IP Control Unit

Element	Functionality
<b>Serial</b>	For connecting the IP Control unit to serial manageable devices, such as power management units and routers, via the RS232 cable.
<b>Power</b>	For connecting the IP Control unit to a grounded AC electrical outlet via a power cord.
<b>Go Local button</b>	Pressing this button disconnects the remote session and accesses the computer locally.
<b>Power LED</b>	Indicates the state of the IP Control unit: Green indicates that the unit is powered on; Red indicates that the unit is powered off.

## 2.3 Mounting the IP Control Unit

You can connect the IP Control unit to a server rack or under a tabletop, using the supplied rack mounting kit.



*Figure 3 – IP Control Unit Connected to a Rack*



*Figure 4 – IP Control Unit Connected to a Tabletop*

### 2.3.1 Rack Mounting Safety Considerations

When mounting IP Control onto a rack, avoid the following conditions:

- **Elevated operating ambient temperature** – The operating ambient temperature of the rack environment may be greater than the room ambient temperature. Therefore, take special care when installing the unit in a closed or multi-unit rack assembly that the environment is 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.
- **Uneven mechanical loading** – Uneven loading can cause damage to the equipment or personal injury. Mount the equipment in the rack in such a way that a hazardous condition does not result due to uneven mechanical loading.
- **Circuit overloading** – When connecting the equipment to the supply circuit, make sure that the total power of all the components does not exceed the circuit capabilities. Overloading of circuits can affect over-current protection and supply wiring, potentially resulting in fire and shock hazards.
- **Unreliable earthing** – Maintain reliable earthing of rack-mounted equipment. Pay attention to supply connections other than direct connections to the branch circuit (for example, use of power strips).

### 2.3.2 Mounting the Unit

The IP Control unit comes with screw holes on the side, for easy rack or tabletop mounting.



*Figure 5 – Holes for Rack/Tabletop Mounting*

➔ **To rack mount the IP Control unit:**

1. Connect the L-shaped brackets to the IP Control unit, using the screws provided. The length of the screws used for connecting the brackets to the IP Control unit must not exceed 5 mm.

## Installation

### Connecting the System



**L-shaped Brackets**

*Figure 6 – Connecting the L-shaped Bracket to Unit*

2. Install the IP Control unit into the server rack by connecting the bracket to the rack with screws, according to the rack manufacturer's instructions.

## 2.4 Connecting the System

### ➔ To connect the target server / KVM switch to the IP Control unit:

1. Connect the single connector of the KVM 1 to 3 CPU cable to the KVM In port of the IP Control unit.
2. Connect the other end of the KVM cable to the KVM ports of the target server / KVM switch.
3. Connect a Network cable to the IP Control LAN port and to an Ethernet port on your Network switch.
4. Connect the power adapter.



It is recommended to place cables away from fluorescent lights, air conditioners, and machines that are likely to generate electrical noise.

Figure 7 and Figure 8 illustrate the connections to a computer and KVM switch respectively, with the optional KVM console.

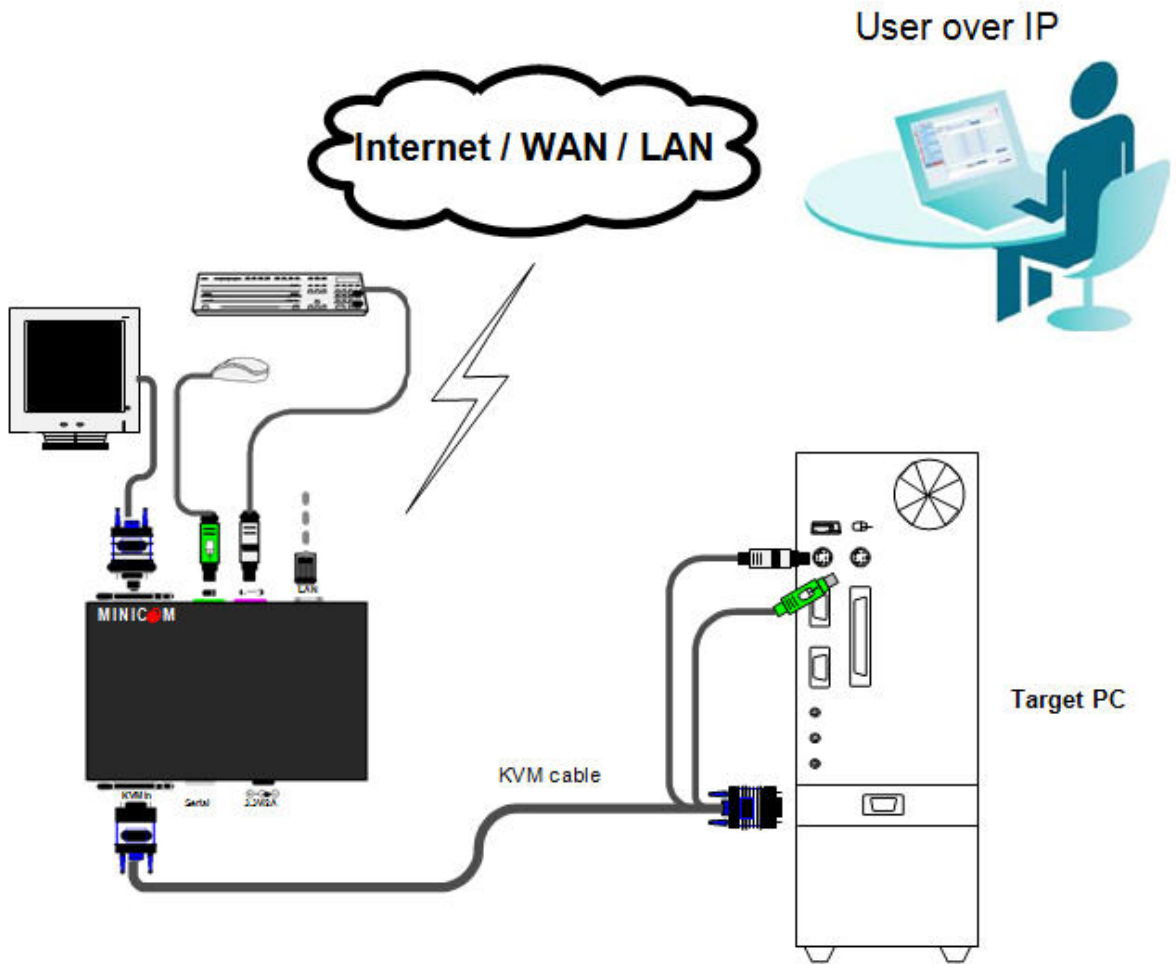


Figure 7 – IP Control Connections to a Computer

## Installation

### Connecting the System

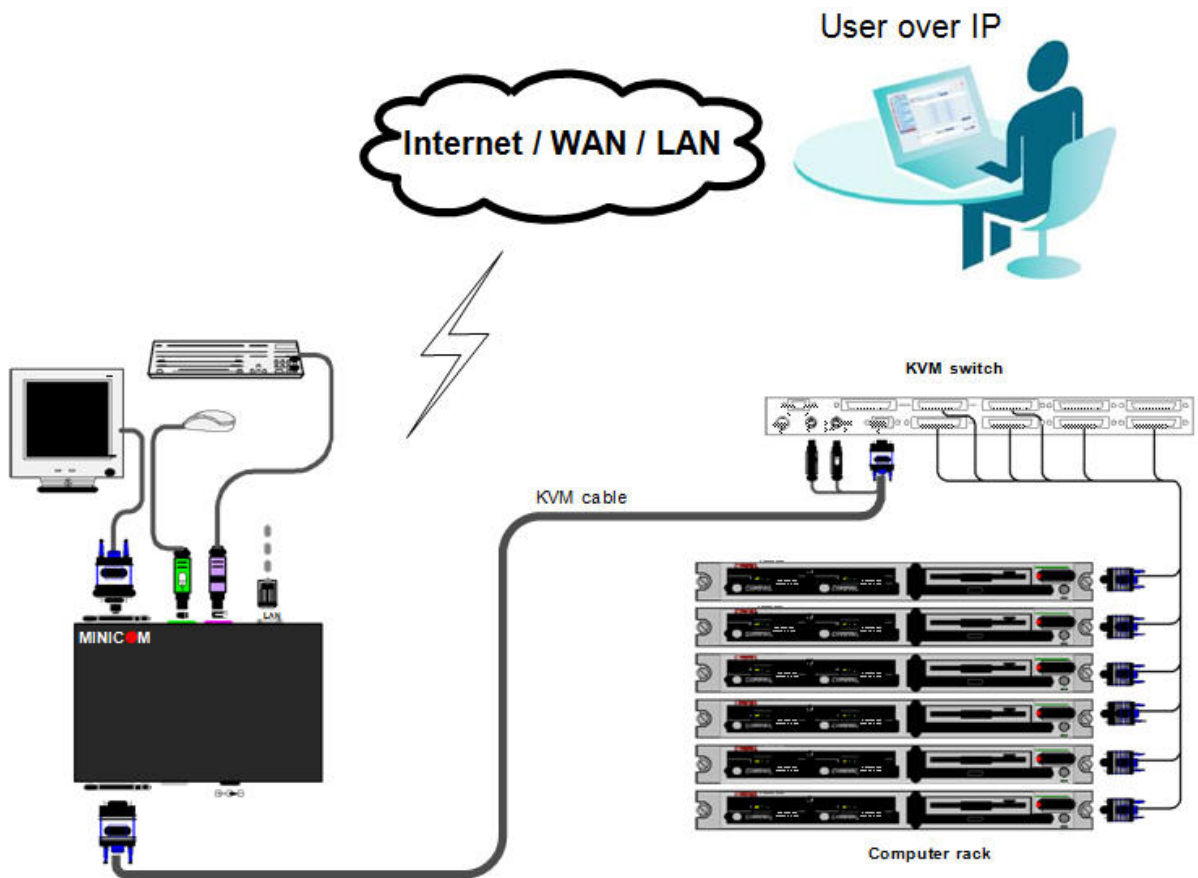


Figure 8 – IP Control Connections to a KVM Switch

## 3 Configuring the Network

After the system has been installed and all connections have been made, you must configure the IP Control system as follows:

1. Configure IP Control's network settings, which includes configuring:
  - Device ID settings
  - IP Control's IP address
  - Centralized Management
2. Configure the SNMP settings.
3. Add, edit, remove, and block system Users.
4. Configure the KVM switch settings.
5. Configure the Serial port settings.
6. Configure the security settings.
7. Configure the system date and time.

You can also perform the following additional operations, as required:

1. Install an SSL certificate.
2. Upgrade firmware.
3. Restore factory settings.

### 3.1 Boot-Up Process

By default, IP Control boots with an automatically assigned IP address from a DHCP (Dynamic Host Configuration Protocol) server on the network (see Figure 9 for an overview of the boot-up process). The DHCP server assigns the IP Control a valid IP address, gateway address, and subnet mask.

This automatically assigned IP address can be identified according to the IP Control MAC address that appears on the underside of the IP Control box, next to the device number (D.N.).

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



If a DHCP server later becomes available, the unit picks up the IP settings from the DHCP server. To keep the static IP address, you can disable DHCP, as explained in Section 3.3.2 on page 24.

## Configuring the Network

### Logging Onto the Web Configuration Interface

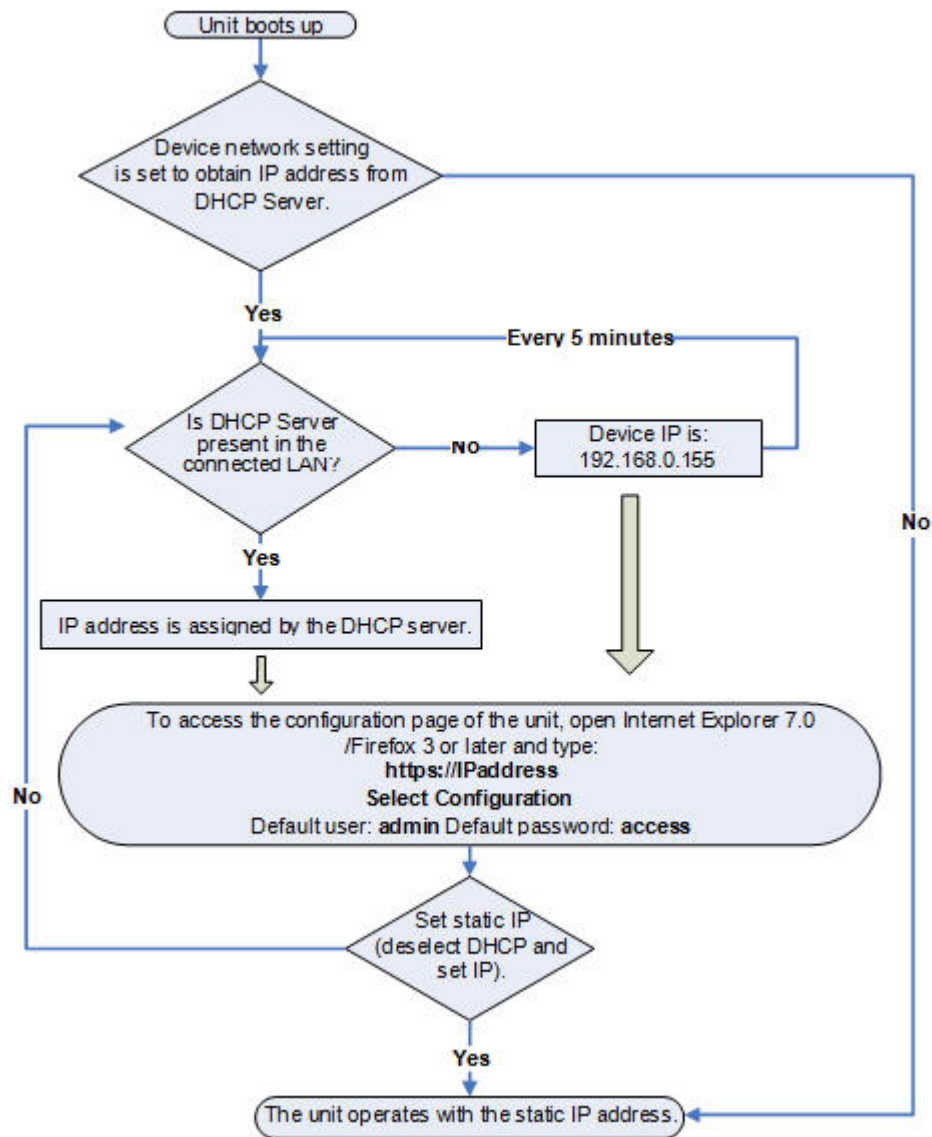


Figure 9 – Boot-Up Process

### Assigning Static IP Addresses for a Number of Units

You can connect more than one IP Control to the same network. If there is no DHCP server, or you want to use static IP addresses, connect the IP Control units one at a time and change the static IP address of each unit before connecting the next unit.

## 3.2 Logging Onto the Web Configuration Interface

You can complete the initial setup of the IP Control system via the Web configuration interface.

Only one Administrator at a time can log onto the Web configuration interface. An idle timeout of 30 minutes terminates the session.

Before logging on the first time, verify that you have the latest Java installed on your computer. If not, you can download and install Java from:

<http://www.java.com/en/download/index.jsp>

➔ **To log into the Web interface:**

1. Open your Web browser (Internet Explorer 7.0 / Firefox 3 or later).
2. Type the IP Control system IP address [https://IP address/](https://IP_address/), and press **Enter**.

The Web page appears.

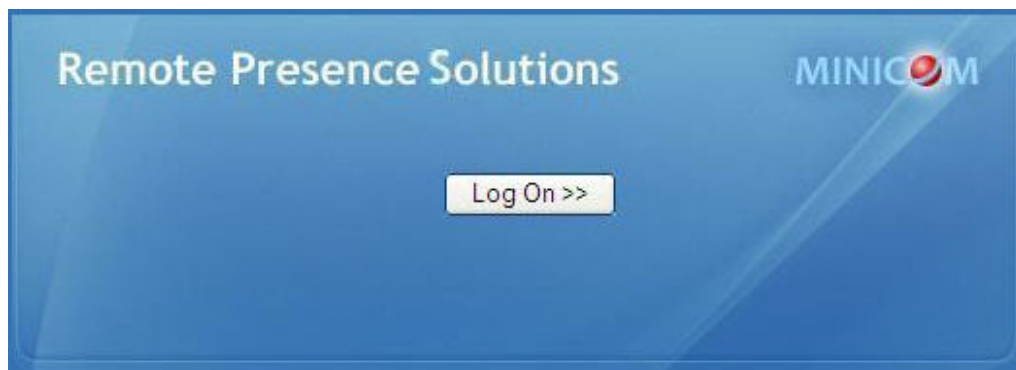


Figure 10 – Web Page

3. Click **Log On**.

Java installs. After installation has completed, the logon page appears.

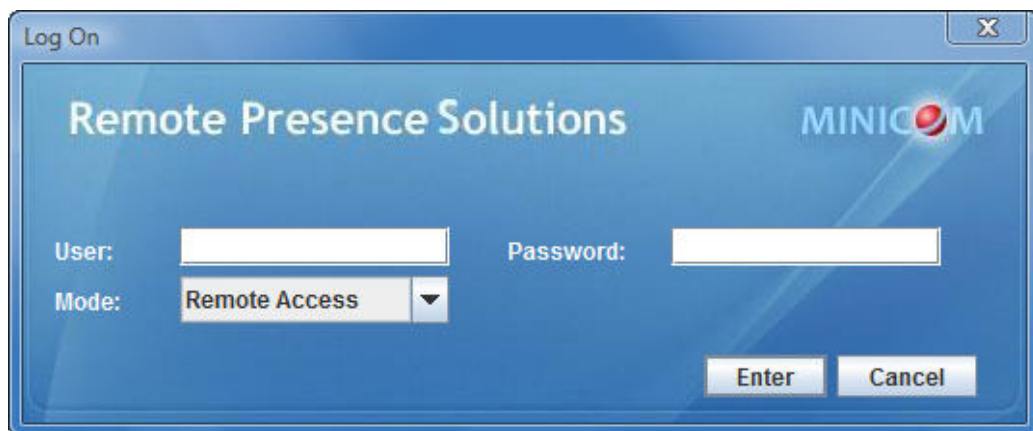


Figure 11 – Logon Page

4. In **User**, type the default Administrator name **admin** and in **Password**, type **access** (both lower case).
5. In **Mode**, select **Configuration**.

## Configuring the Network

### Logging Onto the Web Configuration Interface

6. Click Enter.

The Network configuration page appears with the Device tab open.

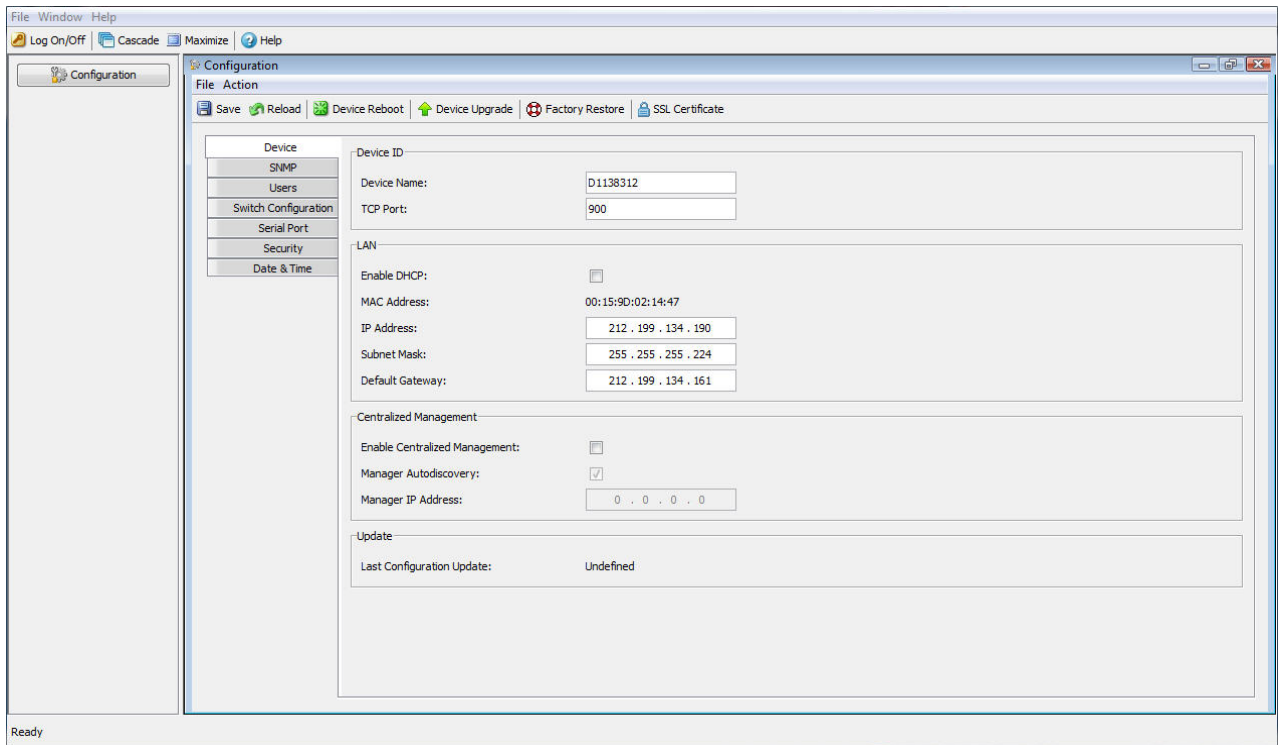



Figure 12 – Network Configuration – Device Tab

From the Configuration menu, you can configure the network, SNMP, Users, Switch Configuration, Serial Port, Security, and Date and Time settings. **After making all configuration changes, you must click the  Save button in the toolbar for the changes to go into effect.**

### 3.2.1 Web Configuration Interface Tabs







The following table summarizes the Web configuration interface tabs.

Tab	Description
Device	For configuration of the device settings, IP address, and centralized management
SNMP	For configuration of network SNMP settings
Users	For adding, editing, deleting, and blocking system Users
Switch Configuration	For configuration of the KVM switch settings
Serial Port	For configuration of the Serial port settings
Security	For configuration of the security settings

Tab	Description
Date & Time	For setting the system date and time

### 3.2.2 Web Configuration Toolbar Buttons

The following table describes the functionality of the Web configuration toolbar buttons.

Button	Functionality
 Save	Saves the configuration changes
 Reload	Reloads the device settings into the configuration page parameter settings
 Device Reboot	Reboots the device
 Device Upgrade	Upgrades the device firmware
 Factory Restore	Restores the device with factory settings
 SSL Certificate	Installs the SSL certificate onto the device

## 3.3 Configuring the Network Settings

On the network configuration page (see Figure 12), you can configure the following:

- Device ID
- Device IP address
- Centralized Management

Consult your Network Administrator for the network settings.

### 3.3.1 Configuring Device ID Settings

You can assign a name to the IP Control device, and select a TCP port.

The default device name consists of the letter 'D' followed by the 6-digit device number (D.N.), which is printed on the silver label on the underside of the IP Control box.

If the DHCP server is published in the DNS server, you can connect to the IP Control system using the device name, as follows: <https://DeviceName>.

You can select 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.



Firewall or router security access list must enable inbound communication through the selected TCP port for the IP Control'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.

➔ **To configure Device ID settings:**

1. In **Device Name**, type a name for IP Control.
2. In **TCP Port**, type the number of the port (from 800 to 65535).

### 3.3.2 Configuring the Device IP Address

When a DHCP server is active on the same network to which IP Control is connected, the DHCP can provide automatic IP assignment. However, best practices recommend using MAC address reservations in the DHCP server to ensure that the IP address of the IP Control will not be changed.

Consult your Network Administrator regarding the use of the DHCP.



If you have access to the server, your configured (or default) IP Control device name will appear on the DHCP server's interface, making it easy to locate.

➔ **To configure the device IP address, do one of the following:**

- **Select automatic IP address assignment** – Select the **Enable DHCP** checkbox to enable a DHCP server that is active on the same network to which IP Control is connected, to provide automatic IP assignment.
- **Select manual IP address assignment** – Clear the **Enable DHCP** checkbox to disable the DHCP, and then type the **IP Address**, **Subnet Mask**, and **Default Gateway** for **LAN 1**, provided by your Network Administrator.

### 3.3.3 Configuring Centralized Management Settings

Minicom's Centralized Management IP-based systems ensure secure control of servers and network devices, and 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.

➔ **To configure Centralized Management settings:**

1. Select the **Enable Centralized Management** checkbox to enable IP Control to be remotely managed by a Centralized Management system.

When managed by Centralized Management, only Network Configuration is available from the IP Control configuration page. All other settings, such as Device Upgrade, Factory Restore, and SSL Certificate are disabled and are managed from Centralized Management.

2. Select the **Manager Auto Discovery** checkbox to cause the Centralized Management system to automatically detect IP Control, if they both reside on the same network segment

OR

In **Manager IP Address**, type the static IP address of the Centralized Management Manager.



Although not required, it is recommended to type the **Manager IP Address** even if the IP Control resides on the same network segment as the Centralized Management Manager.

### 3.4 Configuring Network SNMP Settings

You can activate SNMP logging to provide support network monitoring. This will cause the IP Control to send monitoring events (such as log entries) to the SNMP server.

#### ➔ To enable and configure SNMP logging:

1. From the configuration menu, select **SNMP**.

The SNMP page opens.

Figure 13 – SNMP Settings

2. Select the **Enable Traps** checkbox to enable SNMP traps of IP Control events and operation.
3. In **Community**, type the name of the SNMP community.
4. In **SNMP Manager IP**, type the SNMP Server IP address.

### 3.5 Configuring User Settings

An Administrator can add, edit, remove, and block Users.

## Configuring the Network

### Configuring User Settings

There are two levels of user access:

- **Administrator** – has unrestricted access to all windows and settings, and can change the name and password of all users
- **User** – can access and control target servers, but cannot use advanced mouse settings and power cycle; cannot access the Web configuration interface

### 3.5.1 Adding a User

➔ **To add a User:**

1. From the configuration menu, select **Users**.

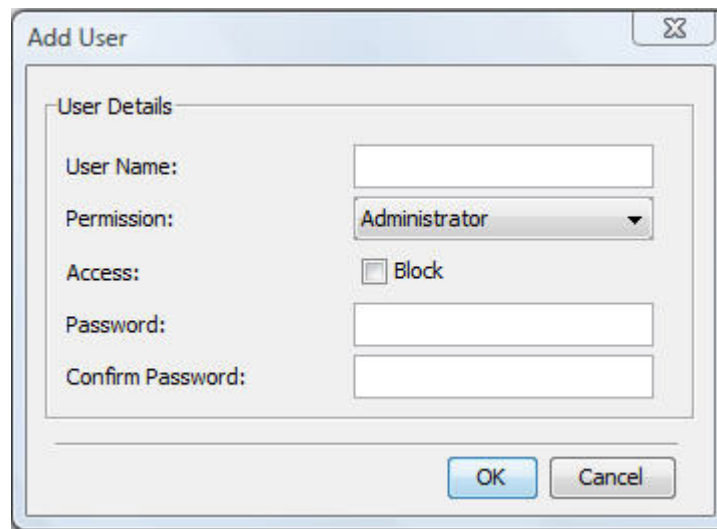
The Users page opens and displays the existing Users.



Figure 14 – Users Page

2. Click the **Add** button.

The Add User page appears.



**Add User**

User Details

User Name:

Permission: Administrator

Access:  Block

Password:

Confirm Password:

OK Cancel

Figure 15 – Add User Page

3. Type a **User Name** and **Password**. The password must be at least six alphanumeric characters long and cannot include the user name, even if other characters are added.



The "special" characters **&**, **<**, **>**, and **"** cannot be used for either the user name or password.

The **User Name** and **Password** parameters depend on the security level chosen (see Section 3.8 on page 32).

4. In **Confirm Password**, retype the password.
5. In the **Permission** dropdown menu, select the permission type: **Administrator** or **User**.
6. Click **OK**.

The User is added to the list of Users.

### 3.5.2 Deleting User(s)

You can delete one or multiple Users at a time from the system.



You cannot delete an Administrator who is logged onto the system.

#### ➔ To delete a User:

1. In the **Users** page (see Figure 14), select User(s) to delete. Select a group of Users by selecting the first User in the group, pressing the **Shift** button, and then selecting the last User.
2. Click the **Delete** button.

The Delete confirmation page appears.

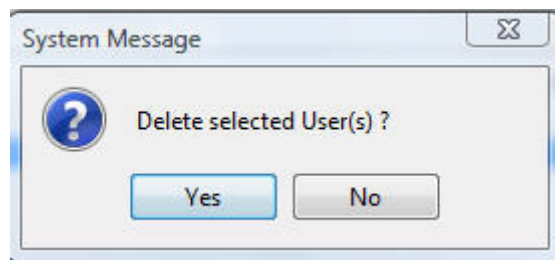


Figure 16 – Delete User Confirmation

3. Click **Yes**.

The User(s) are deleted from the system.

#### 3.5.3 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.

➔ **To block a User:**

1. In the **Add User** page (see Figure 15), in the **Access** parameter, select the **Block** checkbox.

#### 3.5.4 Editing User Information

You can change any of the following User parameters: **Permission**, **Access**, and **Password**.

➔ **To edit User information:**

1. In the **Users** page (see Figure 14), select a User and click the **Edit** button.

The Edit User page appears, with the User's information in the parameters.

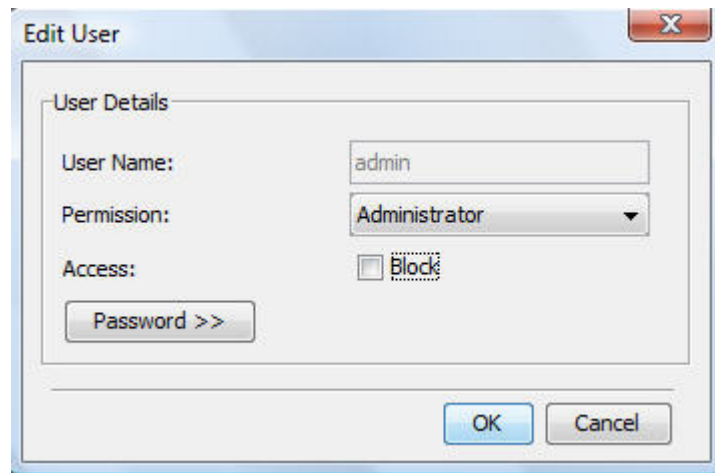


Figure 17 – Edit User Page

2. Change the **Permission** and/or **Access** as required.

3. To change the password, click .

The **Password** parameter opens. In the upper textbox, type the new password; in the lower textbox, confirm the new password.



You cannot change the password of an Administrator who is currently logged on to the system.

4. Click **OK**.

The User page opens with the user information changed accordingly.

## 3.6 Configuring the KVM Switch

When a KVM switch is connected to the IP Control system, configure the following switch parameters:

- The KVM switch manufacturer and model
- The names of the servers connected to the KVM switch – It is recommended to give the servers connected to IP Control unique names, so that users accessing the system can easily identify them.
- The number of POCs attached to those servers that are configured with POCs attached to them

### ➔ To configure a KVM switch:

1. From the configuration menu, select **Switch Configuration**.

The KVM Switch Configuration page appears.

Manufacturer & Model		
Manufacturer:	(None)	
Model:	(None)	

Server Name		
1	Server1	0

Install Switch Definition File	
File:	<input type="text"/> ...
<input type="button" value="Import Sdf"/>	

Figure 18 – KVM Switch Configuration Page

2. From their respective dropdown lists, select the **Manufacturer** and **Model** of the connected KVM switch.



If the KVM switch type used by the system does not correspond to any of those listed in the **Manufacturer/Model** dropdown lists, download the correct Switch Definition file, as described in Section 3.6.1.

The servers that can potentially be connected to the selected KVM switch, appear in the **Server Name** section. The number of servers that appear corresponds to the number of ports in the selected KVM switch.

## Configuring the Network

### Configuring the KVM Switch

The screenshot shows a configuration window for a KVM switch. At the top, there are dropdown menus for 'Manufacturer' (Minicom) and 'Model' (Smart CAT5 16 Ports (PrtScr)). Below this is a 'Server Name' section containing a table with 8 rows. The first row is labeled 'Server 1' and has a POC count of 9. The other 7 rows are labeled 'UNUSED' and have a POC count of 0. At the bottom, there is an 'Install Switch Definition File' section with a 'File:' input field and an 'Import Sdf' button. Annotations on the left side of the image point to the 'Server name' column and the 'Number of POCs connected to the Server' column.

Server Number	Server Name	POCs	POCs
1	Server1	0	9
2	UNUSED	0	10
3	UNUSED	0	11
4	UNUSED	0	12
5	UNUSED	0	13
6	UNUSED	0	14
7	UNUSED	0	15
8	UNUSED	0	16

Figure 19 – Servers of Selected KVM Switch

The following information is displayed for each potential server:

- The server number
  - The server name, if the server is connected to the KVM switch; UNUSED if the server is not connected
  - The number of POCs attached to the server, provided that POCs are attached to the server; otherwise, it displays "0"
3. To change the name of a connected server, highlight the current server name, and type a new name.



Servers named **UNUSED** (see Figure 19) are not connected to the KVM Switch, and their names cannot be changed. You can only change the names of servers that are connected to the KVM Switch.

4. If POCs are attached to the server (see Section 3.7.1), type the number of POCs attached to the server.

### 3.6.1 Installing the Switch Definition File

If the KVM switch type used by the system does not correspond to any of those listed in the Manufacturer/Model dropdown lists, you can find the relevant Switch Definition file in the Support section of our website – <http://www.minicom.com/phandlj.htm>

➔ **To install the Switch Definition file:**

1. Navigate to <http://www.minicom.com/phandlj.htm>, download the Switch Definition file onto the client computer, and unzip it.
2. Click the Browse button adjacent to the **File** parameter, to locate and select the relevant KVM switch definition file.

The filename appears in the **File** textbox.

3. Click **Import Sdf**.

The Switch Definition file is replaced.

## 3.7 Configuring the Serial Port Settings

When you have a Serial device connected to the system, you must configure the Serial Port settings.

➔ **To configure the serial port settings:**

1. From the configuration menu, select **Serial Port**.

The Serial Port page appears.

Serial Port 1	
Device Name:	Serial
Baud Rate:	9600
Parity:	NONE
Show:	<input checked="" type="checkbox"/>
Char Set:	ANSI
Data Bits:	8
Stop Bits:	1
Assign to:	NONE

Figure 20 – Serial Port Page

2. Type a **Device Name** and choose the correct device parameters.
3. Select the **Show** checkbox to display the Serial device in the list of servers/devices that can be accessed.

### 3.7.1 Assigning Serial Port

When a Minicom Serial Remote Power Switch (RPS) or POC is connected to the Serial port, select **RPS** or **POC**, respectively, from the **Assign to** dropdown list. All other parameters are then grayed out. See the RPS or POC Installation Guide for further information on installing and operating the RPS or POC, respectively.



After assigning the Serial Port to POC, go to the Switch Configuration page to type the number of POCs attached to each server (see Section 3.6 above).

## 3.8 Configuring the Security Settings

This section describes how to configure the security features, such as Account Blocking, Password Policy, and Idle Timeout.

You can choose a standard or high security level of password. The following table describes both these options.

Standard Security Policy	High Security Policy
At least six characters	At least eight characters; must include at least one digit, one uppercase letter, and one of the following "special" characters: !, @, #, \$, %, ^, *, (), _ - , +, =, [], ' , ; , ? , /, or {}
Must not include the user name	Must not include the user name

### ➔ To configure the security settings:

1. From the configuration menu, select **Security**.

The Security page appears.

The screenshot shows the Security Page configuration interface with three sections:

- Account Blocking:** Block after: 3 attempts within (hr:min): 1 : 0. Block account:  for period (hr:min): 1 : 0,  forever.
- Password Policy:**  High security password policy.
- Idle Timeout:** Disconnect after: 10 minutes of inactivity.

Figure 21 – Security Page

2. In the **Account Blocking** section:

- In **Block after**, type the number of allowable attempts to log in with a wrong username or password in a time period specified in **attempts within**, prior to a forced time lock.
  - In **Block account**, select **for period** to block the account for a specified period of time, or **forever** for a total block.
3. Select the **High security password policy** checkbox to enable the high security password policy; clear the checkbox for the standard security policy to apply.
  4. In **Disconnect after**, select the timeout inactivity period after which the user is disconnected from the system. Select **No Timeout** to disable timeout.

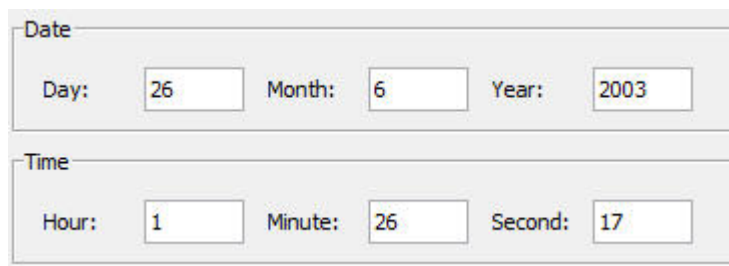
### 3.9 Configuring the System Date and Time

This section describes how to configure the system date and time.

➔ **To configure the date and time:**

1. From the configuration menu, select **Date & Time**.

The Date and time page appears.



Date		
Day:	26	Month: 6
Year:	2003	

Time		
Hour:	1	Minute: 26
Second:	17	

Figure 22 – Date and Time Page

2. In **Date**, type the current date: **Day**, **Month**, and **Year**.
3. In **Time**, type the current time: **Hour**, **Minute**, and **Second**.

### 3.10 Performing Additional Configuration Operations


You can perform the following additional operations on IP Control:

- Install an SSL certificate.
- Upgrade firmware.
- Restore factory settings.

#### 3.10.1 Installing an SSL Certificate

You can install an SSL Certificate, to ensure secure transactions between the Web servers and browsers.

➔ **To install an SSL Certificate:**

1. In the toolbar, select  **SSL Certificate**.

The SSL Certificate page appears.

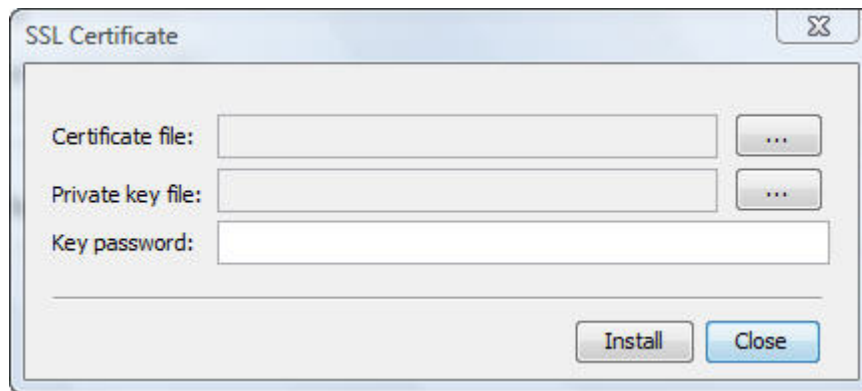


Figure 23 – SSL Certificate Page



2. In **Certificate file**, browse to locate the **Cer** file.
3. In **Private key file**, locate the **private key** file in Microsoft pvk format.
4. In **Key password**, type the password required to upload the Private Key file.



Each Private Key file is generated with a unique password.

5. Click **Install**.

The SSL Certificate is installed.


6. Save the changes and restart the system, by clicking the  **Save** button, and then the  **Device Reboot** button.

#### 3.10.2 Upgrading Firmware

You can upgrade the IP Control firmware to take advantage of new features.

➔ **To upgrade firmware:**

1. Download the firmware from Minicom's website at:  
<http://www.minicom.com/phandlh.htm>.
2. Save the firmware file on the client computer.

- In the toolbar, select  **Device Upgrade**.

The Device Version Upgrade page appears, displaying the current firmware version on the device.

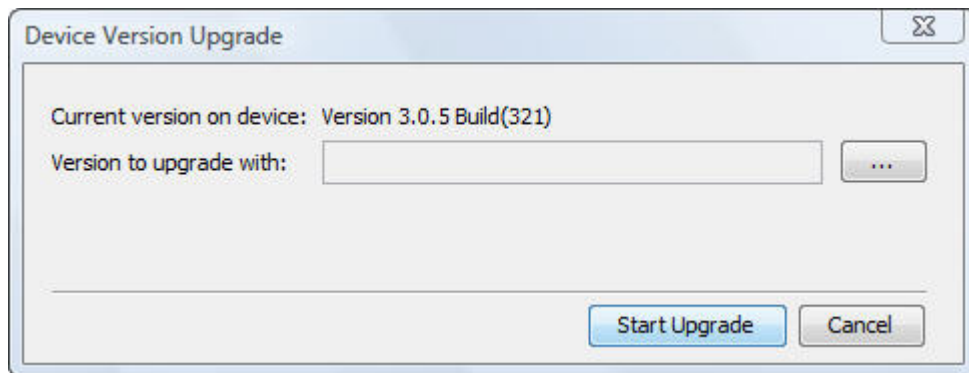



Figure 24 – Device Version Upgrade Page

- In **Version to upgrade with**, browse to locate and upload the firmware file.
- Verify the current and uploaded version of the firmware.
- Click **Start Upgrade**.

The upgrade starts.

- On upgrade completion, on the toolbar, click  **Device Reboot**.

A confirmation box appears.

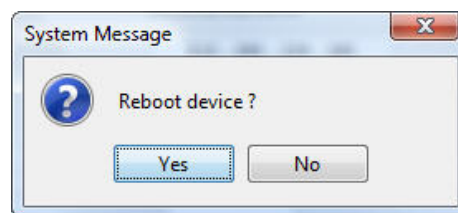


Figure 25 – Reboot Confirmation Page

- Click **Yes**.

The unit reboots. After about 30 seconds, the Login page appears.



Depending on the type of firmware upgrade, the following settings may be erased: User settings, KVM switch settings, mouse and video adjustments, and RS232 settings. The network settings remain intact. For more information, refer to the firmware release notes.

### 3.10.3 Restoring Factory Settings


You can restore the IP Control unit to its factory settings. This restores the original IP Control parameters, resetting all the information added by the administrators, including: Network settings\*, Servers, Switches, Users, and Passwords.

\* You have the option to preserve Network settings – as explained in the following procedure.



Once reset, the data cannot be retrieved.

➔ **To restore factory settings:**

1. In the toolbar, select  **Factory Restore**.

The Restore Factory Settings page appears.

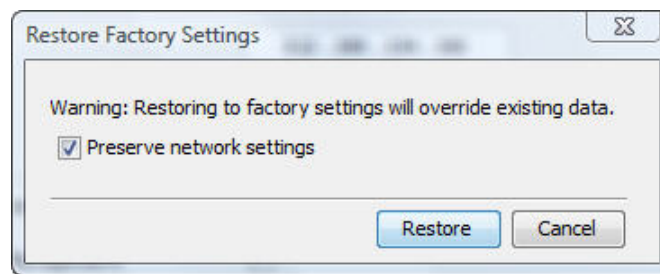


Figure 26 – Restore Factory Settings Page


2. To preserve network settings, select the **Preserve network settings** checkbox.
3. Click **Restore**.

Factory settings are restored.

## 3.11 Reloading a Page

You can load the parameters on any configuration page with the settings from the IP Control device. This is convenient if you have already changed settings on the page, and want to restore the device settings.

➔ **To reload a page:**

1. In the Configuration page toolbar, click the  **Reload** button.

The parameters are populated with the device settings.


## 3.12 Saving Changes and Logging Out

Once you have completed configuration changes, you must save them.

Changes to the SSL Certificate pages require saving and restarting.

Saving the configuration changes after changing the Device page restarts the unit automatically.

### ➔ To save changes:

1. In the Configuration page toolbar, click the  Save button.

If you made changes to the Device page, the system automatically prompts you to reboot and restart the device, by displaying the following device reboot confirmation box:

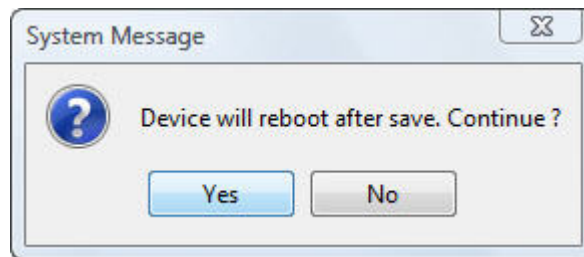


Figure 27 – Device Reboot Confirmation Message

1. Click **Yes**.

A message box informs that Save has completed.

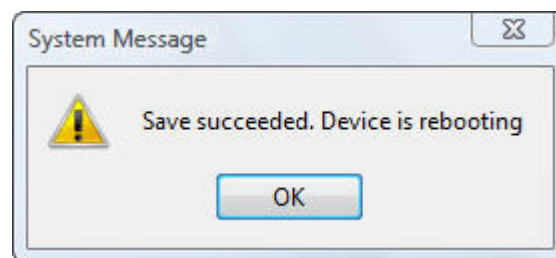


Figure 28 – Save Succeeded Message

2. Click **OK**.

Device reboots, and when it completes a Logon page appears.

## Configuring the Network

---

### Saving Changes and Logging Out

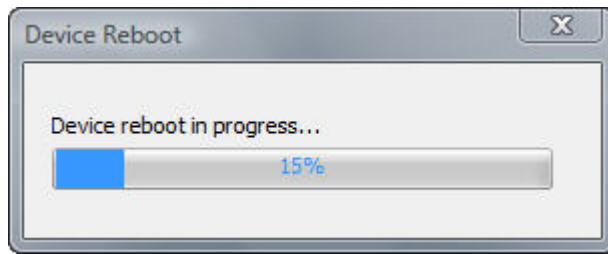


Figure 29 – Device Rebooting Progress Box

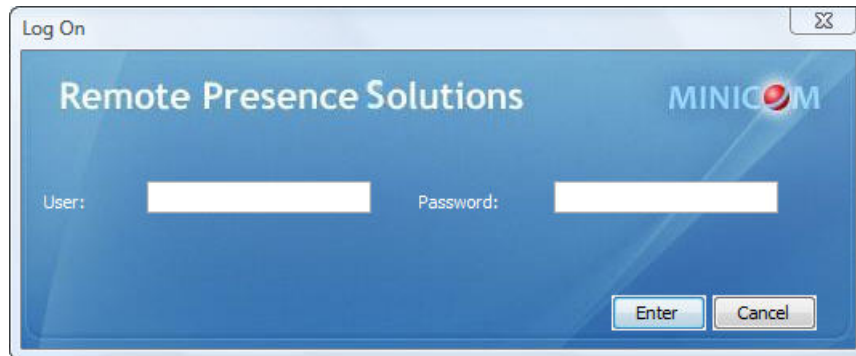
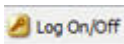


Figure 30 – Logon Page after Rebooting

3. Type your **User** name and **Password** and click **Enter**.

The Configuration page opens.

➔ **To log off:**

1. In the screen toolbar, click the  button.

The Configuration screen is closed, and the session closes.

## 4 Conducting a Remote Session

The remote session enables remotely accessing the server connected to IP Control. Before starting a remote session, IP Control must be fully configured.

You can perform the following from the remote session:

- Display/hide the toolbar.
- Set the session profile.
- Display the session in full screen mode.
- Verify Remote Presence Solutions information.
- Adjust video settings.
- Power manage the target servers, provided that you have installed POC or RPC.
- Manage keyboard sequences.
- Synchronize mouse pointers.
- Switch to a different server or device.

### 4.1 Starting a Remote Session

On first connection, install the Minicom certificate and verify that you have the latest Java installed on your computer. If not, you can download and install Java from: <http://www.java.com/en/download/index.jsp>

When using the Firefox browser, install the Minicom Firefox add-on.

The following procedure describes how to log into a remote session from a client computer.

➔ **To log onto a remote session:**

1. Open your Web browser (Internet Explorer 7.0 / Firefox 3 or later).
2. Type the IP Control system IP address - [https://IP address/](https://IP_address/) and press **Enter**.

The Web page appears (see Figure 10).

3. In the Web page, click **Log On**.

Java installs. After installation has completed, the logon page appears.

## Conducting a Remote Session

### Starting a Remote Session

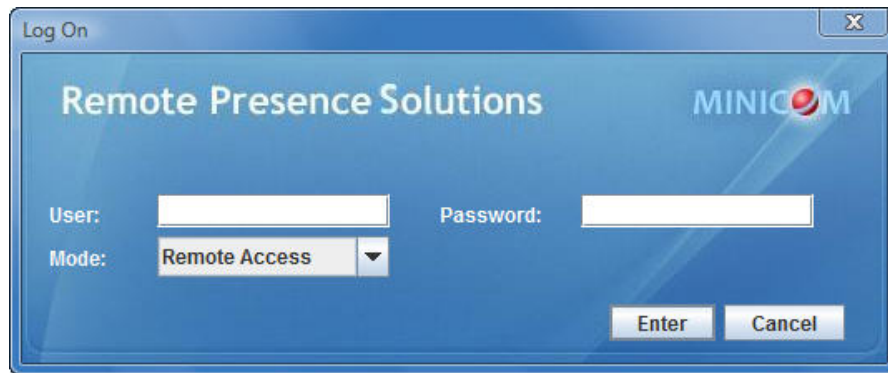


Figure 31 – Logon Page

Leave **Mode** as **Remote Access**.

4. In **User** and **Password**, type the default Administrator name and password, **admin** and **access** respectively (both lower case).
5. Click **Enter**.

The screen of the target server or the currently selected server on the KVM switch that is connected directly to IP Control, appears with the IP Control toolbar.

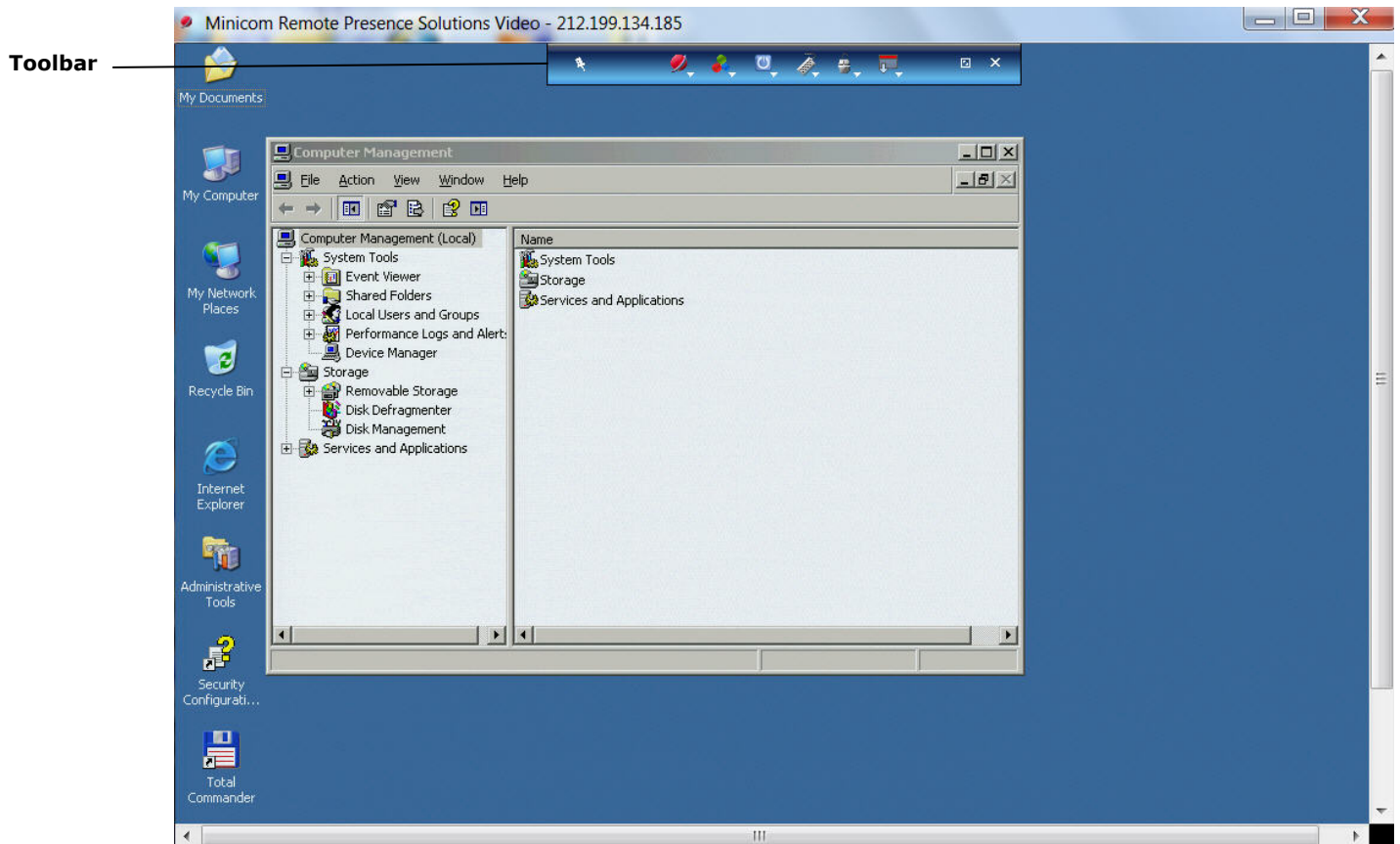










Figure 32 – Remote Session Page

### 4.1.1 Remote Session Toolbar Buttons

The following table describes the functionality of the Remote Session toolbar buttons.

Button	Description
	Toggle button for displaying/hiding toolbar.
	Session button. Pressing this button opens up a dropdown menu for selecting: <b>Session Profile</b> – enables configuring remote session profile session <b>About</b> – displays client, firmware, Switch File, and KME version information
	Video button. Pressing this button opens up a dropdown menu for performing: <b>Refresh</b> – for refreshing the video image <b>Video Adjust</b> – for automatically adjusting the video image <b>Advanced</b> – for manually setting video settings <b>Performance</b> – changing video performance by changing mode and/or bandwidth
	Keys button. Pressing this button opens up a dropdown menu with predefined key sequence names and <b>Special Keys</b> item which enables you to: add a keyboard sequence, record a new custom key, edit an existing key sequence, and delete a key sequence
	Mouse button. Pressing this button opens up a dropdown menu for performing: <b>Calibrate</b> – calibrates the speeds of the mouse pointers of the target server and client computer in Win98, NT or 2000 <b>Align</b> – for aligning the local mouse pointer with the remote target server mouse pointer <b>Mouse Settings</b> – for manually synchronizing the mouse pointers
	Server/Serial button. Pressing this button displays the connected servers and serial devices. You can switch to a different server/device.
	Restore button. To toggle Full screen mode on and off.
	Logoff button. Closes the current remote session and displays the logon Web page.

## 4.2 Sharing a Remote Session

Users who want to remotely work on a server at the same time and collaborate their work, can share a remote session. All users in the remote session can connect to see the video at the same time and share the Keyboard/Mouse control. Up to five users can share the same remote session.

When connecting to a target server that other users are already connected to, the following message appears:

### Displaying the Toolbar

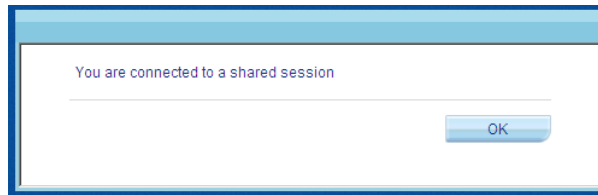



Figure 33 – Shared Remote Session

#### 4.2.1 Exclusive Session

When starting a remote session and there are no other logged in users, a user can prevent other users from connecting to the session (see Section 4.4, step 4). This means that the user is the only one who can see the video and control the Keyboard/Mouse, enabling the user to work on the server without anyone seeing or interfering in the user's work.

### 4.3 Displaying the Toolbar

The Toolbar appears briefly at the top of the screen (see Figure 32). 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 tack icon  on the toolbar.

### 4.4 Setting the Session Profile

You can set the remote session display features, as follows:

- Select the format of the mouse pointer, or hide it
- Hide the toolbar
- Display the session in full screen mode – You can work on the target server as if you are working on a local computer, using full screen mode. In Full Screen mode, the desktop window disappears, and is replaced by the accessed target server desktop.

- Prevent other users from logging into the same session

➔ **To set the session profile:**

1. On the toolbar, select  > **Session Profile**.

The Session Profile window appears.

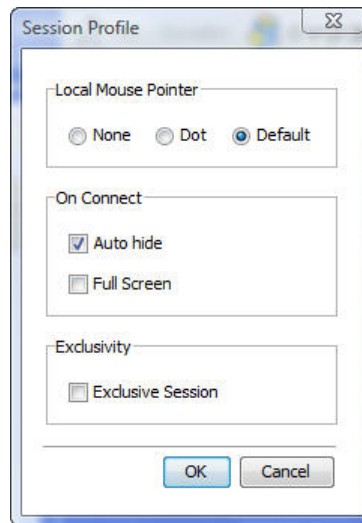




Figure 34 – Session Profile Dialog Box

2. In **Local Mouse Pointer**, select one of the following options to set the appearance of the client computer mouse pointer:
  - **None** – to hide the mouse pointer
  - **Dot** – for the mouse pointer to appear as a dot
  - **Default** – for the mouse pointer to appear as a regular-shaped mouse cursor
3. In **Auto Connect**, select:
  - **Auto hide** – to hide the toolbar from the next connection onwards
  - **Full Screen** – to display the remote session screen in full screen mode from the next connection onwards. To toggle full screen mode on and off, you can click the Restore button  (see Section 4.4.1).
4. In **Exclusivity**, select the **Exclusive Session** checkbox when starting a remote session and there are no other logged in users; this prevents other users from logging into the session.

#### 4.4.1 Full Screen Mode

You can work on the target server as if you are working on a local computer, using full screen mode. In Full Screen mode, the desktop window disappears, and is replaced by the accessed target server desktop.

##### ➔ To work in full screen mode:

1. Ensure that the client computer has the same screen resolution as the target server.
2. On the toolbar, click the Restore button .

## Conducting a Remote Session

### Verifying Remote Presence Solutions Information

The desktop window disappears.

➔ **To exit full screen mode:**

1. On the toolbar, click the Restore button .

The desktop window appears.




Full screen mode can also be activated from the Session Profile box, see Section 4.4, step 3.

## 4.5 Verifying Remote Presence Solutions Information

You can verify the client, firmware, KME (Keyboard/Mouse Emulation firmware), and Switch file versions installed on your IP Control. This information can assist system administrators in troubleshooting and support.

➔ **To verify Remote Presence Solutions information:**

1. On the toolbar, select  > **About**.

The information screen appears.

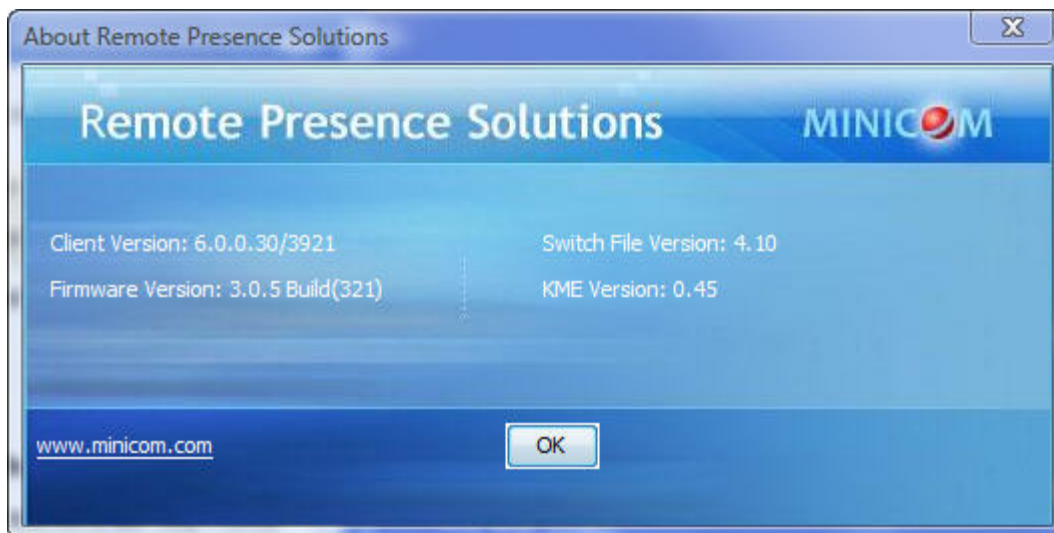


Figure 35 – Remote Presence Solutions Information

## 4.6 Changing the Video Performance Settings

From the toolbar, you can alter the video performance settings, by selecting a different mode or bandwidth.

The mode can be set to:

- **Fixed** – Enables you to select any bandwidth option. For example, in a LAN environment, it is best to set the bandwidth setting to **High**. For VPN and Internet environments, you may want to alter the settings to increase responsiveness.
- **Adaptive** – Automatically adapts to the best compression and colors according to the network conditions.

You can choose to display more colors for more fidelity, or less colors to reduce the volume of data transferred through the network. Choosing more colors requires more bandwidth.

The bandwidth can be set to:

- **Maximum** – For optimal performance when working on a LAN. This gives no compression and high color (16 bit)
- **High** – For low compression and high color (16 bit)
- **Medium** – For medium compression and either high color or 256 colors; Recommended when using a standard Internet connection
- **Low** – For high compression and 16 colors

➔ **To alter the settings:**

1. On the toolbar, select  > **Performance**.

The Performance dialog box appears.

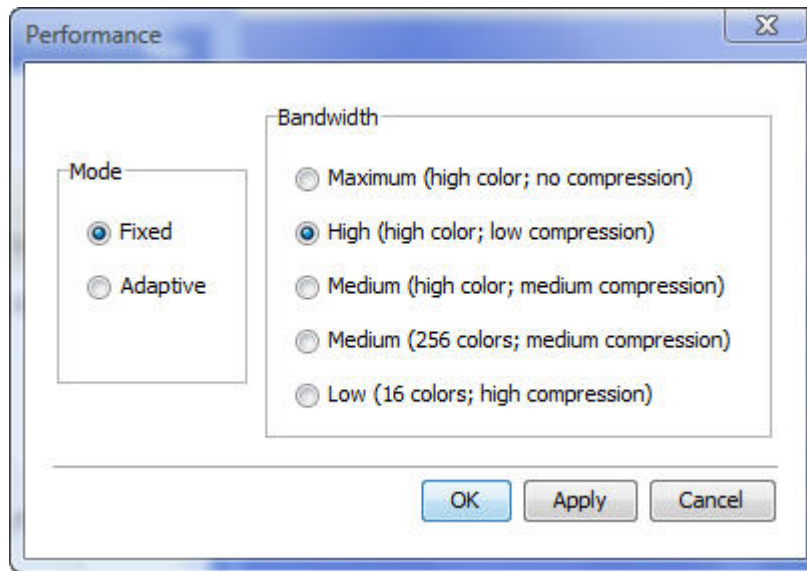


Figure 36 – Performance Settings

2. In **Mode**, select **Fixed** or **Adaptive**.
3. For **Fixed** mode, in **Bandwidth**, select **Maximum**, **High**, **Medium** (high color or 256 colors), or **Low**.
4. Click **OK**.

The chosen setting takes effect and the screen of the last accessed target server appears.

## 4.7 Adjusting the Video


There are three ways to adjust the video image:

- Refreshing the video image
- Automatically adjusting the video image
- Manually changing advanced video settings

### 4.7.1 Refreshing the Video Image

The video image may require refreshing when changing the display attributes of a target server. Refreshing completely regenerates the video image.

➔ **To refresh the video image:**

1. On the toolbar, select  > **Refresh**.

The image is refreshed.

## 4.7.2 Automatically Adjusting the Video Image

The video view may need to be adjusted for each target server or new screen resolution. In most cases, adjusting the video view using the default video settings gives the optimal view.

➔ **To automatically adjust the video image:**

1. On the toolbar, select  > **Video Adjust**.

The progress of video adjustment is displayed.

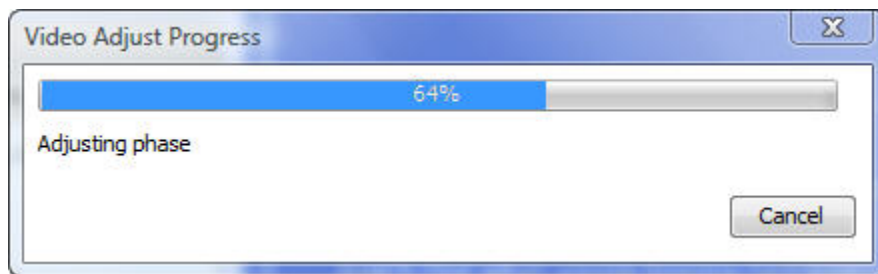


Figure 37 – Video Adjust Progress

The process takes a few seconds. If the process runs more than a few times, it is an indication that 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.

## 4.7.3 Manually Adjusting Video Settings


Although automatic adjustment of video generally optimizes the video view, you may want to fine-tune the results.

You can use the advanced video adjustment options:

- To fine-tune the target server video settings after auto adjustment
- To adapt to a noisy environment or a nonstandard VGA signal
- When in full-screen DOS/CLI mode

After adjusting the video settings manually, you can always revert to automatically adjusting the video settings, as explained in Section 4.7.2.

➔ **To manually adjust the video settings:**

1. On the toolbar, select  > **Advanced**.

The manual controls appear.

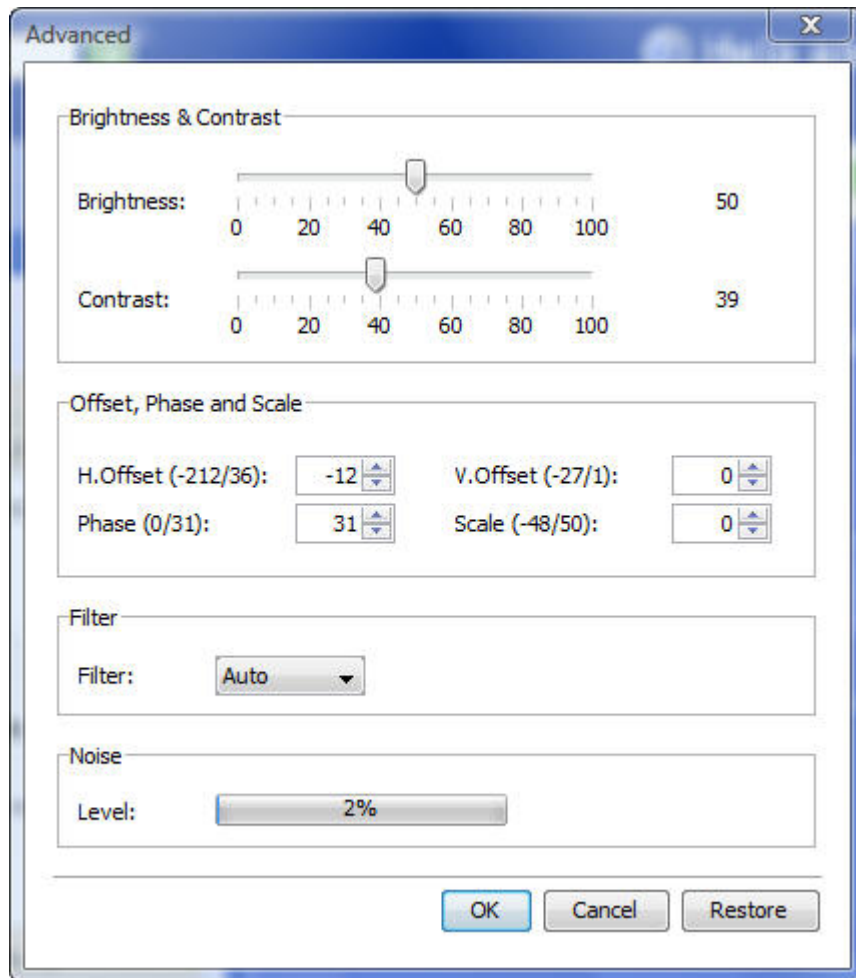


Figure 38 – Manual Video Adjustments Controls

2. In **Brightness** and **Contrast**, use the scales to adjust the brightness and contrast of the displayed image, respectively. Move the sliders to change the displayed image. Click in the area of the sliders for fine-tuning.
3. In the **Offset, Phase and Scale** section:
  - In **H. Offset**, select the starting position of each line on the displayed image.
  - In **V. Offset**, select the vertical starting position of the displayed image.
  - In **Phase**, select the point at which each pixel is sampled.
  - In **Scale**, select the scale resolution of the session image.

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


4. In **Filter**, select the filter of the input video from the server. A higher filter reduces the noise level but makes the image heavier. Options are: **Auto**, **No Filter**, **Low**, **Medium**, and **High**.

5. **Level** displays the Video "noise" level when a static screen is displayed.
6. Click **OK**.

## 4.8 Power Managing the Target Servers

When a Minicom Remote Power switch or POC is connected to the Serial port of the IP Control unit, you can power manage the target servers via the Power menu.

### ➔ To power manage the target servers:

1. On the toolbar, click .

The Power menu appears.

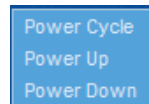



Figure 39 – Power Menu

2. Select one of the following options:
  - **Power Cycle** – to send a power cycle to the currently accessed target server, meaning that the target server is first powered down and then powered up
  - **Power Up** – to power up the currently accessed target server
  - **Power Down** – to power down the currently accessed target server



Only the currently accessed target server is affected. Therefore, to power manage other target servers, you must access each one individually.

## 4.9 Managing Keyboard Sequences

You can select any keyboard sequence (a combination of keys that performs a specific process) that appears in the dropdown menu of the toolbar button  to send it to the target server to initiate its associated process. For example, selecting **Ctrl-Alt-Del** sends this three-key sequence to the target server to initiate its Shutdown/Login process.

When clicked, these key sequences transmit directly to the target server, and do not affect the client computer.

This section describes how to:

- Add predefined keyboard sequences to the list of keyboard sequences


## Conducting a Remote Session

---

### Managing Keyboard Sequences

- Create customized keyboard sequences
- Edit existing keyboard sequences
- Delete existing keyboard sequences

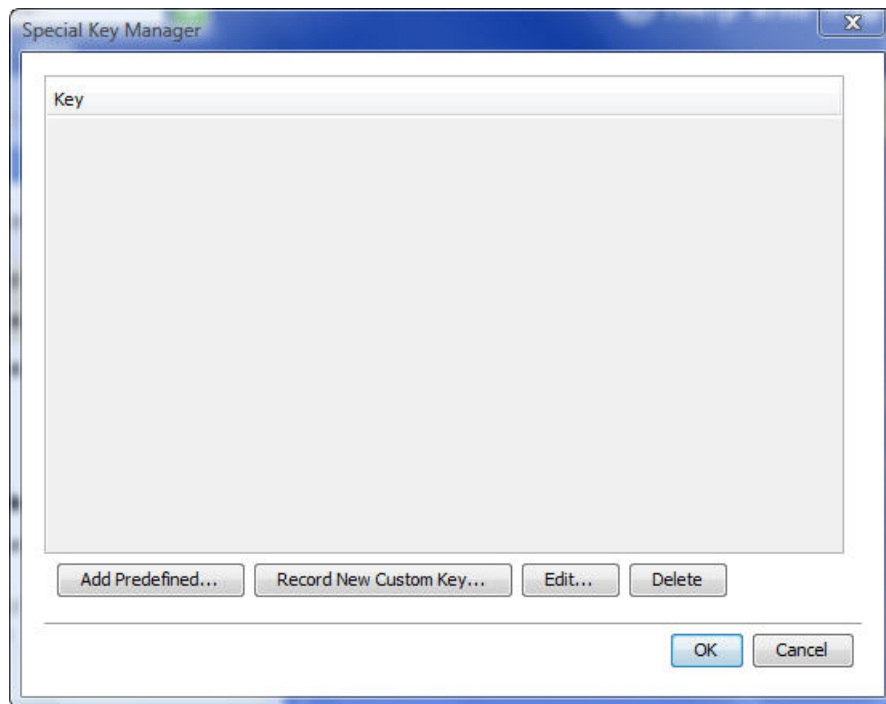
#### 4.9.1 Adding a Keyboard Sequence

You can add predefined keyboard sequences to the list of keyboard sequences that can be accessed directly from the dropdown list of the toolbar item .

➔ **To add a keyboard sequence:**

1. On the toolbar, click  > **Special Keys**.

The Special Key Manager box appears.



*Figure 40 – Special Key Manager*

2. Click the **Add Predefined** button.

A list of existing sequences appears.

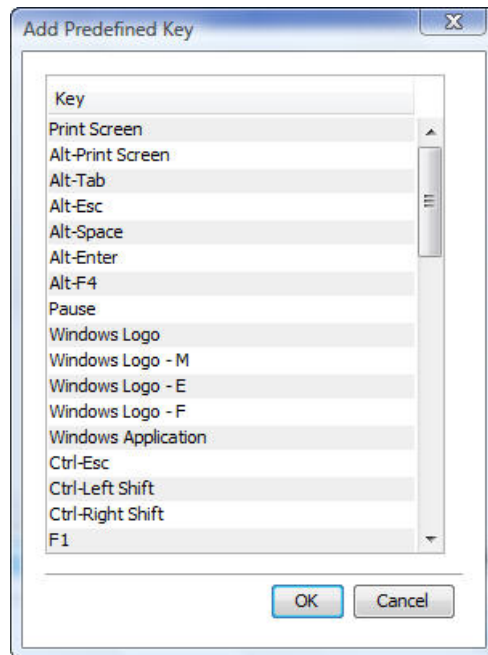


Figure 41 – Add a Predefined Key Dialog Box


3. Select a key sequence and click **OK**.

The sequence appears in the Special Key Manager box.

4. In the Special Key Manager box, click **OK**.

The sequence appears in the Keyboard Key sequence list.

#### 4.9.2 Recording a New Custom Key

This section describes how to define a new keyboard sequence. After defining the keyboard sequence, you can add it to the list of keyboard sequences that can be accessed directly from the dropdown list of the toolbar item  (see Section 4.9.1).

➔ **To record a keyboard sequence:**

1. In the Special Key Manager box (see Figure 40), click **Record New Custom Key**.

The Record Macro box appears.

## Conducting a Remote Session

### Managing Keyboard Sequences

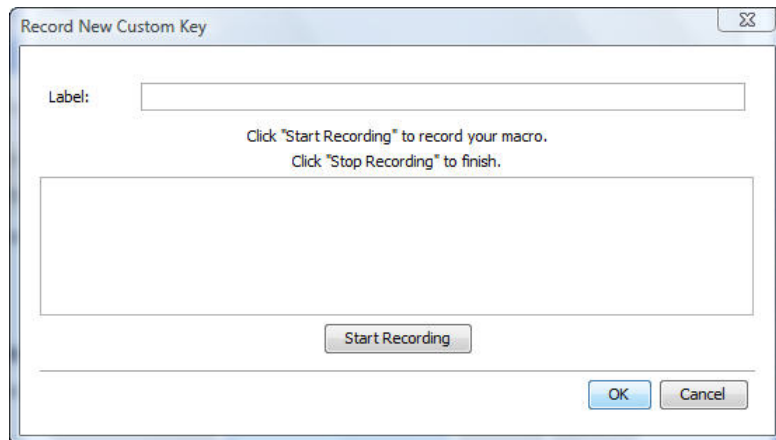


Figure 42 – Record Macro Box

2. In **Label**, type a name for the new key sequence.
3. Click **Start Recording**.
4. On your keyboard, press the keys to include in the key sequence.

The names of the pressed keys appear in the provided area.

5. Click **Stop Recording**.
6. Click **OK**.

The new key sequence is now on the list of predefined key sequences.

### 4.9.3 Editing a Key Sequence

#### ➔ To edit a predefined keyboard sequence:

1. In the Special Key Manager box (see Figure 40), select the desired key sequence and click **Edit**.

The Record Macro box appears (see Figure 42). The name of the key sequence to edit appears in the **Label** field.

2. Click **Start Recording**.
3. On your keyboard, press the keys to include in the key sequence.

The names of the pressed keys appear in the provided area.

4. Click **Stop Recording**.
5. Click **OK**.

The key sequence definition is updated in the system.

### 4.9.4 Deleting Key Sequence(s)

You can delete a single or multiple key sequences from the system.

➔ **To delete a keyboard sequence:**

1. In the Special Key Manager box (see Figure 40), select the desired key sequence(s) to delete. Select a group of keys by selecting the first key in the group, pressing the **Shift** button, and then selecting the last key.
2. Click **Delete**.

The delete confirmation box appears.

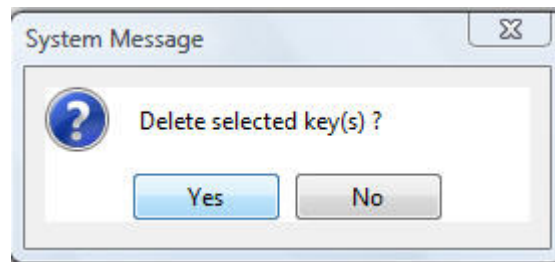


Figure 43 – Delete Key(s) Confirmation Box

## 4.10 Synchronizing Mouse Pointers

For best mouse performance and superior customer experience, Minicom recommends that you set certain mouse settings in the target operating system. This applies to all targets running Windows, such as XP, Windows 7, Windows Server 2003, and Windows Server 2008.

When working at the client computer, two mouse pointers appear – one of the client computer and one of the target server; the former is on top of the latter. The mouse pointers should be synchronized. The following explains what to do if they are not synchronized.



Before synchronizing mouse pointers, adjust the video of the target server (see Section 4.7); otherwise, mouse synchronization may not work.

### 4.10.1 Manually Synchronizing the Mouse

If the mouse settings on the target server have been changed, or when the operating system on the target server is Windows XP / 2003 Server / 7 / 2008 Server, Linux, Novell, SCO UNIX, or SUN Solaris, you must synchronize the mouse pointers manually.

➔ **To manually synchronize mouse pointers:**

1. On the toolbar, select  > **Mouse Settings**.

The Mouse Settings box appears.

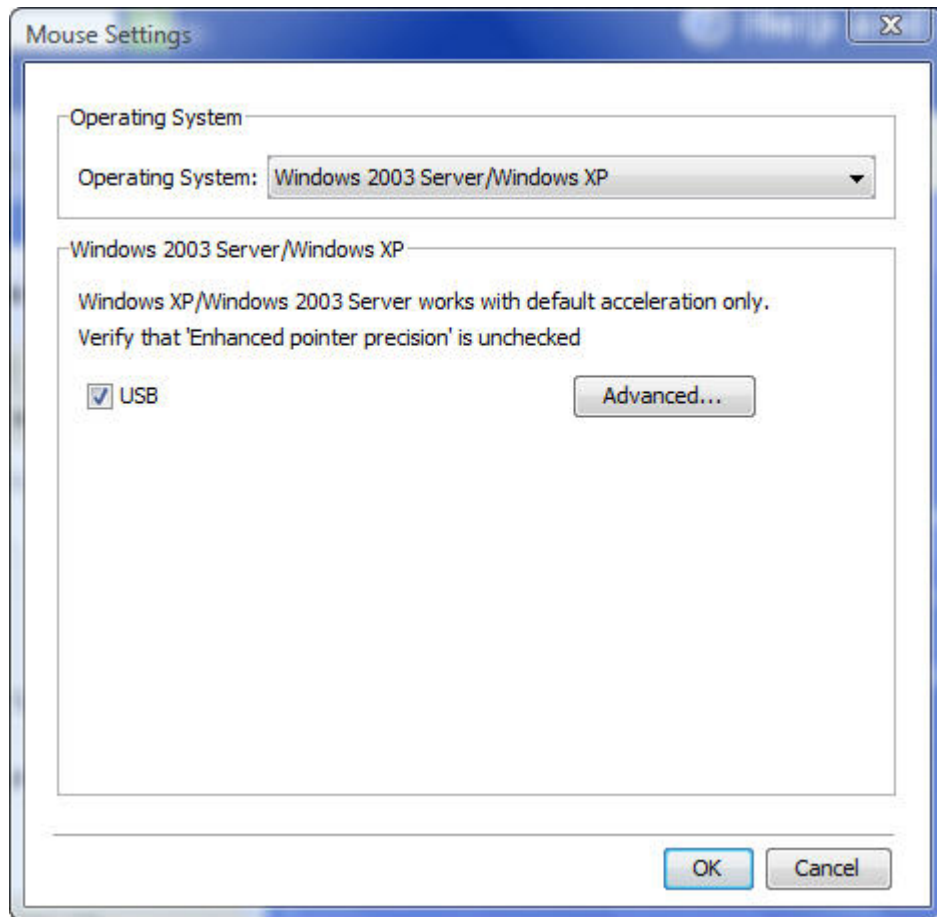


Figure 44 – Relative Mouse Settings

2. In **Operating System**, from the dropdown menu, select the target’s operating system.  
Instructions and sliders appear.
3. Follow the instructions and set any relevant sliders to the same values as set in the target’s Mouse Properties window.
4. Click **OK**.  
The mouse pointers are synchronized.

### Examples

The following are examples of the instructions for two different target operating systems. After performing the instructions for the selected operating system, you should click **OK** to synchronize the mouse pointers.

1. For **Windows 7**: Go to the Mouse Properties on the target and clear the **Enhance pointer precision** checkbox.

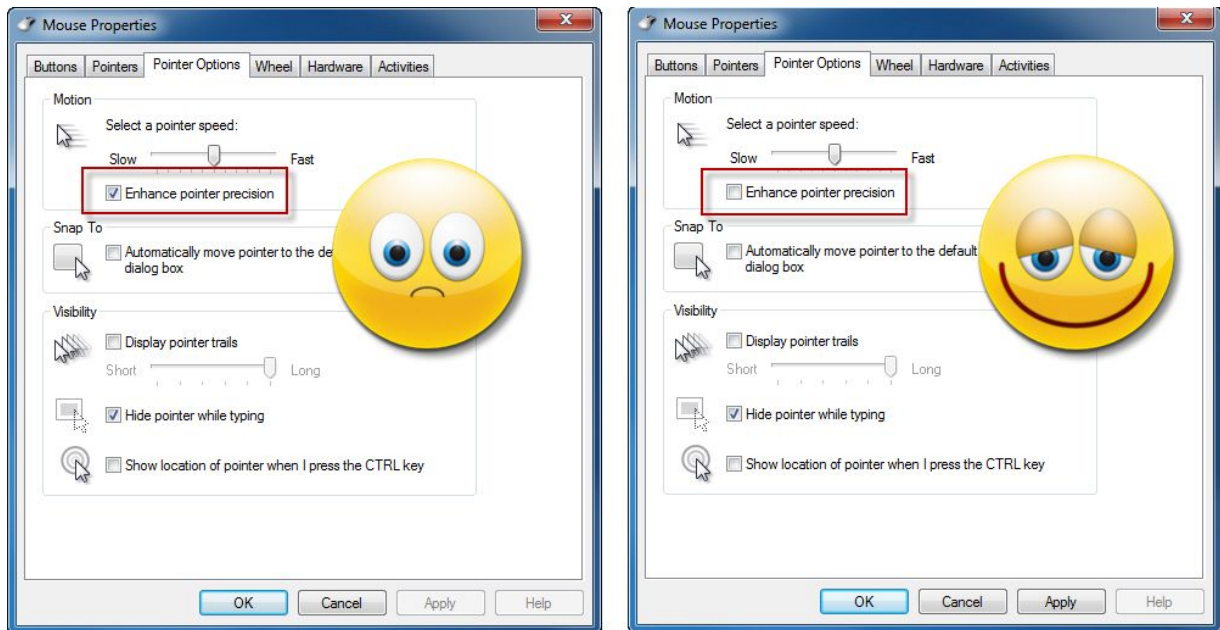


Figure 45 – Windows 7 Mouse Properties

2. For **Windows 2000**: If Mouse Properties were ever changed for the target – even if they have been returned to their original state – clear the **Default** checkbox

Default

### The USB Option

You can use the **USB** option if you have USB to PS2 conversion between IP Control and the target server via any of the following:

- USB-to-PS/2 adapter
- USB KVM dongle, such as RICC/ROC USB, X-RICC USB, and Phantom Specter USB
- Unsupported operating systems
- SUN Solaris

Use this option if you are sure of the custom acceleration algorithm you are using, or have been informed to do so by customer support.

If you have USB to PS2 conversion between IP Control and the target server (either USB-to-PS/2 adapter, or USB KVM dongle, such as RICC/ROC USB, X-RICC USB, and Phantom Specter USB, or unsupported operating systems or SUN Solaris), use the **USB** option.

#### **Advanced Mouse Emulation**

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

These settings come into effect when IP Control resets the local mouse after the KVMIP session is over.

➔ **To set the type of mouse that you want IP Control to emulate:**

1. In the **Mouse Settings box** (see Figure 44), click **Advanced**.

The Mouse Emulation box appears.

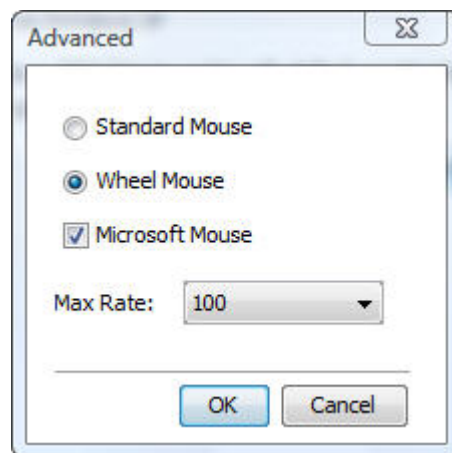


Figure 46 – Mouse Emulation Box

2. Select the mouse connected to the Local Console port on the IP Control, as follows:

- **Standard Mouse** – if the local mouse is a non-Microsoft two-button mouse; in this case, clear the **Microsoft Mouse** checkbox.
- **Wheel Mouse** – Microsoft mouse or Microsoft optical mouse

3. In **Max Rate**, select the maximum mouse report rate.

For Sun Solaris the default value is 20 in order to support older Sun versions.

4. Click **OK**.

#### **4.10.2 Aligning the Mouse Pointers**

When accessing the target server, the mouse pointers may appear at a distance to each other, due to the mouse on IP Control losing sync with the mouse on the host system. You can align the local mouse pointer with the remote target device's mouse pointer.

**➔ To align the mouse pointers:**

1. On the toolbar, select  > **Align** (or press **Ctrl+M**).

The mouse pointers align.


### 4.10.3 Calibrating Mouse Pointers

A target server may have a different mouse pointer speed than the client computer. Calibrating automatically discovers the mouse speed of the target server and aligns the two pointers.

You can perform automatic calibration when the target server operating system is Windows NT4, 2000, or 98.

IP Control saves this alignment so that calibration is only needed once per target server.

**➔ To perform the calibration:**

1. On the toolbar, select  > **Calibrate**.

If the Video Noise Level is above zero, calibration may not work. In this case, go to Video Adjustment and try to eliminate the noise by automatically adjusting the video (see Section 4.7.2) and/or adjusting the bars in manual video adjust (see Section 4.7.3), and then performing the mouse calibration.



If the mouse settings on the target server have been changed, you must synchronize mouse pointers manually, as explained below.

## 4.11 Switching to a Different Server/Device

In the middle of a remote session, you can switch to a different server or device.

**➔ To connect to a different server or device:**

1. On the toolbar, click .


A list of connected servers/devices appears. There is a checkmark near the server/device of the remote session.

2. Click the desired server or Serial device.

The screen of the server or Serial device terminal emulation window appears.

## 4.12 Disconnecting the Remote Session

➔ To disconnect the session:

1. On the toolbar, click .

The Login Web page appears. You can re-login or close the browser window.

## 5 Troubleshooting – Safe Mode

From Safe mode, you can:

- **Restore factory defaults** – When you cannot access the system (for example, you have forgotten the Username or Password), you can restore factory defaults from Safe mode (see Section 3.10.3 on page 36 on 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 Safe mode, using a special update file.

### 5.1 Entering Safe Mode

The following flowchart provides an overview on how to enter Safe mode.

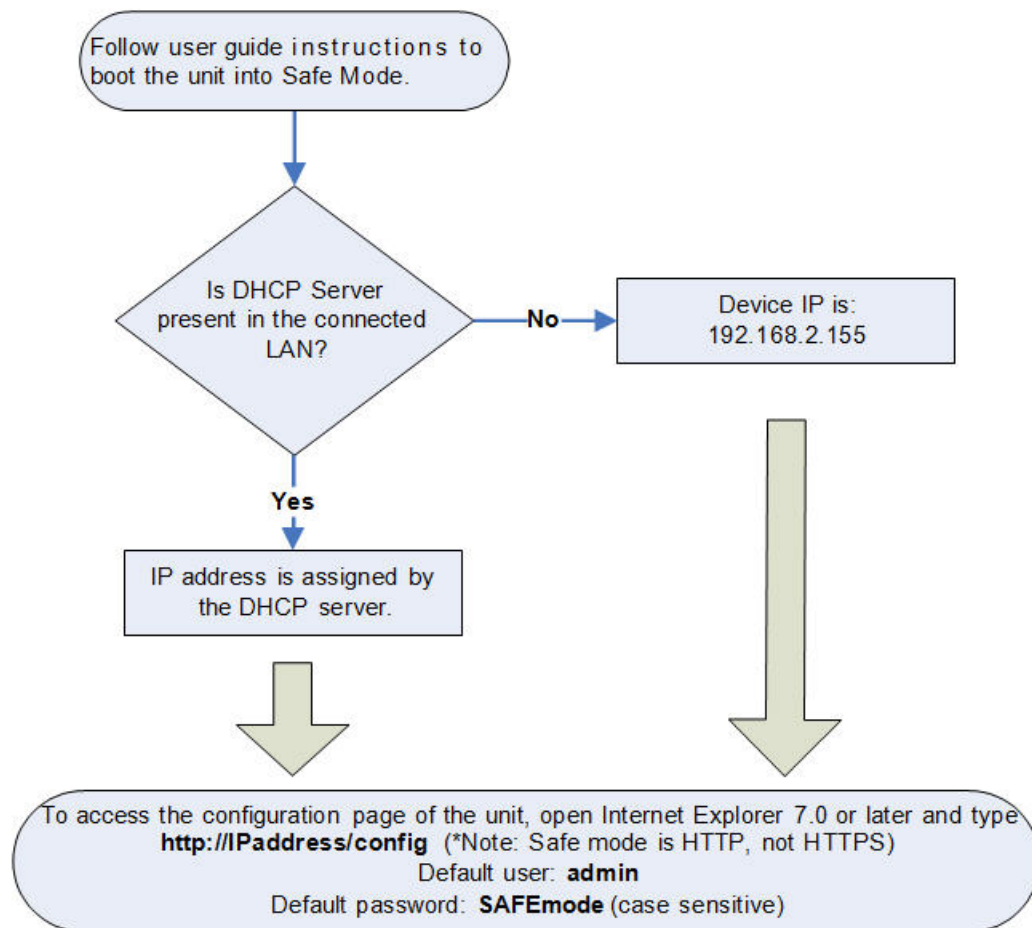


Figure 47 – Safe Mode Procedure

## Troubleshooting – Safe Mode

---

### Entering Safe Mode

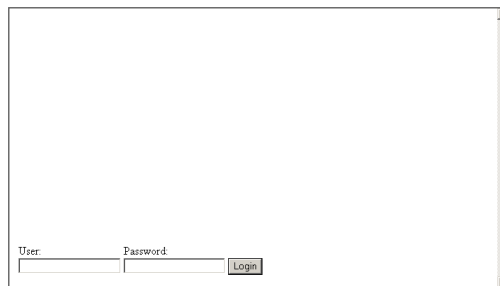
➔ **To enter Safe mode:**

1. While powering up IP Control, press and hold down the **Go Local** button on the back panel of the unit for three to four seconds.

The device boots up in Safe mode.

2. Wait until the unit finishes booting (one to two minutes).
3. Determine the IP address of the IP Control unit. The IP address depends on whether or not there is a DHCP server on the network. If there is, the DHCP server assigns an IP address to the IP Control unit. If there is no DHCP server, the unit boots with the static IP address 192.168.2.155.
4. Open Internet Explorer and type into the Address box: <http://IP address/config>. (Do not start the address with **https**.)

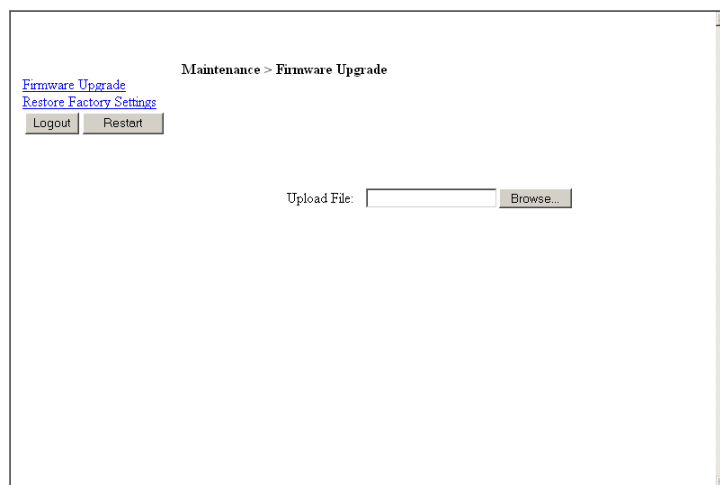
The Login page appears.



*Figure 48 – Login Page*

5. In **User**, type username **admin**, and in **Password**, type **SAFEmode** (case sensitive). (This username and password works only in Safe mode.)

A menu appears.



*Figure 49 – Safe Mode Menu*

## 5.2 Restoring Factory Defaults

You can restore all IP Control settings to their default values.

➔ **To restore factory defaults:**

1. In the Safe Mode menu (see Figure 49), click **Restore Factory Settings**.

A warning appears.

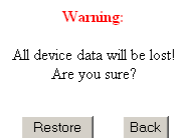


Figure 50 – Warning

2. Click **Restore**.

An additional warning appears.



Figure 51 – Additional Warning

3. Click **OK**.

The factory defaults are restored. When the process finishes, the following figure appears.

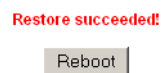


Figure 52 – Reboot

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

## 5.3 Restoring the Device Firmware

To receive the Upgrade firmware required to restore the device firmware, contact Minicom Technical Support [support@minicom.com](mailto:support@minicom.com). Save the Upgrade firmware on the hard disk of a computer connected to the network.

## Troubleshooting – Safe Mode

---

### Restoring the Device Firmware

➔ **To restore device firmware:**

1. In the Safe Mode menu (see Figure 49), click **Firmware Upgrade**.

A warning appears.

2. Locate the Upgrade firmware, click **Install**, then click **Start Upgrade**.

The firmware upgrades. When the process finishes, the following figure appears.

Upgrade succeeded

Reboot

*Figure 53 – Update Succeeded*

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

## 6 Technical Specifications

Specification	Description
Operating systems	<p><b>Target server</b> – DOS, Windows, Novell, Linux, or SUN Solaris for PC</p> <p><b>Client computer</b> – Windows 2000 or later with Internet Explorer 7.0 / Firefox 3.0 and later; Linux x86 with Firefox 3.0 and later</p>
Resolution	<p><b>Target server</b> – Up to 1600 x 1200 @ 85 Hz</p> <p><b>Client computer</b> – Recommended resolution should be higher than ontarget server</p>
Video and mouse synchronization	Both auto and manual modes
Security	SSL, high grade 256-bit AES encryption
Connections	<p><b>Ethernet</b> – RJ45 – 10/100 Mbit/sec autosensing</p> <p><b>Serial</b> – RJ45</p> <p><b>Local KVM connection</b> – Screen HDD15; Keyboard/Mouse – MiniDIN6</p> <p><b>Computer / switch connection</b> – HDD15, KVM cable 1.8 m., Monitor HDD15, Keyboard/Mouse – MiniDIN6</p>
Weight	0.2 kg / 0.45 lb
Dimensions (H x D x W)	3 x 10 x 8 cm / 1.2 x 3.9 x 3.1 in
Power adapter	3.3 VDC, 2 A.
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

## 7 Video Resolution and Refresh Rates

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

