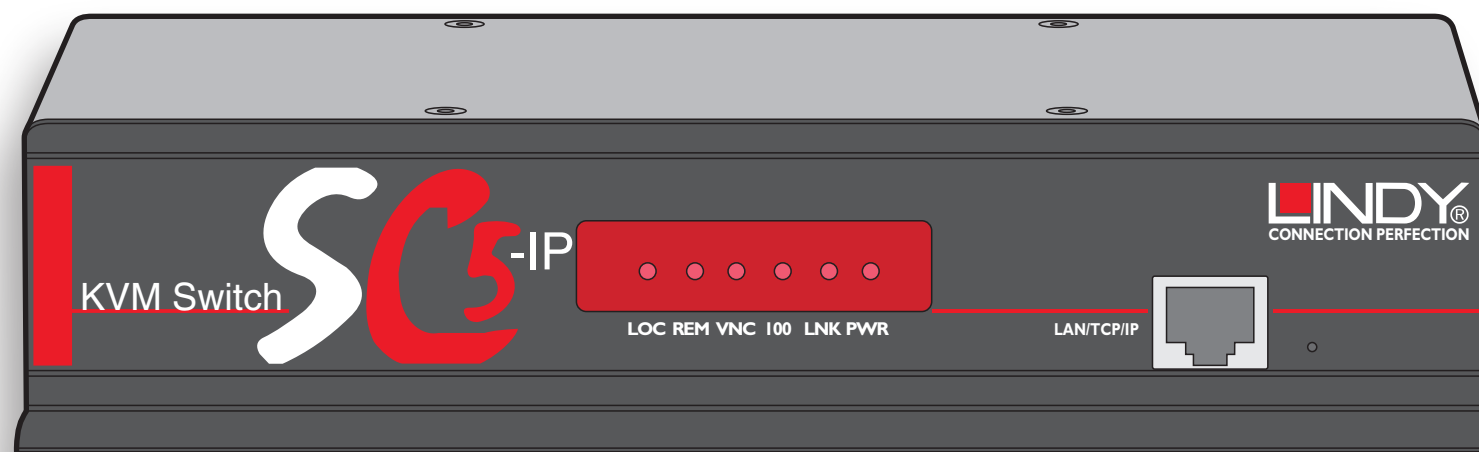




SC5-IP

User Guide



[CONTENTS](#)

Contents

Introduction

SC5-IP features - front and rear	5
What's in the box	6
What you may additionally need	6

Installation

Mounting	7
Connections	8
Local user	9
Global user (IP network port)	10
Computer system (via CAM)	11
Power in connection	12
Cascading multiple units	13
Connecting units in cascade	14
Addressing computers in a cascade	15
Using cascaded computers	15
Multiple video head connections	16
Remote switching control	17

Configuration

Overall initial configuration	18
Initial configuration	19
Main menu	20
General security and configuration steps	21
Registering users and host computers	21
What to do if the ADMIN password has been forgotten	22
Clearing IP access control	23
Full configuration by global user	24
Encryption settings	25
Networking issues	26
Upgrading SC5-IP models	30
Recovering from a failed upgrade	30



INSTALLATION



CONFIGURATION

OPERATION

FURTHER
INFORMATION

INDEX

Operation

The front panel indicators	31
Accessing the SC5-IP	31
Local user access	32
Selecting a computer	32
Logging in and out	34
The confirmation box	35
The reminder banner	35
User preferences and functions	36
Orange dot indicators in the Select Host menu	36
Global user access	37
Global user access via VNC viewer	38
Global user access via web browser	39
Using the viewer window	40
The menu bar	40
When using the viewer window	40
Mouse pointers	41
Host selection	41
Configure	41
Auto calibrate 	42
Re-synchronise mouse 	42
Access mode - shared/private	42
Controls	43
If you need to enter a port number	47
Viewer encryption settings	47
Supported web browsers	47

Further information

Troubleshooting	48
Getting assistance	48
Appendix 1 – Local setup menus	49
Functions	50
User Preferences	51
Global Preferences	52
Setup Options	53
Configuration	54
Unit Configuration	55
Network Configuration	56
Serial Configuration	57
Reset Configuration	58
Appendix 2 - Configuration pages via viewer	59
User accounts	60
Unit configuration	61
Advanced unit configuration	62
Time & date configuration	63
Network configuration	64
Setting IP access control	65
Serial port configuration	66
Host configuration	67
Logging and status	68
LDAP configuration	69



INSTALLATION

CONFIGURATION

OPERATION

FURTHER
INFORMATION

INDEX

Appendix 3 - VNC viewer connection options	70
Colour/Encoding	70
Inputs	71
Misc	72
Scaling	73
Identities.....	74
Load / Save	74
Appendix 4 - VNC viewer window options	75
Appendix 5 - Browser viewer options	76
Encoding and colour level.....	76
Inputs.....	76
Security	76
Misc.....	76
Appendix 6 – Addresses, masks and ports	77
IP addresses	77
Net masks	77
Net masks - the binary explanation	78
Calculating the mask for IP access control.....	79
Ports.....	80
Security issues with ports.....	80

Appendix 7 – Cable and connector specifications	81
Multi-head synchronisation cable.....	81
Appendix 8 – Hotkey sequence codes.....	82
Permissible key presses	82
Creating macro sequences	82
Appendix 9 – Supported video modes	83
Warranty	84
Safety information	84
WEEE (Waste of Electrical and Electronic Equipment), Recycling of Electronic Products	85
End user licence agreement.....	86
Radio Frequency Energy.....	87

Index



INSTALLATION

CONFIGURATION

OPERATION

FURTHER
INFORMATION

INDEX

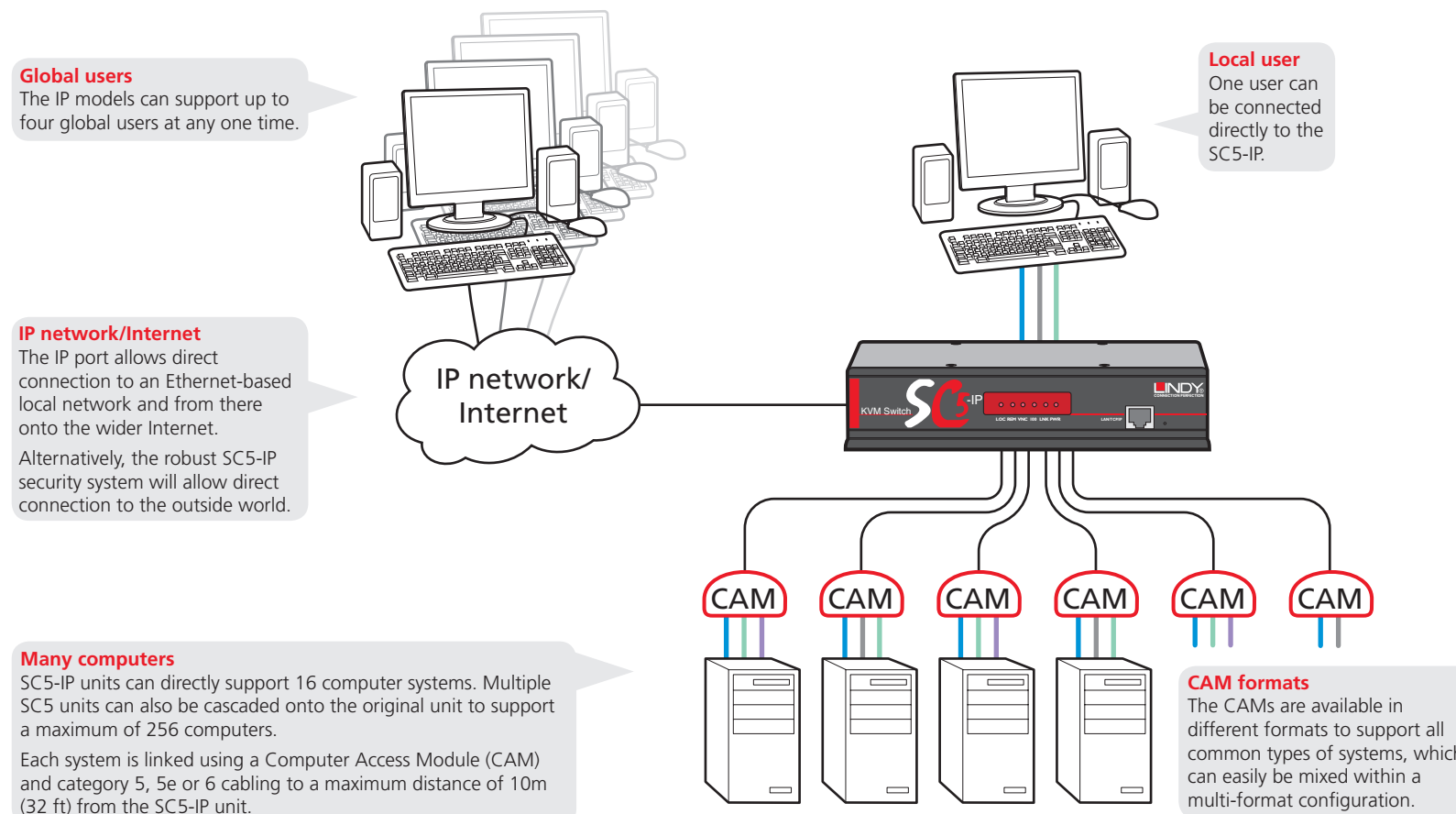
Introduction



Thank you for choosing the SC5-IP from LINDY. This compact unit has been created to allow a single operator to take full control of many computer systems. Like the other models within the highly successful SC5 family, this unit takes full advantage of category 5, 5e or 6 structured cabling to provide flexible installation and configuration. Every connected computer is linked by up to ten metres of standard CATx cable and one of five

types of CAM (Computer Access Module) according to the port arrangements on each computer. The SC5-IP supports up to sixteen computers directly. This number, however, can be increased at any time thanks to the ability to connect SC5 units in cascade to provide a much larger network of controlled computers. Full enterprise level security is fitted as standard to restrict access to authorised personnel.

In addition to the local user console, the SC5-IP units provide true global control for the multiple host systems. Up to four global users can share access to a computer from anywhere via an IP network/internet connection using a Real VNC client application. Each SC5-IP is even able to provide the VNC application to each global user, either as a standalone application or as a Java applet within a standard internet browser.



INSTALLATION

CONFIGURATION

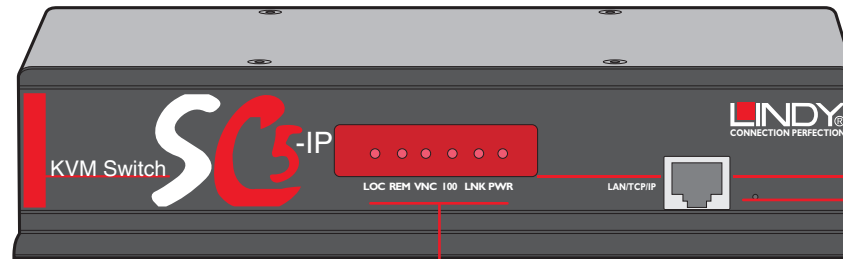
OPERATION

FURTHER INFORMATION

INDEX

SC5-IP features - front and rear

The SC5-IP units pack a great deal of functionality into a compact space. Both models occupy half of a single 1U rack space and provide most of their connectors at the rear face. The smart front face features the remote user link port and the operation indicators.



IP network port

The port by which global users are linked to the SC5-IP unit. This intelligent Ethernet port can automatically sense whether it is attached to a 10Mb or 100Mb network.

Indicators

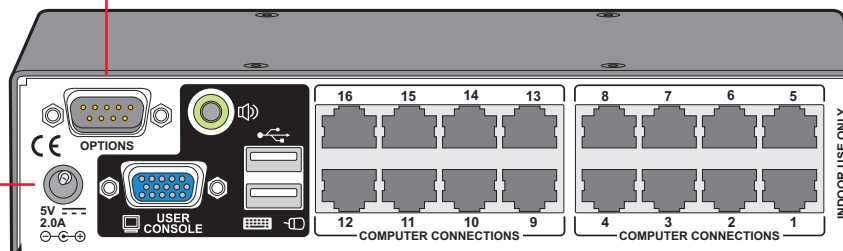
These six indicators clearly show the key aspects of operation:

- **LOC** Keyboard or mouse data are being received from the local console.
- **REM** Keyboard or mouse data are being received from the remote console.
- **VNC** Indicates that a global user is connected and active.
- **100** Indicates the Ethernet network speed (10/100Mbps).
- **LNK** Indicates that a network link is present.
- **PWR** Indicates that power is present.

Options port

This RS232 serial port can separately support the following functions:

- Remote control switching - commands can be received that will change the channel, as necessary.
- Synchronisation - allows the actions of two or more SC5-IP switches to be synchronised so that multiple computers/video screens can be switched and accessed.



Power input
The power supply connects here.

Local user port

Connect a USB keyboard and mouse, plus a video monitor to these connectors. These allow you to perform the initial configuration of the SC5-IP. Additionally, you can use these to locally control the connected computer(s).

Computer ports

Each computer connects to one of these ports via standard category 5, 5e or 6 cabling. At the other end of the cabling a CAM (Computer Access Module) is used to provide the necessary keyboard, video and mouse connections.



INSTALLATION

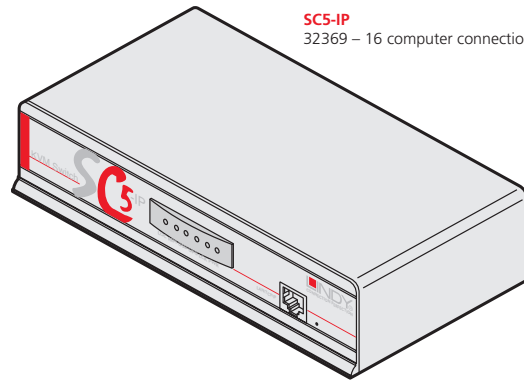
CONFIGURATION

OPERATION

FURTHER INFORMATION

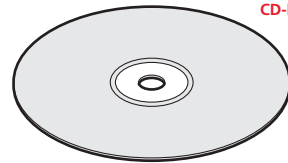
INDEX

What's in the box

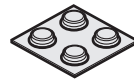


SCS-IP

32369 – 16 computer connections, 1 local console connection, 1 global user (network) connection

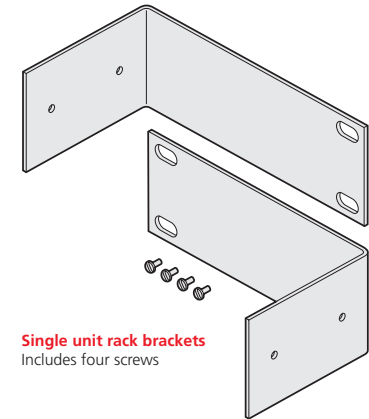
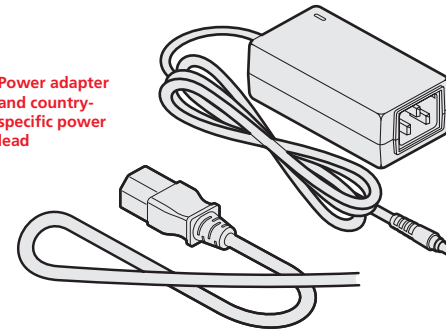


CD-ROM



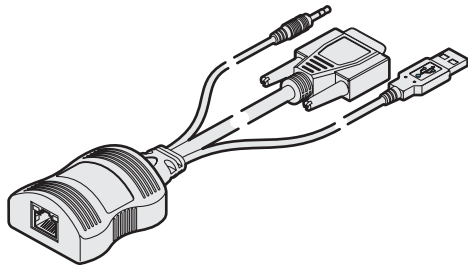
Four self-adhesive rubber feet

Power adapter and country-specific power lead



Single unit rack brackets
Includes four screws

What you may additionally need



Computer Access Modules

One required per connected computer. There are five different formats, depending on the required computer connections:

PS/2-style

Connectors: Analog video, PS/2-style keyboard and PS/2-style mouse.
Part number: 39351

PS/2-style with audio

Connectors: Analog video, PS/2-style keyboard, PS/2-style mouse and 3.5mm audio jack.
Part number: 39353

USB

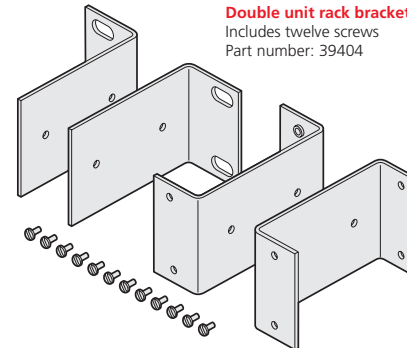
Connectors: Analog video and USB keyboard/mouse.
Part number: 39352

USB with audio

Connectors: Analog video, USB keyboard/mouse and 3.5mm audio jack.
Part number: 39354

Sun with audio

Connectors: Analog video, Sun keyboard/mouse and 3.5mm audio jack.
Part number: 39355



Double unit rack brackets

Includes twelve screws
Part number: 39404



INSTALLATION

CONFIGURATION

OPERATION

FURTHER INFORMATION

INDEX

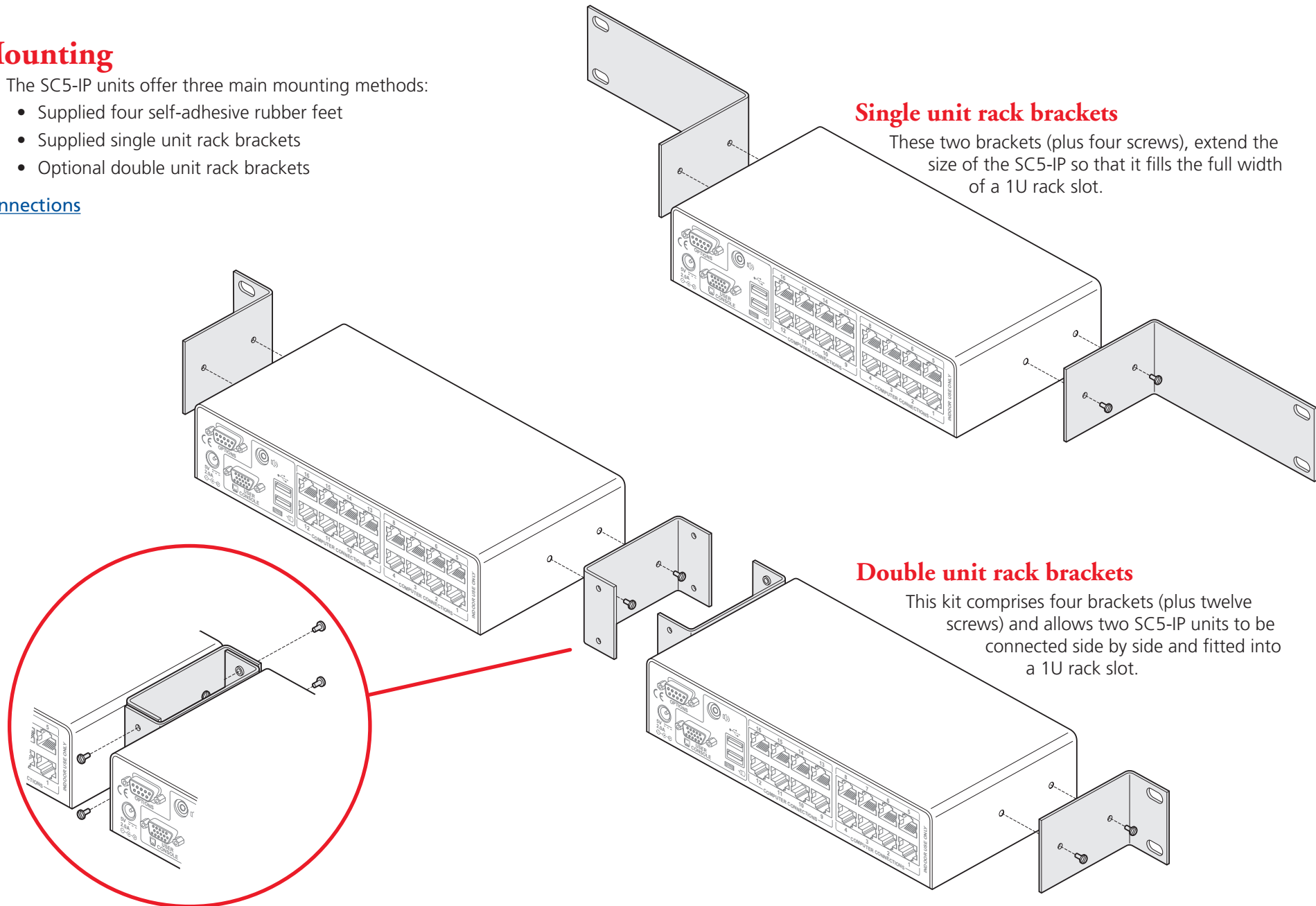
Installation

Mounting

The SC5-IP units offer three main mounting methods:

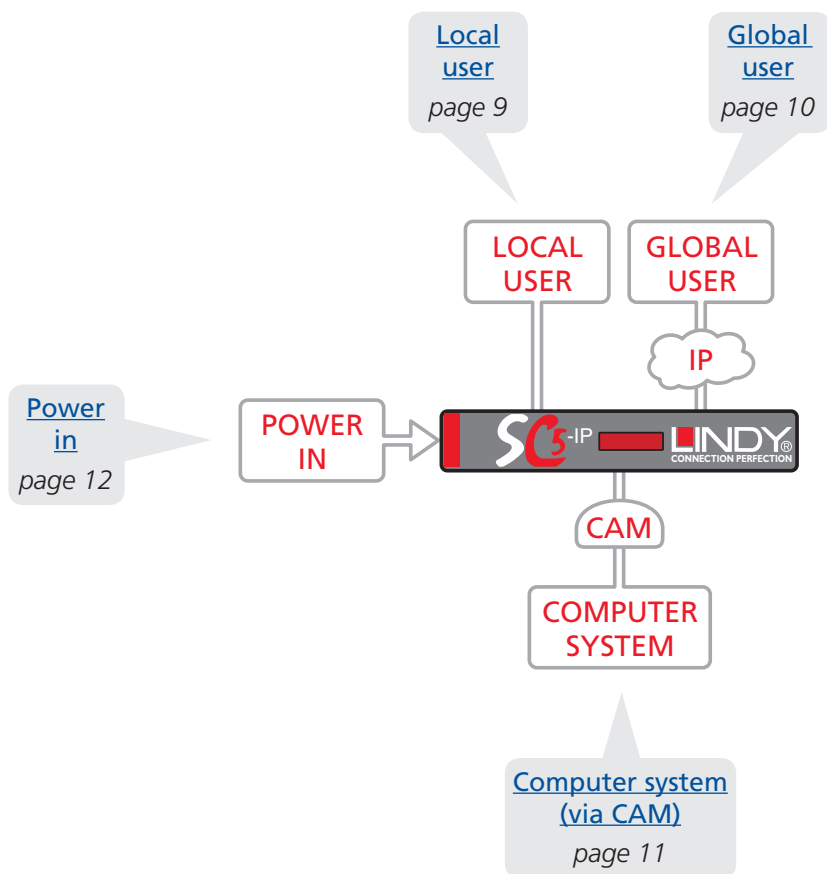
- Supplied four self-adhesive rubber feet
- Supplied single unit rack brackets
- Optional double unit rack brackets

Connections

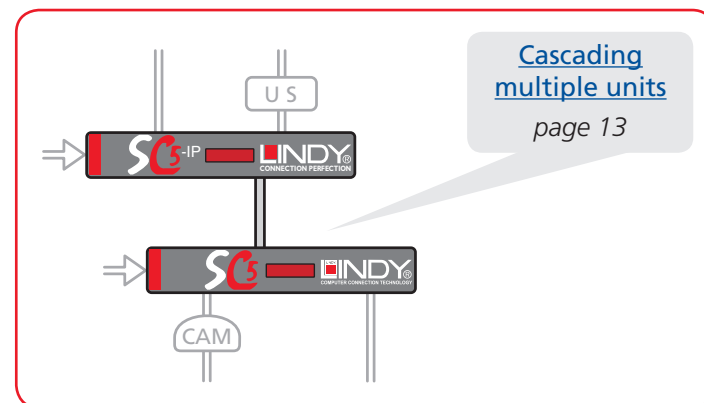
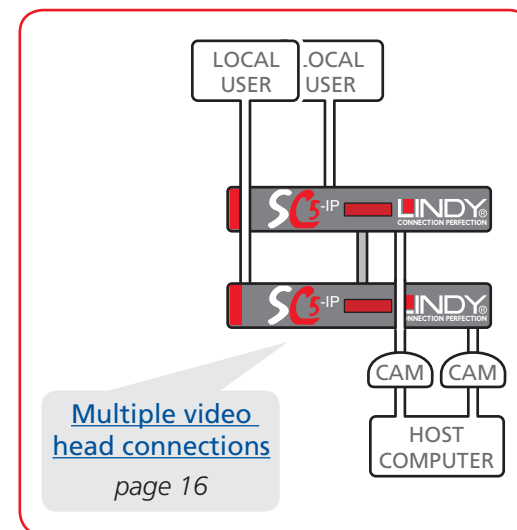


Connections

The SC5-IP provides a great deal of flexibility in its configurations. This chapter details the various connections that can be made to achieve the required installation.



Connections do not need to be carried out in the order given within this guide, however, where possible connect the *power in* as a final step.



INSTALLATION

CONFIGURATION

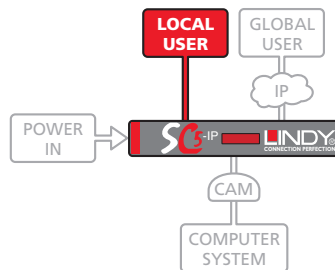
OPERATION

FURTHER INFORMATION

INDEX

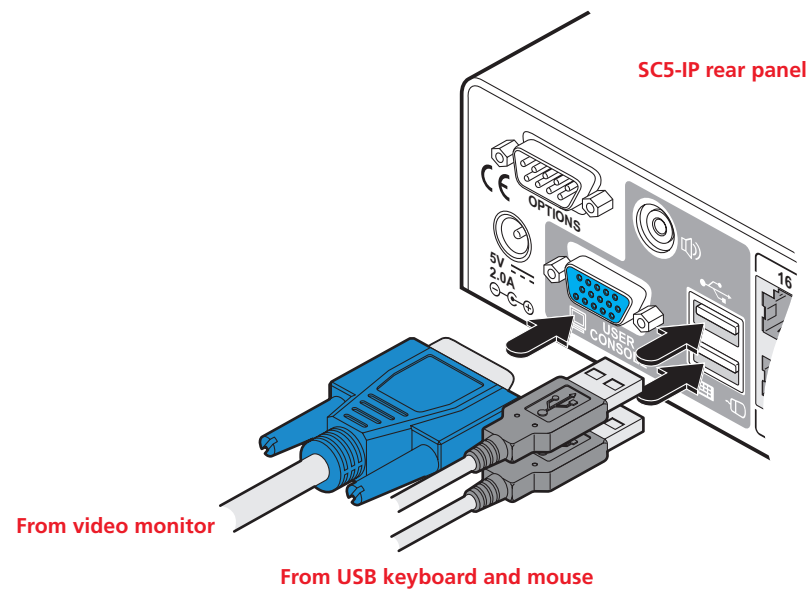
Local user

A locally connected video monitor, keyboard (and mouse) are required during the initial configuration. These are also useful during normal use to allow quick local control of any connected computer systems. The SC5-IP unit directly supports USB style keyboards and mice.



To connect the local user port

- 1 Position a suitable video monitor, keyboard and mouse in the vicinity of the SC5-IP unit such that their cables will easily reach.
- 2 Attach the video monitor, keyboard and mouse connectors to the sockets, collectively labelled as USER CONSOLE, at the rear of the SC5-IP unit.



INSTALLATION

CONFIGURATION

OPERATION

FURTHER
INFORMATION

INDEX

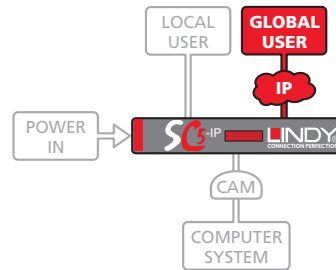
Global user (IP network port)

The SC5-IP models provide an autosensing Ethernet IP port that can operate at 10 or 100Mbps, according to the network speed. The SC5-IP models are designed to reside quite easily at any part of your network:

- They can be placed within the local network, behind any firewall/router connections to the Internet, or
- They can be placed externally to the local network, on a separate sub-network or with an open Internet connection.

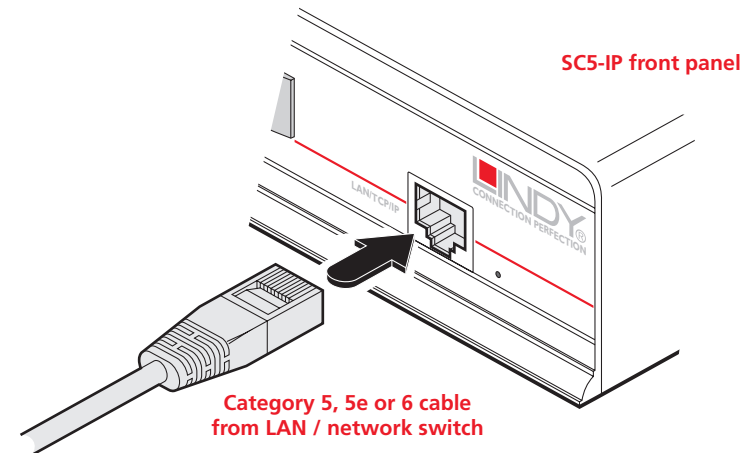
Wherever in the network an SC5-IP is situated, you will need to determine certain configuration issues such as address allocation and/or firewall adjustment to allow correct operation. Please refer to [Networking issues](#) within the Configuration chapter for more details.

IMPORTANT: When an SC5-IP is accessible from the public Internet or dial up connection, you must ensure that sufficient [security measures](#) are employed.



To connect the Global user (IP network) port

- 1 Depending upon where in the network the SC5-IP is being connected, run a category 5, 5e or 6 link cable from the appropriate hub or router to the SC5-IP unit.
- 2 Connect the plug of the link cable into the IP port on the front panel of the SC5-IP unit.



- 3 Configure the network settings as appropriate to the position of the SC5-IP within the network - see [Networking issues](#) for details.



INSTALLATION

CONFIGURATION

OPERATION

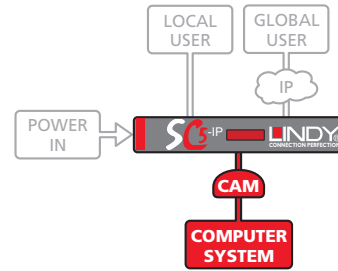
FURTHER INFORMATION

INDEX

Computer system (via CAM)

Each computer system is connected to the SC5-IP unit via a Computer Access Module (CAM) and standard category 5, 5e or 6 cabling. CAMs are available in various formats to suit differing computer system types and their particular connector styles.

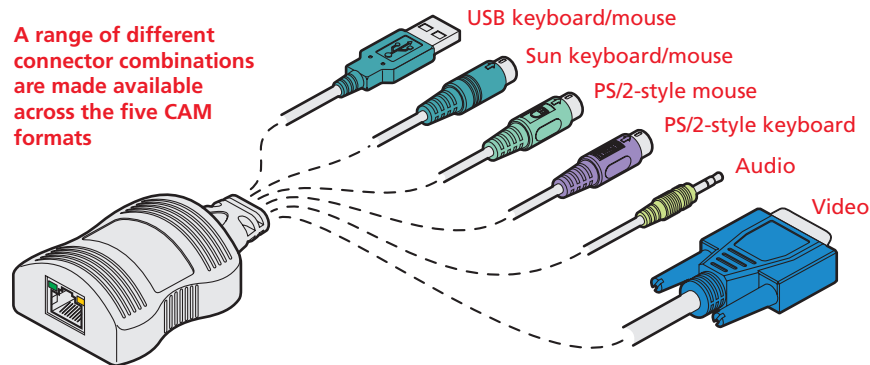
Each CAM uses Keep Alive technology to ensure that the keyboard and mouse inputs to the computer remain active, even when the particular channel is not selected. This action ensures that there are no connection delays or problems as the port is selected.



To connect a computer system

- 1 Ensure that power is disconnected from the SC5-IP unit and the system to be connected.
- 2 Locate the required CAM (there are five types available) and attach its video, keyboard and mouse (PS/2-style, USB or Sun) to the relevant sockets on the computer system.

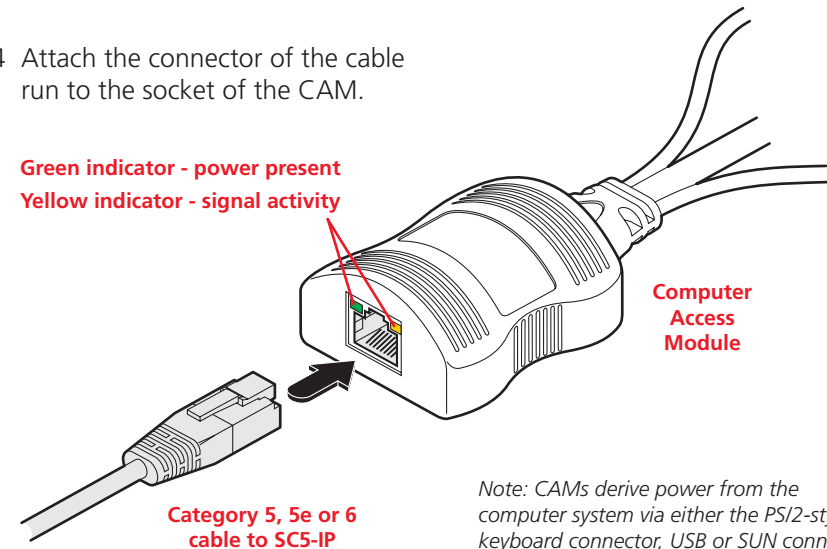
A range of different connector combinations are made available across the five CAM formats



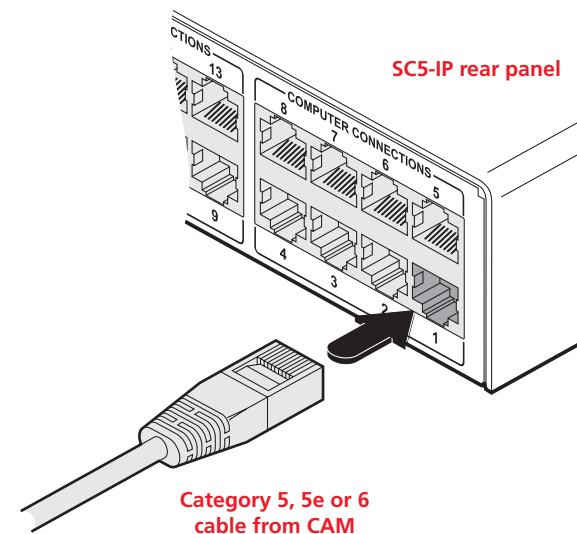
- 3 Lay a suitable length of category 5, 5e or 6 cabling between the computer system and the SC5-IP unit. The maximum length of the cable is 10 m (32 feet).

- 4 Attach the connector of the cable run to the socket of the CAM.

Green indicator - power present
Yellow indicator - signal activity



- 5 At the other end of the cable run, attach the cable connector to one of the sockets labelled COMPUTER CONNECTIONS on the rear panel of the SC5-IP unit.



INSTALLATION

CONFIGURATION

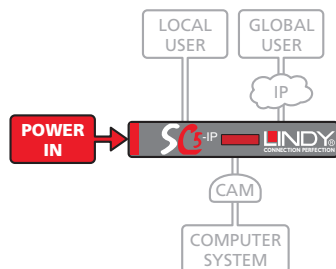
OPERATION

FURTHER INFORMATION

INDEX

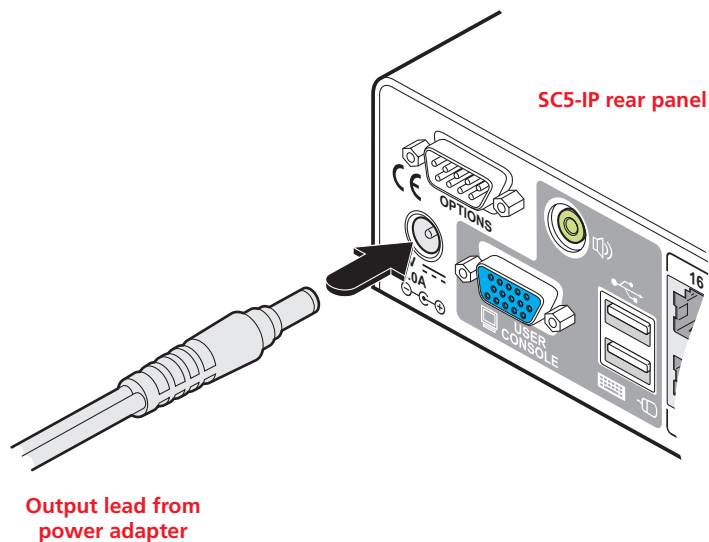
Power in connection

The SC5-IP unit is supplied with a standard 5V power adapter. There is no on/off switch on the unit, so operation begins as soon as a power adapter is connected.

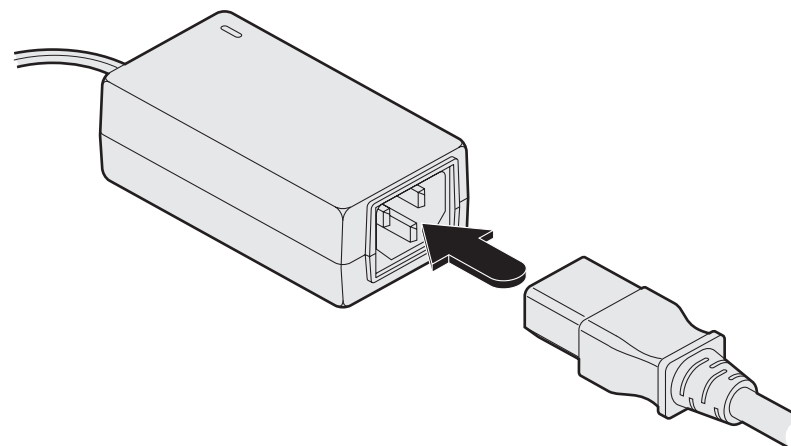


To connect the power supply

- 1 Attach the output lead from the power adapter to the 5V socket on the rear panel of the SC5-IP.



- 2 Connect the IEC connector of the supplied country-specific power lead to the socket of the power adapter.



- 3 Connect the power lead to a nearby main supply socket.

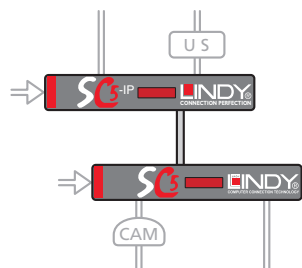
Note: Both the SC5-IP and its power supply generate heat when in operation and will become warm to the touch. Do not enclose them or place them in locations where air cannot circulate to cool the equipment. Do not operate the equipment in ambient temperatures exceeding 40 degrees Centigrade. Do not place the products in contact with equipment whose surface temperature exceeds 40 degrees Centigrade.

Cascading multiple units

The SC5-IP supports up to sixteen *directly* connected computer systems, however, this is by no means the limit. Instead of connecting computers to every output port, you can instead link SC5 units (not IP variants). Thus, each output of the original SC5-IP unit can link through to many more computers connected to the secondary SC5 units.

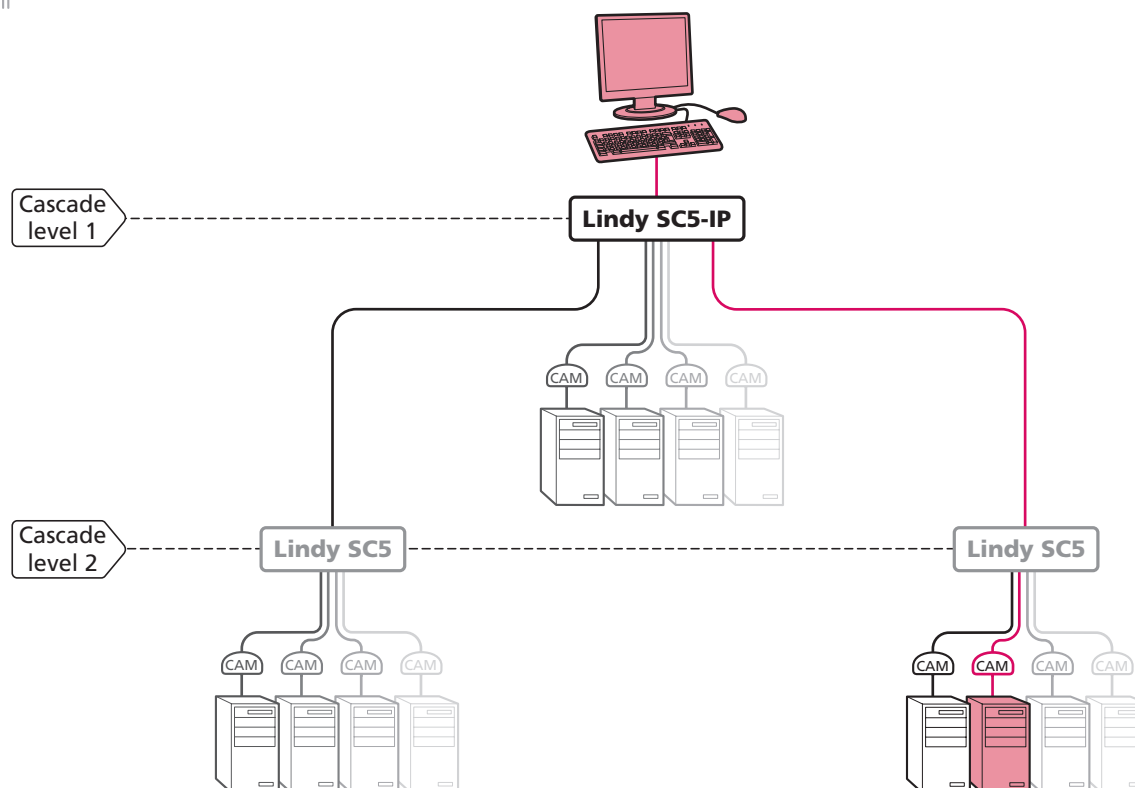
The combination of SC5 units can be arranged two levels deep forming a tree, or *cascade* arrangement, with computer systems situated at either level within that cascade tree.

Note: It is not possible to cascade two SC5-IP units together because they do not have a Remote User Port on their front panels. The lower units must always be the non-IP SC5 variants.



The cascade tree

The diagram shows how an SC5-IP unit and multiple SC5 units can be cascaded to two levels. Computer systems can be connected at any level. The local or global users can access computer systems situated anywhere within the cascade tree.



See also

- [Connecting units in cascade](#)
- [Addressing computers in a cascade](#)



INSTALLATION

CONFIGURATION

OPERATION

FURTHER INFORMATION

INDEX

Connecting units in cascade

The method for cascading SC5-IP and SC5 units is straightforward and requires no hardware settings or lengthy configuration process.

The method of linking units is the same regardless of the cascade level, or number of devices attached. Put simply:

- A single cascade link is made by connecting a **COMPUTER CONNECTIONS** socket of the **SC5-IP** unit to the **REMOTE USER PORT** socket of the **SC5** unit below it.

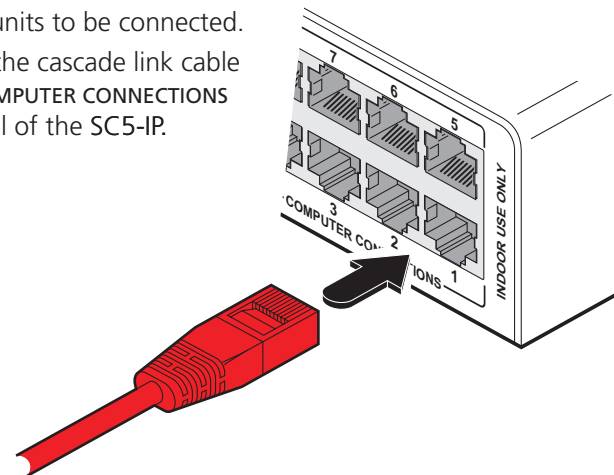
Please consider the following when making cascade connections between units.

Tips for successful cascading

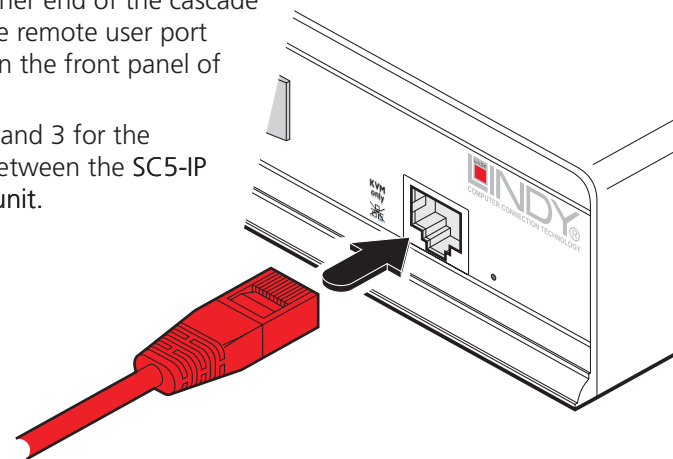
- The maximum number of levels for a cascade is two.
- For each cascade link, use a standard category 5, 5e or 6 twisted-pair cable, terminated at each end with an RJ45 connector. There must be no crossover connections within the cable. The cascade link cables can be up to 10m (32 feet) in length providing that the total length from the SC5-IP or SC5 to any CAM also does not exceed 10m.
- The procedure given opposite may be carried out in any order but for clarity the instruction will begin at the SC5-IP unit. The procedure remains the same regardless of exactly which cascade levels are being connected. The basic rule is that each link is made by connecting a **COMPUTER CONNECTIONS** port of the SC5-IP (upper switch) to the **REMOTE USER PORT** (on the front panel) of the SC5.

To connect units in cascade

- 1 Ensure that power is disconnected from the SC5-IP and all other units to be connected.
- 2 Connect one end of the cascade link cable to an appropriate **COMPUTER CONNECTIONS** port on the rear panel of the SC5-IP.



- 3 Connect the other end of the cascade link cable to the remote user port (RJ45 socket) on the front panel of the SC5 unit.
- 4 Repeat steps 2 and 3 for the cascade links between the SC5-IP and each SC5 unit.



Once the units and computers have been connected, you can edit their names to make it much easier to locate them. See the [To create a new host entry](#) section in the 'Host configuration' page of Appendix 2 for more details.

See also

- [Addressing computers in a cascade](#)



INSTALLATION

CONFIGURATION

OPERATION

FURTHER INFORMATION

INDEX

Addressing computers in a cascade

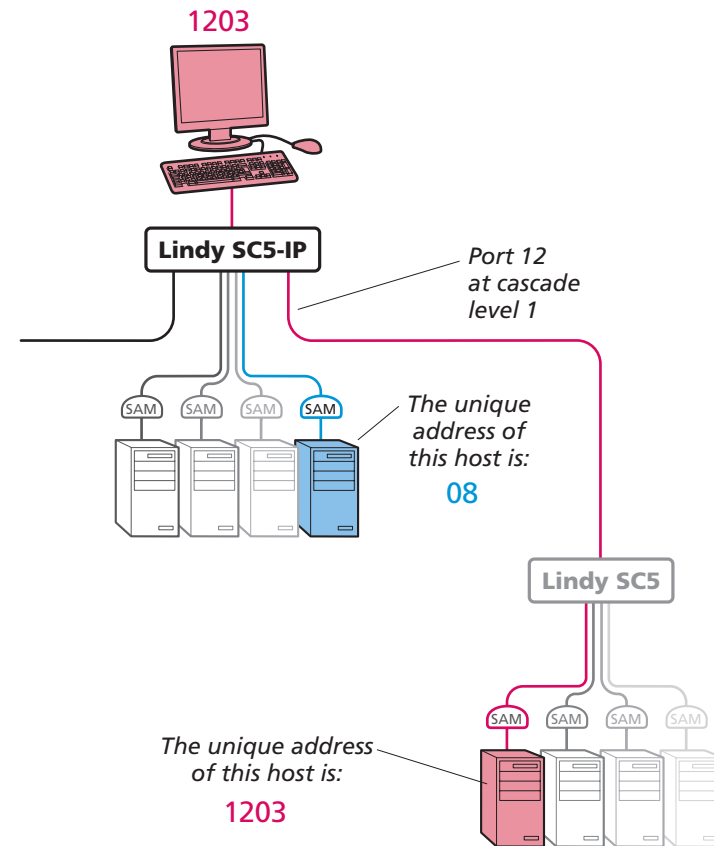
Computer systems connected within a cascade arrangement are addressed using up to four digits, two for each cascade level. The pairs of digits specify which of the **COMPUTER CONNECTIONS** ports on each of the SC5 units must be enabled to reach a specific computer. In the diagram given here, a portion of the previous cascade diagram indicates how the routes to two particular computers are formed and addressed.

Each cascade level requires two digits, hence the computer marked in red requires a longer address (1203) as it is situated at cascade level 2, compared to the blue computer at the top level with its two digit port number.

The first time that you make a connection between an SC5-IP and an SC5, the master unit will detect this and ask (via the on screen menu) if you want to automatically add computers. If you choose 'Yes' then the ports on the cascade will be automatically added to the on screen menu.

Using cascaded computers

In use, cascaded computers can be accessed using exactly the same methods as for those connected directly to the SC5-IP. However, by far the easiest way is to use the on screen menu. This is because it displays the computer names and does not require any knowledge of port addresses. See either [Selecting a computer](#) (for local user access) or [Host selection](#) (for global user access) for more details.



INSTALLATION

CONFIGURATION

OPERATION

FURTHER INFORMATION

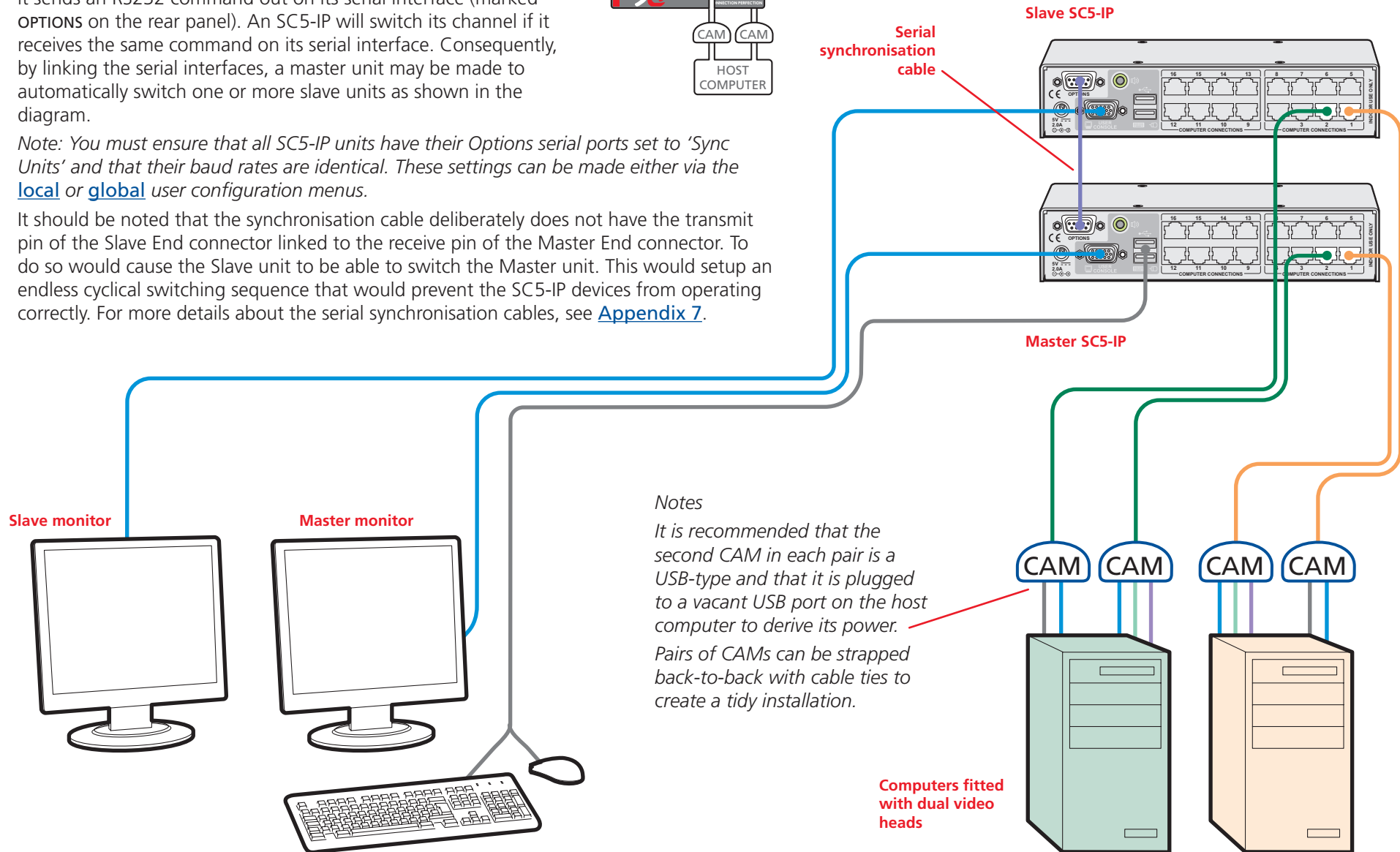
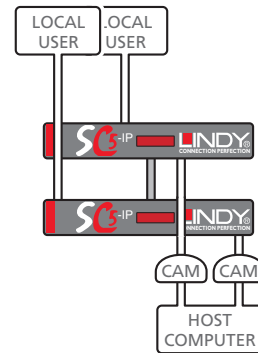
INDEX

Multiple video head connections

Two or more SC5-IP units can be connected together so that they operate in a synchronised manner. Synchronised operation is useful for applications that require multiple video signals to be switched together. This type of operation is usually required where each computer is fitted with multiple video cards or video cards with multiple video heads. Whenever an SC5-IP channel is switched, it sends an RS232 command out on its serial interface (marked **OPTIONS** on the rear panel). An SC5-IP will switch its channel if it receives the same command on its serial interface. Consequently, by linking the serial interfaces, a master unit may be made to automatically switch one or more slave units as shown in the diagram.

Note: You must ensure that all SC5-IP units have their Options serial ports set to 'Sync Units' and that their baud rates are identical. These settings can be made either via the [local](#) or [global](#) user configuration menus.

It should be noted that the synchronisation cable deliberately does not have the transmit pin of the Slave End connector linked to the receive pin of the Master End connector. To do so would cause the Slave unit to be able to switch the Master unit. This would setup an endless cyclical switching sequence that would prevent the SC5-IP devices from operating correctly. For more details about the serial synchronisation cables, see [Appendix 7](#).



Notes

It is recommended that the second CAM in each pair is a USB-type and that it is plugged to a vacant USB port on the host computer to derive its power. Pairs of CAMs can be strapped back-to-back with cable ties to create a tidy installation.

Remote switching control

The port switching functions of the SC5-IP units can be remotely controlled by an RS232 link to the **OPTIONS** port on the rear panel.

The sending device must use the following RS232 communication settings:

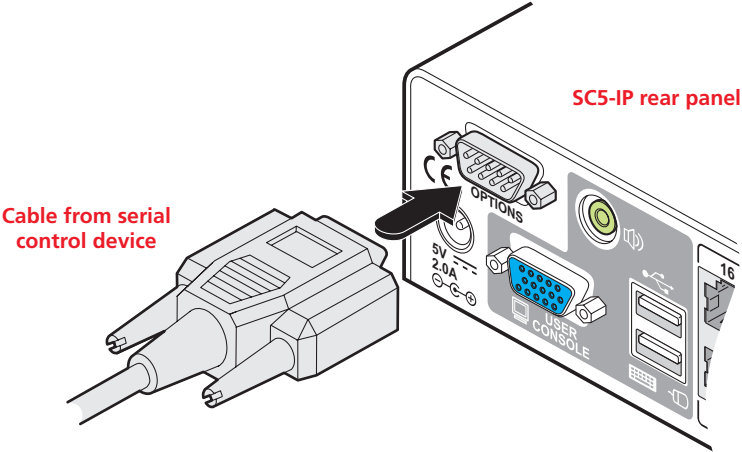
Baud rate: 19200 bps
Data bits: 8
Parity: None
Stop bits: 1

No handshaking is implemented, however, valid command characters will be echoed back to the sending device.

Note: You must ensure that the SC5-IP unit has its Options serial ports set to 'Sync Units'. This setting (together with the baud rate selection) can be made either via the [local](#) or [global](#) user configuration menus.

The value of the byte received via the serial link determines which computer port should be linked through to the user port. The table given here summarises the valid control codes:

Host computer port/channel																
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	0 (video off)
10	11	12	13	14	15	16	17	18	19	1A	1B	1C	1D	1E	1F	71



INSTALLATION

CONFIGURATION

OPERATION

FURTHER INFORMATION

INDEX

Configuration

Almost all configuration and operational aspects of the SC5-IP units are controlled via [on-screen menu](#) displays.

Overall initial configuration

When setting up a new installation, the following stages are recommended:

1 [Enable the general 'Security' option.](#)

With security disabled (default setting), a local or remote user attached to the SC5-IP will have full and unrestricted access to all computers and all SC5-IP settings. In larger installations, you are strongly recommended to enable security and set up individual user accounts with access privileges.

2 [Create an ADMIN \(administration\) password.](#)

All SC5-IP units have a fixed user account that cannot be deleted or renamed, called ADMIN. This user account is the only one that is able to make important system changes. If you intend to use security, then it is important to allocate a password to the ADMIN account.

3 [Create user accounts and allocate access rights.](#)

Use the ADMIN account to add user profiles, passwords and access rights for each of the system users.

4 [Provide names for computers.](#)

When numerous computers are attached, you are strongly advised to provide names for each, to assist with recognition.

5 Configure the required '[Setup Options](#)' and '[Global Preferences](#)'

Use the ADMIN account to determine key SC5-IP settings and timing characteristics.



INSTALLATION

CONFIGURATION

OPERATION

FURTHER
INFORMATION

INDEX

Initial configuration

The SC5-IP unit provides an initial configuration sequence to assist you to make the necessary settings.

When the SC5-IP is switched on for the first time, you should see the unit configuration screen, as shown here ➡

IMPORTANT: Complete the initial IP configuration and invoke security measures BEFORE the unit is connected to an open IP network.

If the SC5-IP unit has been previously configured, it will display either the Login dialog or the Select Host screen, as shown here ↓

SC5-IP Login

Username:

Password:



SC5-IP Select Host

Computer	Port	
Computer 01	01	●
Computer 02	02	●
Computer 03	03	●
Computer 04	04	●
Computer 05	05	●
Computer 06	06	●
Computer 07	07	●
Computer 08	08	●

User: Status:

admin Shared

F1 - more menus F3 - Find

ESC - Quit F4 - Logout



SC5-IP Main Menu

Functions

User Preferences

Global Preferences

Setup Options

Configuration

Back

If the Login is shown, enter your 'admin' Username and Password - or press twice if none have yet been defined.

From the Select Host screen, press to display the Main Menu. See [Main Menu](#) for more details.

Within the Main Menu, use the and keys to highlight an option, then press to select.

The Configuration option provides access to separate Unit, Network and Serial Configuration screens that are similar in function to the first three setup screens shown on the right.

1

SC5-IP Unit Config

Hardware SC5-IP 64M+64M

Firmware 1.00

Keybd Layout

Admin Passwd

Unit Name

Time

Date

Encryption

Screen 1 of 5

Next

Admin password

Enter a password of at least six characters that has a mix of letters and numerals. The background colour provides an indication of password suitability and is initially red to indicate that the password is not sufficient. When a password with reasonable strength has been entered it will change to green.

Time and Date

Set these correctly as all entries in the activity log are time stamped using them.

Encryption

See [Encryption settings](#) for a description of the issues and the settings.

2

SC5-IP Network Config

MAC Address 66:CB:23:00:00:22

Use DHCP

IP Address 192.168.1.22

Net Mask 255.255.255.0

Gateway

UNC Port 5900

HTTP Port 80

Screen 2 of 5

Next

Use DHCP/IP address/Net Mask/Gateway

You need to either set the DHCP option to 'Yes' or manually enter a valid IP address, Net mask and Gateway. See [Networking issues](#) for more details.

VNC and HTTP ports

These should remain set to 5900 and 80, respectively, unless they clash with an existing setup within the network. See [Networking issues](#) for more details.

3

SC5-IP Serial Config

Options Port

Options Baud

Screen 3 of 5

Next

Option port (serial) details

These two items control the use of the OPTIONS port on the rear panel of the unit. The port can be used to synchronise the operation of two separate SC5-IP units.

If neither of these features are required, then you do not need to change anything on this screen.

4

SC5-IP Secure Keys

Random data is required to generate encryption keys for secure UNC access. Please press keys until the bar becomes full.

-

Screen 4 of 5

Secure keys generation

With every mouse move and keypress, the single dash will move across the screen (unless the same key is pressed repeatedly). Periodically, a new star character will be added to the bar as the random data are accepted as part of the new encryption key. When the bar is full, the final encryption keys for your SC5-IP will be created – this process takes roughly 30 to 40 seconds. Once the secure keys have been calculated the SC5-IP will show either the Login dialog or Select Host screen.

Note: Screen 5 of 5 is displayed while the secure keys are being generated.



INSTALLATION

CONFIGURATION

OPERATION

FURTHER INFORMATION

INDEX

Main menu

The main menu allows you to determine many aspects of the SC5-IP capabilities. From here you can:

- Provide names for all connected computers to allow quick recognition,
- Set individual and global settings for users,
- Run various functions, such as mouse restore operation,
- Configure unit, network and serial port settings.

To access the main menu

- 1 If the select host menu is not already displayed, press and hold **Ctrl** **Alt** and then press **M** using a keyboard attached to a SC5-IP user port.

The select host menu will be displayed:

SC5-IP Select Host		
Computer	Port	
Computer 01	01	●
Computer 02	02	●
Computer 03	03	●
Computer 04	04	●
Computer 05	05	●
Computer 06	06	●
Computer 07	07	●
Computer 08	08	●
User	Status	
admin	Shared	
F1 - more menus	F3 - Find	
ESC - Quit	F4 - Logout	

Default names for each computer port

Availability of each computer:
Green - accessible
Red - inaccessible
Orange - an inconsistency related to a cascade linked host has been detected - [More !+!](#)

Port numbers

Connection status

Your Login name

Assistance for keypress options

- 2 Press **F1** to display the main menu:

SC5-IP Main Menu	
Functions	
User Preferences	
Global Preferences	
Setup Options	
Configuration	
Back	

- 3 Use the **↓** and **↑** keys to highlight an option, then press **↵** to select.

Hotkeys

Note: **Ctrl** and **Alt** are the standard hotkeys and can be [altered](#) to avoid clashes with other devices or software. If you change the hotkeys, remember to use the new ones in place of **Ctrl** and **Alt** when following the instructions in this guide.

Security

Note: If the security option has been enabled, you will be asked for a valid user name and password before the main menu can be displayed.

SC5-IP Login	
Username :	<input type="text"/>
Password :	<input type="password"/>

IMPORTANT: When supplied, SC5-IP units have their security features disabled, which means that any attached users have access to all connected computers and all SC5-IP settings. You are strongly recommended to [enable the 'Security' feature](#) and set an access password for the ADMIN account.

Menu layout

The various menu options are arranged as shown here →
For a description of each option within the Configuration menus, see [Appendix 1](#) for more details.



Main Menu	Functions	Restore Standard Mouse Restore Intellimouse Access Mode
	User Preferences	Reminder Banner Reminder Colour Screen Saver Confirmation Box
	Global Preferences	Mouse Switching Screen Saver OSD Dwell Time User Timeout
	Setup Options	Security Hotkeys Auto Logout
	Configuration	Unit Configuration Network Configuration Serial Configuration Reset Configuration

General security and configuration steps

To enable general security

- 1 Display the [Main menu](#).
- 2 Highlight 'Setup Options' and press .
- 3 Highlight 'Security' and press  (or click one of the arrow buttons) to select 'Enabled'.
- 4 Now create a new password for the ADMIN user account - see below.

To set an ADMIN password


- 1 Display the [Main menu](#).
- 2 Highlight 'Configuration' and press .
- 3 Highlight 'Unit Configuration' and press .
- 4 Using the cursor keys, move the cursor to the 'Admin Passwd' field.
- 5 Enter an appropriate password for the ADMIN user account with regard to the following:
 - The password can be up to 16 characters long.
 - The password can use letters, numerals and/or certain punctuation marks.
 - The password is case sensitive.

Note: The field background colour will remain red until sufficient characters have been entered to form a reasonably robust password.

- 6 Once the password has been entered, you can navigate away from the menu page and it will be automatically saved.

[What to do if the ADMIN password has been forgotten.](#)

To change the hotkeys

The SC5-IP unit uses  and  as its standard hotkeys. These can be changed if they clash with other software or hardware within the installation.

- 1 Display the [Main menu](#).
- 2 Highlight 'Setup Options' and press .
- 3 Highlight 'Hotkeys' and press  (or click one of the arrow buttons) to select the required hotkey combination. The options are: *Ctrl+Alt*, *Ctrl+Shift*, *Alt+Shift*, *Alt Gr*, *Left+Right Alt*, *Left Ctrl+Alt* or *Right Ctrl+Alt*.

Registering users and host computers

All user and host computer registration is achieved solely via the global (network) connection to the SC5-IP unit. See [Appendix 2 - Configuration pages via viewer](#) for details.



INSTALLATION

CONFIGURATION

OPERATION

FURTHER
INFORMATION

INDEX

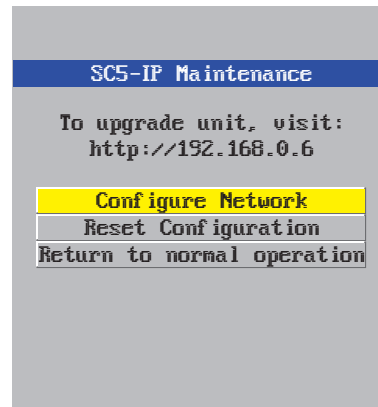
What to do if the ADMIN password has been forgotten

If the ADMIN password becomes mislaid or forgotten, you will not be able to access the SC5-IP to add or edit users and computer names. This situation may be resolved by performing a complete reset to return the SC5-IP.

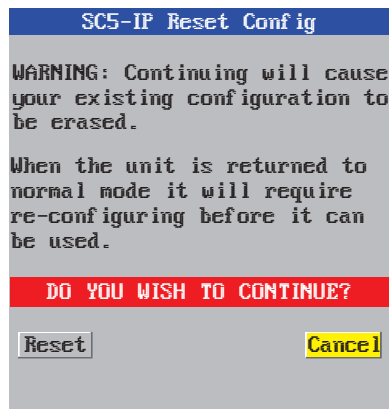
IMPORTANT: A complete reset erases all the user names and computer names that you have setup.

To clear a password (and restore factory default settings)

- 1 Remove power from the SC5-IP unit.
- 2 Press and hold the reset button on the front panel (requires paper clip or similar).
- 3 Apply power and after a couple of seconds release the reset button. The Maintenance menu will be displayed ⇒



- 4 Highlight 'Reset Configuration' and press . The Reset Config warning will be displayed ⇒
- 5 Highlight 'Reset' and press . All settings will be returned to their factory defaults and the previous Maintenance menu will be re-displayed.
- 6 Remove power from the unit and then re-apply it.
- 7 You now need to go through the [initial configuration procedure](#) and re-instate all of the required settings.







Clearing IP access control

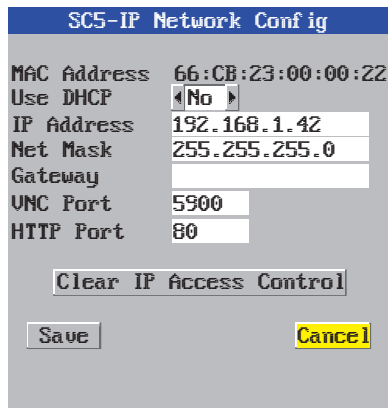
This option removes all entries from the IP access control feature within the SC5-IP.

What is IP access control?

The IP access control feature (configurable by a remote admin user) allows certain network address ranges to be denied access to the SC5-IP. If set incorrectly, it is possible to exclude all network users and so this option provides an emergency recovery point.

To clear IP access control

- 1 From a local keyboard (not accessible from a global keyboard), log on as the 'admin' user.
- 2 Press    (hotkeys can change).
- 3 Press  to select the More Menus.
- 4 Select 'Configuration'.
- 5 Select 'Network Configuration'.



- 6 Highlight the 'Clear IP Access Control' option and press .

Full configuration by global user

Once the basic features have been configured using the SC5-IP configuration menus, further changes can be made by authorised global users via the VNC interface. There are two main ways to use the VNC interface to access the SC5-IP unit:

- [The VNC viewer](#) – a small application supplied on the CD-ROM or downloadable from the RealVNC website or even downloadable from the SC5-IP itself.
- or
- [A standard browser that supports Java](#) – When a web browser makes contact, the SC5-IP provides the option to download a Java application to it. This allows a viewer window to be opened and operation to commence just as it would with the VNC viewer application.

[User Accounts](#)

Allows you to create and manage up to sixteen separate user accounts, each with separate access permissions.

[Unit Configuration](#)

Allows you to alter both basic and fundamental settings within the unit.

[Time & Date Configuration](#)

Allows you to configure all aspects relating to time keeping within the unit.

[Network Configuration](#)

Here you can alter any of the existing network settings plus you can take advantage of the IP access control feature that lets you to specifically include or exclude certain addresses or networks.

[Serial Port Configuration](#)

Lets you setup or alter the details concerning the OPTIONS serial port.

[Host Configuration](#)

Allows you to configure user access and hot key switching for the connected host systems.

[Logging and Status](#)


Provides various details about the user activity on the unit.

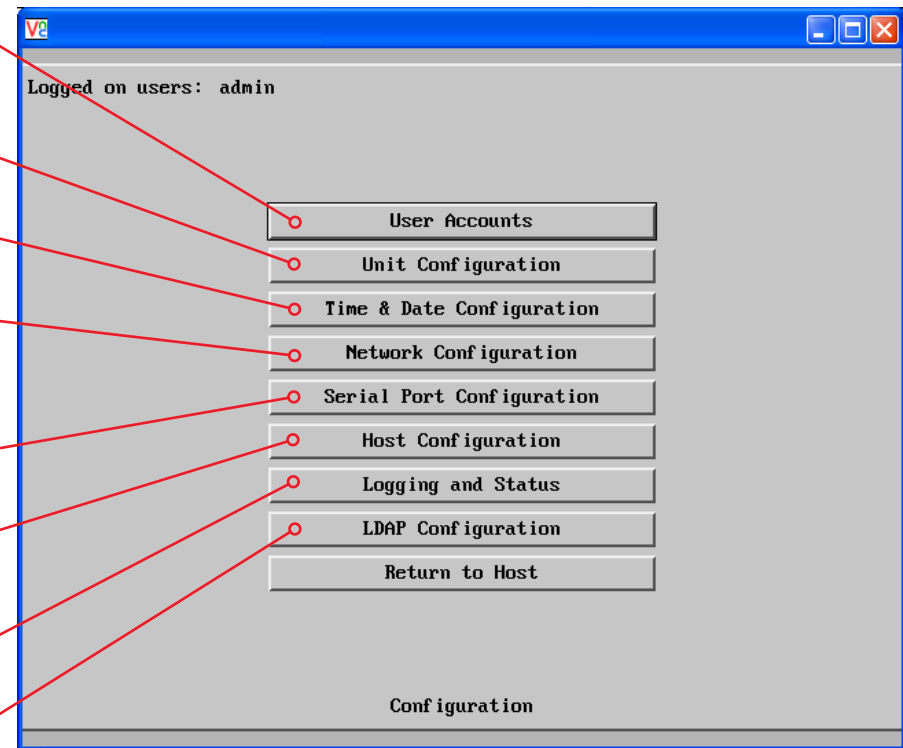
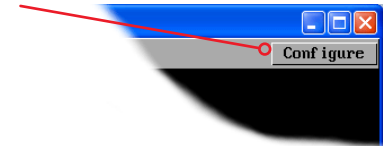
[LDAP Configuration](#)

Allows you to configure settings which enable the unit to consult external databases in order to verify user details.

Shaded items signify options that are not available via the standard configuration menus.

To configure the unit from a global user location

- 1 Use either the VNC viewer or a standard web browser to make remote contact with the SC5-IP – see [Global user access](#) for more details.
- 2 If the username entry is not blanked out, enter 'admin'. Then enter the admin password (if no password is set, then just press ). Once logged in, the SC5-IP will show the video output from the host system (if one is connected), or otherwise a 'No Signal' message.
- 3 Click the Configure button in the top right hand corner of the window to display the main configuration page ↴



For more information about each page, please see [Appendix 2 - Configuration pages via viewer](#) in the 'Further information' chapter.



INSTALLATION

CONFIGURATION

OPERATION

FURTHER INFORMATION

INDEX

Encryption settings

The SC5-IP offers a great deal of flexibility in its configuration and this extends equally to its encryption settings that are used to prevent unauthorised interception of signals. Due to the variety of situations in which the SC5-IP might be used and the range of viewer applications that need to view it, a number of settings are available. The encryption settings to use depend upon how the potential global users will operate.

Important factors to consider when setting these options might be:

- Do all global user connections and operations require encryption?
- Will some global users be using older VNC viewer versions?

SC5-IP encryption settings

The SC5-IP configuration menu offers three encryption settings:

- **Always on** - This setting will force all viewers to use encryption. *Note: This setting will preclude any VNC viewer versions that do not support encryption.*
- **Prefer off** - This setting does not enforce encryption unless a viewer specifically requests it. If a viewer has its 'Let server choose' setting, then an un-encrypted link will be set up.
- **Prefer on** - This setting generally enforces encryption unless an earlier viewer version is unable to support it, in which case the link will be un-encrypted. If a viewer has its 'Let server choose' setting, then the link will be encrypted.

Viewer encryption settings

The web browser viewers and VNC viewers (of level 4.0b5S or higher) offer four encryption settings:

- **Always on** - This setting will ensure that the link is encrypted, regardless of the SC5-IP encryption setting.
- **Let server choose** - This setting will follow the configuration of the SC5-IP. If the SC5-IP has 'Always on' or 'Prefer on' set, then the link will be encrypted. If the 'Prefer off' setting is selected at the SC5-IP, then the link will not be encrypted.
- **Prefer off** - This setting will configure an un-encrypted link if the SC5-IP will allow it, otherwise it will be encrypted.
- **Prefer on** - If the SC5-IP allows it, this setting will configure an encrypted link, otherwise it will be un-encrypted.



INSTALLATION

CONFIGURATION

OPERATION

FURTHER
INFORMATION

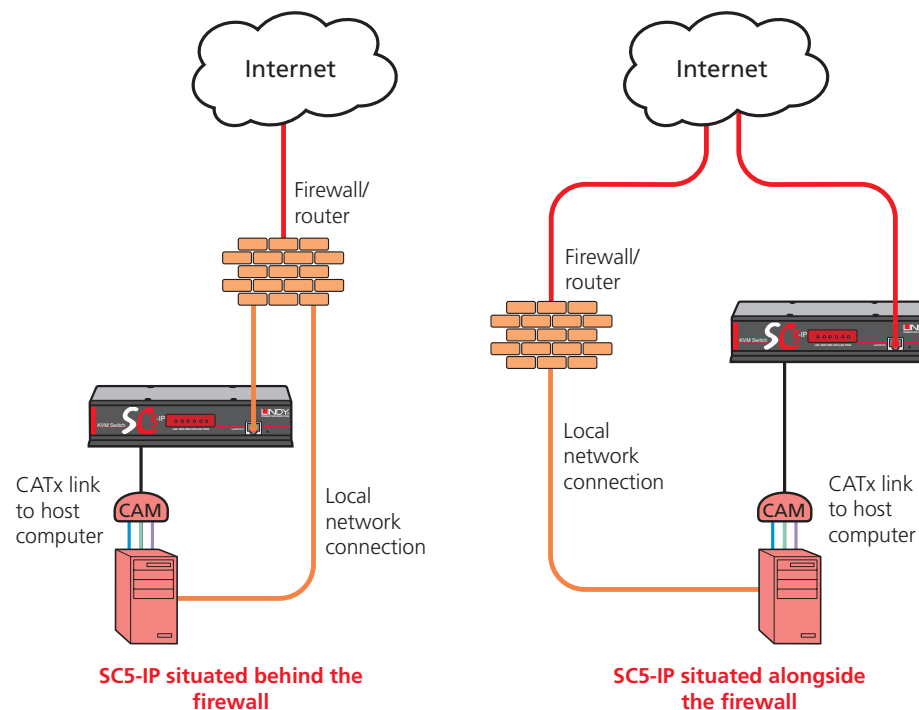
INDEX

Networking issues

Thanks to its robust security the SC5-IP offers you great flexibility in how it integrates into an existing network structure. The SC5-IP is designed to reside either on an internal network, behind a firewall/router or alternatively with its own direct Internet connection.

Positioning SC5-IP in the network

Every network setup is different and great care needs to be taken when introducing a powerful device such as the SC5-IP into an existing configuration. A common cause of potential problems can be in clashes with firewall configurations. For this reason the SC5-IP is designed to be intelligent, flexible and secure. With the minimum of effort it can reside either behind the firewall or alongside with its own separate Internet connection.



IMPORTANT: When the SC5-IP is accessible from the public Internet connection, you must ensure that sufficient [security measures](#) are employed.



INSTALLATION

CONFIGURATION

OPERATION

FURTHER INFORMATION

INDEX

Placing SC5-IP behind a router or firewall

A possible point of contention between the SC5-IP and a firewall can occasionally arise over the use of IP ports. Every port through the firewall represents a potential point of attack from outside and so it is advisable to minimise the number of open ports. The SC5-IP usually uses two separate port numbers, however, these are easily changeable and can even be combined into a single port.

IMPORTANT: The correct configuration of routers and firewalls requires advanced networking skills and intimate knowledge of the particular network. We cannot provide specific advice on how to configure your network devices and strongly recommend that such tasks are carried out by a qualified professional.

Port settings

As standard, the SC5-IP uses two [ports](#) to support its two types of viewer:

- **Port 80** for users making contact with a web browser, and
- **Port 5900** for those using the VNC viewer.

When these port numbers are used, VNC viewers and web browsers will locate the SC5-IP correctly using only its network address. The firewall/router must be informed to transfer any traffic requesting these port numbers through to the SC5-IP.

When a web server is also on the local network

Port 80 is the standard port used by web (HTTP) servers. If the SC5-IP is situated within a local network that also includes a web server or any other device serving port 80 then, if you want to use the web browser interface from outside the local network environment, the HTTP port number of the SC5-IP may need to be changed.

When you change the HTTP port to anything other than 80, then each remote browser user will need to specify the port address as well as the IP address. For instance, if you set the HTTP port to '8000' and the IP address is '192.168.47.10' then browser users will need to enter:

http://192.168.47.10:8000

(Note the single colon that separates the IP address and the port number).

The firewall/router would also need to be informed to transfer all traffic to the new port number through to the SC5-IP.

If you need to change the VNC port number

If you change the VNC port to anything other than 5900, then each VNC viewer user will need to specify the port address as well as the IP address. For instance, if you set the VNC port to '11590' and the IP address is '192.168.47.10' then VNC viewer users will need to enter:

192.168.47.10::11590

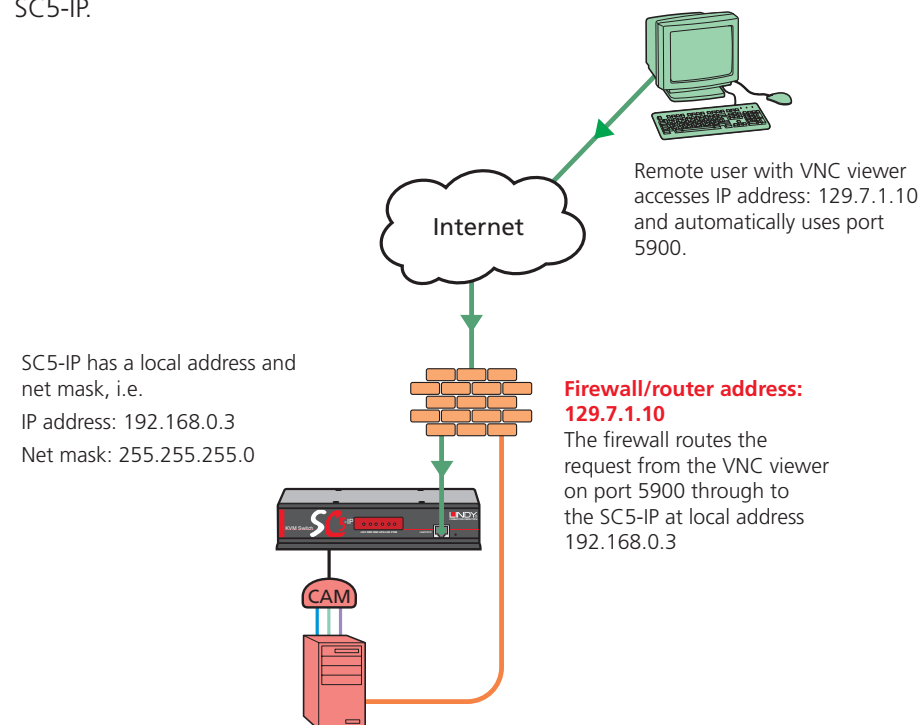
(Note the *double* colons that separate the IP address and port number).

The firewall/router would also need to be informed to transfer all traffic to the new port number through to the SC5-IP.

Addressing

When the SC5-IP is situated within the local network, you will need to give it an appropriate local IP address, IP network mask and default gateway. This is achieved most easily using the DHCP server option which will apply these details automatically. If a DHCP server is not available on the network, then these details need to be applied manually in accordance with the network administrator.

The firewall/router must then be informed to route incoming requests to port 5900 or port 80 (if available) through to the local address being used by the SC5-IP.



To discover a DHCP-allocated IP address

Once a DHCP server has allocated an IP address, you will need to know it in order to access the SC5-IP via a network connection. To discover the allocated IP address:

- 1 In network section of either the [local configuration menus](#) or the [global configuration pages](#), set the 'Use DHCP' option to 'Yes' and select 'Save'. Once the page is saved, the SC5-IP will contact the DHCP server and obtain a new address.
- 2 Re-enter the same 'Network configuration' screen where the new IP address and network mask should be displayed.

DNS addressing

As with any other network device, you can arrange for your SC5-IP to be accessible using a name, rather than an IP address. This can be achieved in two main ways:

- For small networks that do not have a DNS (Domain Name System) server, edit the 'hosts' files on the appropriate remote systems. Using the hosts file, you can manually link the SC5-IP address to the required name.
- For larger networks, declare the IP address and required name to the DNS server of your local network.

The actual steps required to achieve either of these options are beyond the scope of this document.



INSTALLATION

CONFIGURATION

OPERATION

FURTHER
INFORMATION

INDEX

Placing SC5-IP alongside the firewall

SC5-IP is built from the ground-up to be secure. It employs a sophisticated 128bit public/private key system that has been rigorously analysed and found to be highly secure (a security white paper is available upon request from LINDY). Therefore, you can position the SC5-IP alongside the firewall and control hosts that are also IP connected within the local network.

IMPORTANT: If you make the SC5-IP accessible from the public Internet, care should be taken to ensure that the maximum security available is activated. You are strongly advised to enable encryption and use a strong password. Security may be further improved by restricting client IP addresses, using a non-standard port number for access.

Ensuring sufficient security

The security capabilities offered by the SC5-IP are only truly effective when they are correctly used. An open or weak password or unencrypted link can cause security loopholes and opportunities for potential intruders. For network links in general and direct Internet connections in particular, you should carefully consider and implement the following:

- Ensure that encryption is enabled.
By [local configuration menu](#) or [global configuration page](#).
- Ensure that you have selected secure passwords with at least 8 characters and a mixture of upper and lower case and numeric characters.
By [global configuration page](#).
- Reserve the admin password for administration use only and use a non-admin user profile for day-to-day access.
- Use the latest Secure VNC viewer (this has more in-built security than is available with the Java viewer). To [download the viewer](#).
- Use non-standard [port numbers](#).
- Restrict the range of IP addresses that are allowed to access the SC5-IP to only those that you will need to use. To [restrict IP access](#).
- Do NOT Force VNC protocol 3.3.
- Ensure that the computer accessing the SC5-IP is clean of viruses and spyware and has up-to-date firewall and anti-virus software loaded that is appropriately configured.
- Avoid accessing the SC5-IP from public computers.

Security can be further improved by using the following suggestions:

- Place the SC5-IP behind a firewall and use the port numbers to route the VNC network traffic to an internal IP address.
- Review the activity log from time to time to check for unauthorised use.
- Lock your server consoles after they have been used.

A security white paper that gives further details is available upon request from LINDY.

Ports

In this configuration there should be no constraints on the port numbers because the SC5-IP will probably be the only device at that IP address. Therefore, maintain the HTTP port as 80 and the VNC port as 5900.

Addressing

When the SC5-IP is situated alongside the firewall, it will require a public static IP address (i.e. one provided by your Internet service provider).

More addressing information:

[Discover DHCP-allocated addresses](#)

[DNS addressing](#)



INSTALLATION

CONFIGURATION

OPERATION

FURTHER
INFORMATION

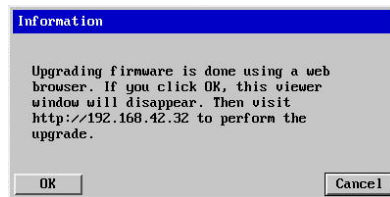
INDEX

Upgrading SC5-IP models

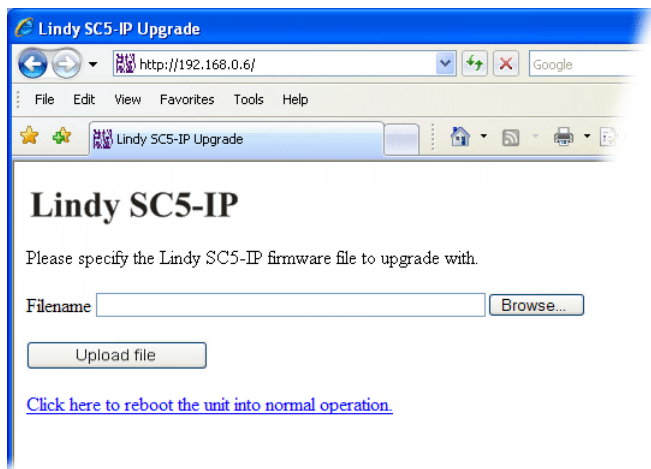
The SC5-IP models are upgraded via global connection (through the IP network port). Upgrades are digitally signed using a secure key. This prevents unauthorised or altered firmware images being downloaded into the SC5-IP.

To upgrade SC5-IP models

- 1 Obtain the latest firmware revision for the SC5-IP from LINDY and decompress the download file. View the decompressed files and make a note of the name and location of the .bin file that was part of the download file collection.
- 2 Make a [global connection](#) to the SC5-IP unit and login as the admin user.
- 3 Once logged in, click the 'Configure' button in the top right corner of the window.
- 4 Click the 'Unit Configuration' button.
- 5 Click the 'Advanced Unit Configuration' button.
- 6 Click the 'Upgrade Firmware' button. This dialog will be displayed:

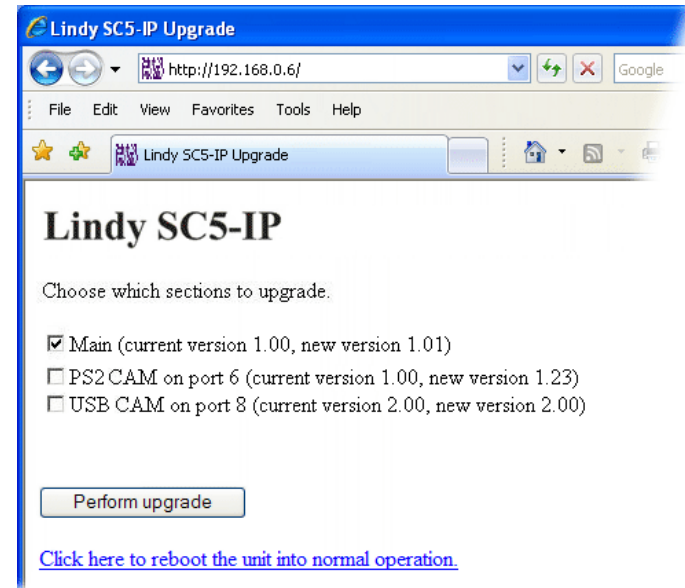


- 7 Click OK. The SC5-IP is now ready to accept the upgrade files. Open your browser and log into the SC5-IP using the IP address that was confirmed in the dialog. Once connected, the SC5-IP will offer the following screen:
- 8 Click the 'Browse' button and locate the .bin upgrade file that you downloaded earlier. Click the 'Upload file' button. The SC5-IP will next show the following screen:



- 9 Select which portion of the SC5-IP that you wish to upgrade:

- Tick the 'Main' option to upgrade the SC5-IP unit itself.
- Tick one or more of the CAM options to include them in the upgrade process.



- 10 When ready, click the 'Perform upgrade' button. The upgrade will take place and its progress will be shown on screen.
- 11 When the upgrade is complete, click the link 'Click here to reboot the unit into normal operation'.

Recovering from a failed upgrade

If a problem is encountered while upgrading the SC5-IP, it is still possible to restart the unit and attempt a new upgrade process.

To invoke backup/recovery mode

- 1 Remove power, press and hold the reset button (insert a thin implement such as a straightened paper clip into the small hole next to the IP connector) and then re-apply power. Then, release the reset button
- 2 Access the SC5-IP using a web browser on an IP connected system. When the upgrade page is displayed, follow the normal instructions, except after step 10, remove and replace the power on the unit.



INSTALLATION

CONFIGURATION

OPERATION

FURTHER INFORMATION

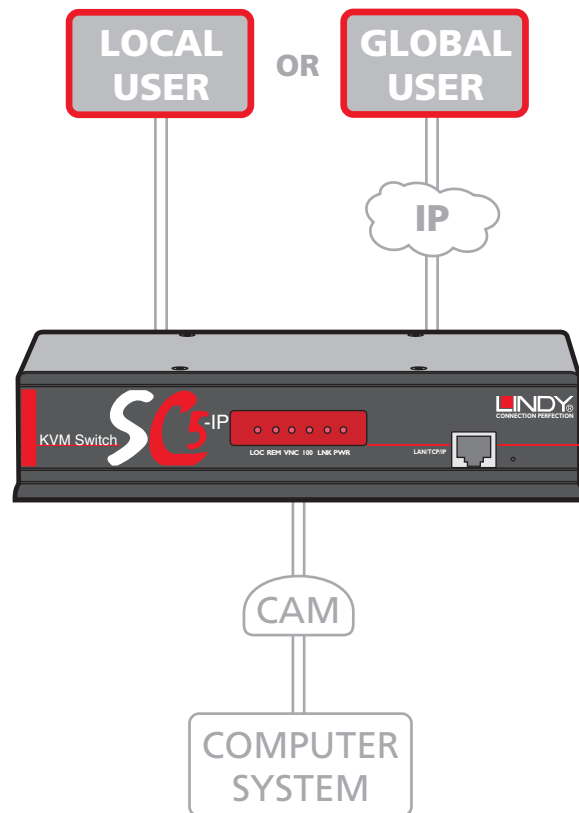
INDEX

Operation

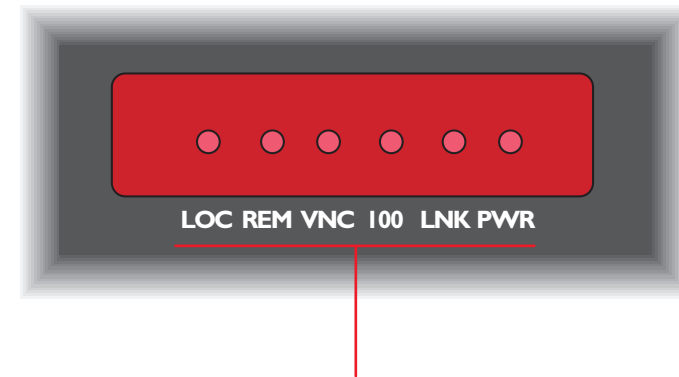
Accessing the SC5-IP

The SC5-IP provides two ways to gain access:

- [Local user access](#), or
- [Global user access](#) via IP network link.



The front panel indicators



Indicators

- **LOC** Keyboard or mouse data are being received from the local console.
- **REM** Keyboard or mouse data are being received from a remote (global) viewer.
- **VNC** Indicates that a global user is connected and active.
- **100** Indicates the Ethernet network speed (10/100Mbps).
- **LNK** Indicates that a network link is present.
- **PWR** Indicates that power is present.

Local user access

To gain access as a local user:

- 1 From the local keyboard, press any key to display the login prompt:



SC5-IP Login

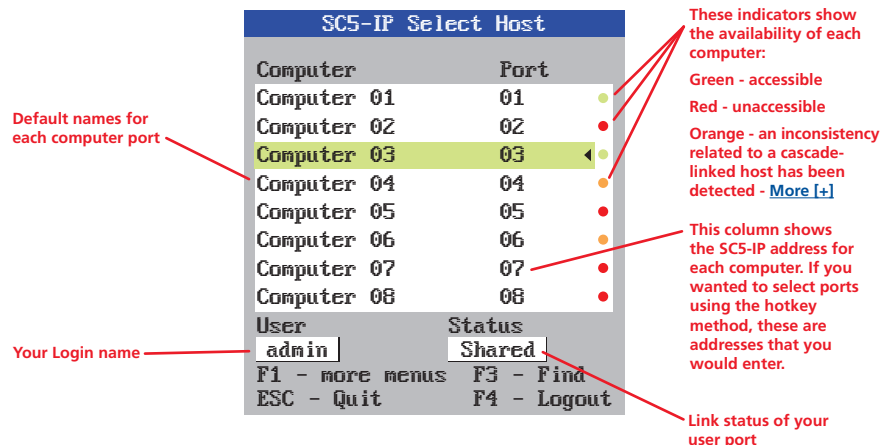
Username:

Password:

Enter your Login name here

If the above login prompt is not displayed, you are either already logged in to the SC5-IP unit, or the security features have not been enabled. In such cases see 'To view this menu at any time' below.

- 2 Enter your username and password. Providing you have the correct permissions, the screen will display the Select Host menu, showing you a list of computers for which you have permission to access:



SC5-IP Select Host

Computer	Port	Status
Computer 01	01	●
Computer 02	02	●
Computer 03	03	●
Computer 04	04	●
Computer 05	05	●
Computer 06	06	●
Computer 07	07	●
Computer 08	08	●

Default names for each computer port

These indicators show the availability of each computer:
Green - accessible
Red - inaccessible
Orange - an inconsistency related to a cascade-linked host has been detected - [More \[+\]](#)

This column shows the SC5-IP address for each computer. If you wanted to select ports using the hotkey method, these are addresses that you would enter.

Your Login name

User: admin Status: Shared

F1 - more menus F3 - Find
ESC - Quit F4 - Logout

Link status of your user port

To view this menu at any time: Press and hold the hotkeys (usually **Ctrl** and **Alt**), then press **M** and finally release all three keys.

*Note: The **Ctrl** and **Alt** keys when pressed in combination are called 'hotkeys' and they signal to the SC5-IP that you wish to control it, rather than the host computer. However, if these particular hotkeys clash with another device or program, then your administrator may change them to a different combination. If the **Ctrl** **Alt** **M** combination fails to work, then please contact your system administrator for details.*

To move the menu (and login) box position

- 1 While viewing any menu, press and hold **Ctrl** and **Alt**.
- 2 Press the **↓**, **↑**, **←** and **→** keys to move the menu to the required position.

Note: The new menu position will be used until power is next re-applied.

Selecting a computer

There are three main ways for local users to select a specific computer channel:

- Using hotkeys (as described below) – this is a good method if you continually access a small number of computers.
- [Using the Select Host menu](#) – this is the best method when there are many connected computers.
- [Using mouse buttons](#) – this is a good method for cycling between a small number of computers.

For all methods (if the [confirmation box option](#) is enabled), when the required port is selected, a pop up message will be displayed to confirm the computer name or number, and its status. Alternatively, an error message explaining why a connection is not possible (press **Esc** to cancel the latter type of message).

To avoid the 'hall of mirrors' effect

IMPORTANT: Never configure a system so that your viewer is viewing itself.

When controlling a host computer via the local user port or a remote user port, if the host computer is networked it is possible to make the VNC viewer or a browser to create a link back to itself via the global (IP) capabilities of the unit. This will set up a 'hall of mirrors' effect, where the computer is viewing itself into infinity. While technically possible, the SC5-IP unit is not designed to withstand this treatment and could sustain damage.

To select a computer using hotkeys

- 1 Simultaneously press and hold **Ctrl** and **Alt**.

*Note: The **Ctrl** and **Alt** keys when pressed in combination are called 'hotkeys' and they signal to the SC5-IP that you wish to control it, rather than the computer. However, if these particular hotkeys clash with another device or program, then your administrator may change them to a different combination. If the **Ctrl** **Alt** combination fails to work, then please contact the system administrator for details.*

- 2 While still holding **Ctrl** and **Alt**, press the first numeral of the required port address, then:

- If the port address is a single character, release all of the keys.
- If the port address is two or more characters, release the first numeral key and press the second – repeat this procedure until all of the port address numerals have been entered, then release **Ctrl** and **Alt**.

Note: The numbers on your keyboard's numeric keypad are not valid, use only the numeral keys above the QWERTY section.

Note: If your user port does not have authorisation to view the selected port then an 'Insufficient user rights' messages will be displayed.

Note: When using hotkeys, the leading zeros for all single digit port numbers (including all cascade levels) are optional, i.e. 01, 02...09.

Standard hotkeys

The range of hotkey combinations are as follows:

*Note: If your hotkeys have been changed, substitute them for **Ctrl** and **Alt** in the examples given here.*

Ctrl **Alt** **1**

Selects port 1

Ctrl **Alt** **2**

Selects port 2

•
•

•
•

Ctrl **Alt** **1** then **0**

Selects port 10

*Note: When entering multiple digit addresses as above, keep **Ctrl** and **Alt** pressed down until all other numbers have been entered.*

Ctrl **Alt** **Tab**

Selects the next available port

Ctrl **Alt** **0**

Switches off the video signal – this will cause a power saving monitor to enter its standby mode. To awaken the monitor, simply select any fixed channel using any of the suggested methods.

Ctrl **Alt** **L**

Logs out the current user (if security is enabled) or selects port 0 to disable the video signal (if security is disabled).

Ctrl **Alt** & **↓**, **↑**, **←** or **→**

Moves the currently displayed on-screen menu around the screen.

To select a computer using the Select Host menu

1 Display the Select Host menu in one of two ways:

- By simultaneously pressing and then releasing **Ctrl** **Alt** **M**, or
- By pressing the middle and right buttons of a three button mouse.

Note: The mouse switching option is usable only if the 'Mouse Switching' option is enabled. See [Global preferences](#) for more details.

At this point, depending on the security settings and the current log in situation, one of two things will be displayed, either the login screen, or the Select Host menu:

SC5-IP Select Host		
Computer	Port	
Computer 01	01	•
Computer 02	02	•
Computer 03	03	•
Computer 04	04	•
Computer 05	05	•
Computer 06	06	•
Computer 07	07	•
Computer 08	08	•
User Status		
admin	Shared	
F1 - more menus	F3 - Find	
ESC - Quit	F4 - Logout	

The Select Host menu – here you can select computers by name.

- 2 Use the **↓** and **↑** keys (or the scroll wheel of an IntelliMouse) to highlight the required computer name. Alternatively (for large configurations), press **F3** to perform an alphabetical search for a particular port name. You can also use the PgUp and PgDn keys to move up or down a full page of list entries at a time, or press the Home and End keys to quickly move to the beginning or end of the list, respectively.

Note: If security has been enabled then only computers to which the current user port has permission will be displayed.

- 3 Press **↵** to select the highlighted port.

*Note: Pressing **↵** will select the highlighted port in shared mode (other users can also view the computer). To select the port in private mode, press **Shift** and **↵** when choosing.*

To select a computer using mouse buttons

Note: This procedure works only with three-button or IntelliMouse devices and only if the 'Mouse Switching' option has been enabled by your administrator.

- 1 Hold down the middle button (or scroll wheel) of the mouse.
- 2 Click the left mouse button to select the next computer port. When the correct port is reached, release the middle button.

*Note: Clicking the left mouse button will select the highlighted port in shared mode (other users can also view the computer). To select the port in private mode, hold **[Shift]** and then click the left mouse button.*

Note: If security has been enabled then only computers to which you have permission will be displayed.

To select a computer using mouse buttons – Advanced method

- 1 Select the on-screen menu by pressing the middle and right buttons of a three button mouse.
- 2 Use the scroll wheel to highlight the required computer port.
- 3 Then, select either:
 - *Shared Use* - press the left mouse button - This *standard* method allows other users to view the same computer port. Control of the port is given to one user at a time, on a first-come, first-served basis and is relinquished after a certain period of inactivity.
 - *Escape without selecting a port* – press the right mouse button.

Logging in and out

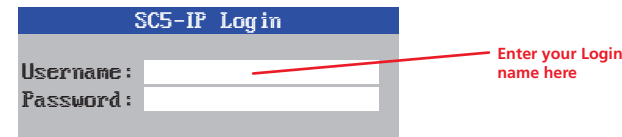
The SC5-IP features a straightforward security system that helps to prevent unauthorised access to some, or all connected computers.

If the security option has been selected by your administrator then you will be asked to enter a *User Name* and *Password* when you first access a user port. When you have finished using the computer, it is then good practice to logout, forcing any other users to authenticate themselves prior to use.

Note: If the security option has not been enabled then no login is required.

To log in

- 1 If it is not already displayed, move the mouse or press any key to display the log in screen.



- 2 Enter your designated *User Name* and press **[Enter]**.
- 3 Enter your designated *Password* and press **[Enter]**. If both entries are correct then the selected port will be displayed.

Note: If either the User Name or Password are incorrect, the entries will be cleared to allow another attempt.

To log out

Either:

- Press **[Ctrl]** **[Alt]** and **[L]** at any time to log out.

or

- 1 Display the Select Host menu in either of two ways:

- By simultaneously pressing and then releasing **[Ctrl]** **[Alt]** **[M]**.

*Note: The **[Ctrl]** and **[Alt]** hotkeys may have been changed. If the combination fails to work, then please contact the system administrator for details.*

- By pressing the middle and right buttons of a three button mouse, or

- 2 Press **[F4]**. You will be logged out and the screensaver will be displayed. Press a key or move the mouse to re-display the login window.

The confirmation box

The SC5-IP provides the option of a confirmation box that is displayed on screen for three seconds after a computer is selected. The confirmation box indicates the current user port and your user name, the selected computer and the connection status. You can enable or disable the confirmation box, as required.

SC5-IP Status			
Computer		Port	
Computer 01		01	
User		Status	
admin		Shared	

To enable/disable the confirmation box

- 1 Display the Select Host menu in one of two ways:
 - By simultaneously pressing and then releasing **Ctrl** **Alt** **M**, or
 - By pressing the middle and right buttons of a three button mouse.

If you are not already [logged in](#), do so now.

- 2 Press **F1** to select 'More menus'.
- 3 Highlight the 'User Preferences' option and press **Enter** to select.
- 4 Highlight the 'Confirmation Box' option and press **Space** to select 'Enabled' or 'Disabled', as required.
- 5 Select the 'Save' button to return to the previous menu.

The reminder banner

As many computer screen layouts can appear very similar, the SC5-IP provides a reminder banner option that indicates which computer port you are currently viewing. The banner is usually displayed at the top of the screen, using white lettering and transparent background. You can:

- Move the banner
- Change the banner colours, and/or
- Disable the banner

To move the reminder banner

- 1 While viewing a computer port, press and hold **Ctrl** and **Alt**.

*Note: The **Ctrl** and **Alt** hotkeys may have been changed. If the combination fails to work, then please contact the system administrator for details.*

- 2 Press the **Down**, **Up**, **Left** and **Right** keys to move the banner to the required position.

To change banner colours or disable the banner

- 1 Display the Select Host menu in one of two ways:
 - By simultaneously pressing and then releasing **Ctrl** **Alt** **M**, or
 - By pressing the middle and right buttons of a three button mouse.
- If you are not already [logged in](#), do so now.
- 2 Press **F1** to select 'More menus'.
- 3 Highlight the 'User Preferences' option and press **Enter** to select.
- 4 Select the required option:
 - To disable the banner – highlight 'Reminder Banner' and press **Space** until 'Disabled' is shown.
 - To change colours – highlight 'Reminder Colour' and press **Space** until the desired colour combination is displayed.
- 5 Select the 'Save' button to return to the previous menu.



User preferences and functions

In addition to customising the reminder banner as described earlier, you can also:

- Change the colour of the reminder banner,
- Select the screen saver style, or
- Restore mouse operation.

All of these options are discussed within [Appendix 1](#).

Orange dot indicators in the Select Host menu

Within the Select Host menu, each listed host has a coloured dot associated with it to indicate its general status: Green for accessible and Red for inaccessible.

SC5-IP Select Host		
Computer	Port	
Computer 01	01	●
Computer 02	02	●
Computer 03	03	●
Computer 04	04	●
Computer 05	05	●
Computer 06	06	●
Computer 07	07	●
Computer 08	08	●
User Status		
admin	Shared	
F1 - more menus F3 - Find		
ESC - Quit F4 - Logout		

Green: Host accessible
Red: Host inaccessible
Orange: Inconsistency related to a cascade connection.

There is, however, a third state where the dot turns Orange. An orange dot against a host entry indicates that an inconsistency relating specifically to cascaded hosts.

The problem can occur for two main reasons, either:

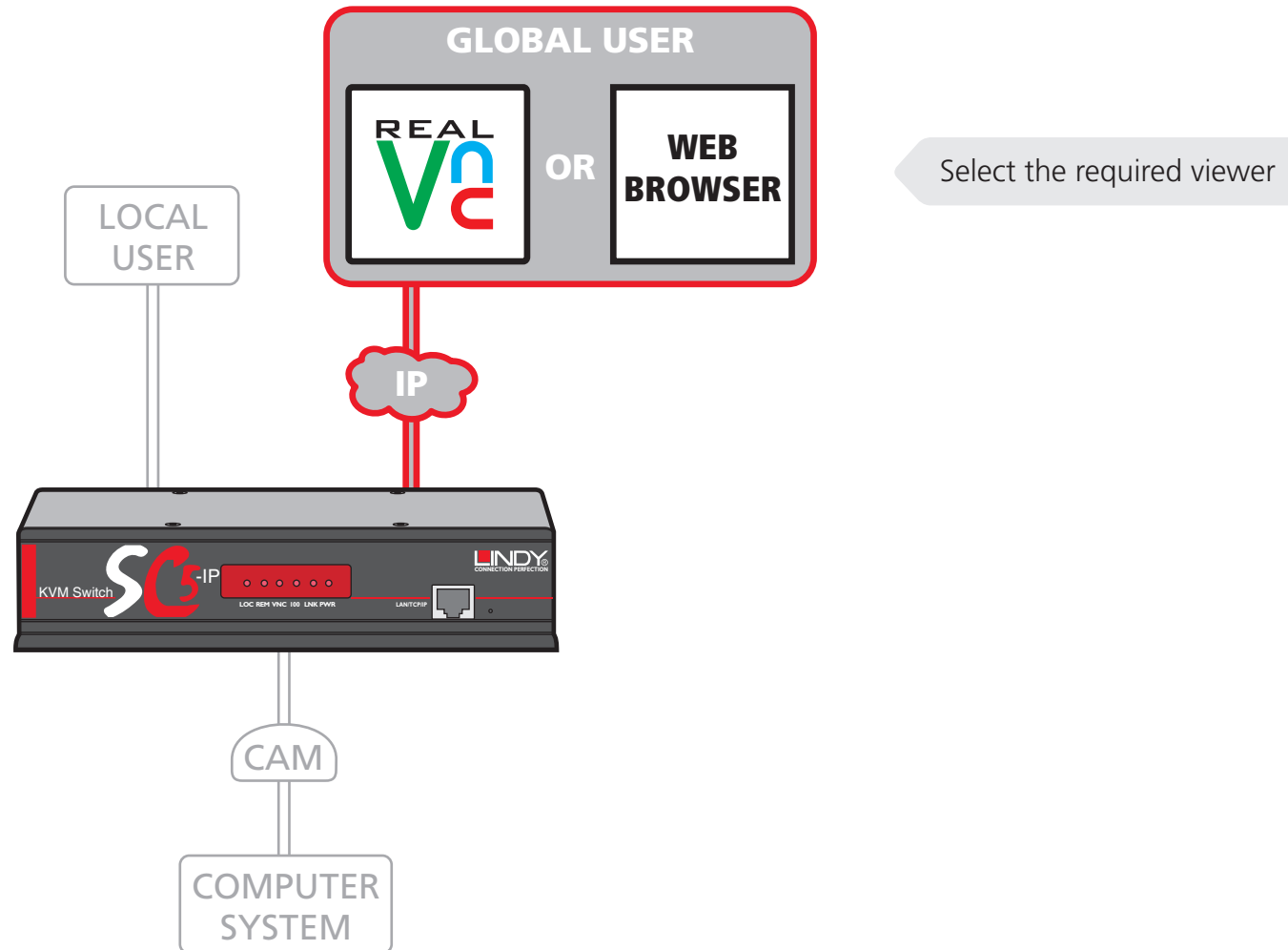
- A cascaded computer (or multiple computers) has been added to an address such as 0301, however, there is still a registered entry for a directly connected host at address 03. Thus, the now non-existent host at 03 will be marked with an orange dot.
- A previously connected cascade has been removed and a computer connected directly instead. This will cause all of the entries for the removed cascaded hosts to be marked with orange dots. If they are not to be re-instated, then the administrator should delete the entries.

If you attempt to select an entry marked with an orange dot (by the menu, by hotkeys or from the VNC viewer) you will see an error message stating 'computer not connected'.



Global user access

Global users access the SC5-IP using a viewer and a network/internet link. There are two types of viewer: a standalone VNC viewer or a VNC Java application used within a standard web browser.



Global user access via VNC viewer

The VNC viewer is a compact application that runs on your IP-connected 'global' system and allows you to view and use the SC5-IP and its host computer(s). VNC viewer is readily available from a number of different sources:

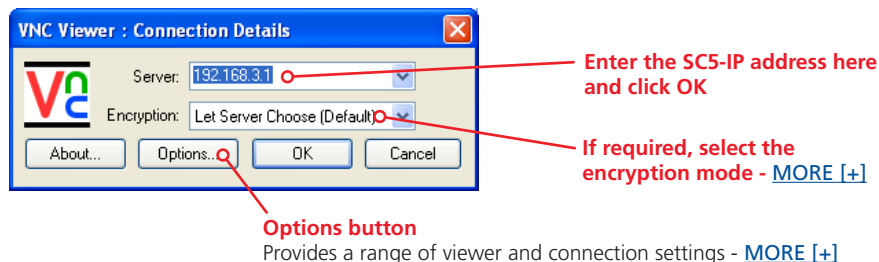
- from the SC5-IP installation CD
- from the SC5-IP itself
- from the [RealVNC website](#)

To access via the VNC viewer

- 1 Locate and select the VNC viewer icon ⇒



A connection details dialog will be displayed:



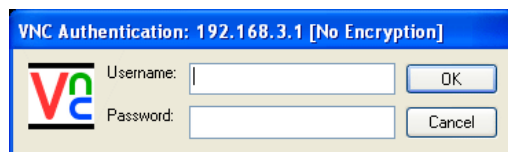
- 2 In the 'Server:' entry, type the address of the SC5-IP as follows:

v.w.x.y

where v.w.x.y is the IP network address, for example 192.168.0.3

- [If you have been asked to also enter a port number.](#)

- 3 Click the OK button. Depending on the options selected, you may need to confirm certain items. A connection attempt will be made and if successful, an authentication dialog will be displayed:



- 4 Enter your Username and Password. The [viewer window](#) should now open and show the current host computer. *Note: If the Username entry is blanked out then only admin user account is currently defined and only a password is required.*

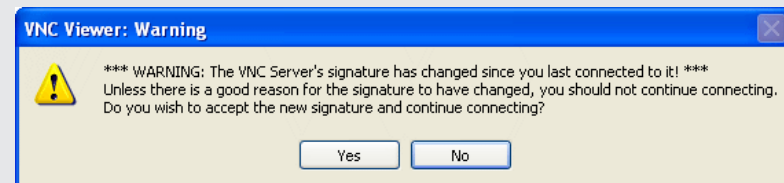
Downloading VNC viewer from the SC5-IP

The SC5-IP has the ability to distribute its own VNC viewer application.

To download the VNC viewer

- 1 Open your Web browser.
- 2 Enter the network address where the SC5-IP is situated (in the form: <http://192.168.0.3>) and make the link.
- 3 In the opening SC5-IP screen, click the link that offers to download the secure VNC viewer 'from the unit'.
- 4 Save the download file (vncviewer.exe) to your system.
- 5 Select and run the downloaded file and then connect to the SC5-IP using the VNC viewer application.

IMPORTANT: During login, if you see a warning message similar to the one shown here, then **stop** and do not proceed.



This message is displayed if an SC5-IP unit, that your viewer has previously visited, has had a change of security keys. This is not uncommon if a unit is reset for some reason. However, it could also mean that your trusted unit is being spoofed and you may not be connecting to the system that you think you are.

Do not click the Yes button until you have checked with your administrator that the trusted SC5-IP unit has been recently reset for some reason.

Global user access via web browser

You can use a standard Web browser ([supported versions](#)) to gain access to the SC5-IP and its host computer(s). As soon as you make contact with the SC5-IP it will begin downloading a small Java application to your browser, which will be used only for the duration of your connection.


To access via your web browser

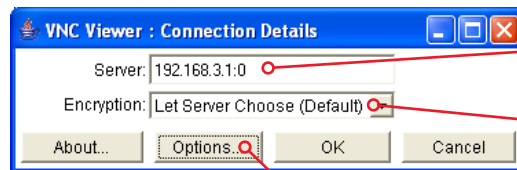
- 1 Launch your standard Web browser as usual.
- 2 In the Address section, type the address of the SC5-IP as follows:

http://v.w.x.y

where v.w.x.y is the IP network address, for example 192.168.0.3

- [If you have been asked to also enter a port number.](#)

- 3 Press . A connection attempt will be made.
- 4 In the browser window, select the 'Connect using built-in Java VNC viewer' option to download a small application that will temporarily empower your browser (on slow connections the application download can take several tens of seconds to complete). Once complete, a connection details dialog will be displayed:

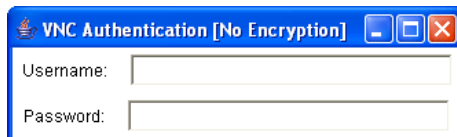


The previously entered SC5-IP address will be shown here
Options button

If required, select the encryption mode - [MORE \[+\]](#)

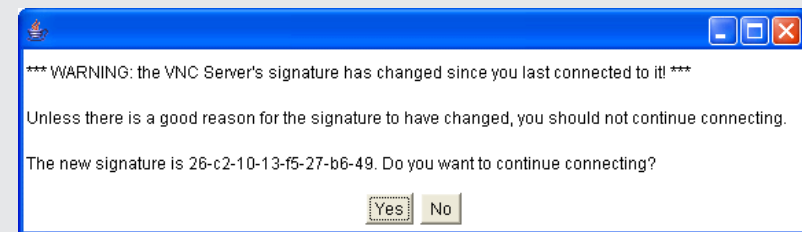
Provides a range of viewer and connection settings - [MORE \[+\]](#)

- 5 Make any necessary option/encryption changes and click the OK button to proceed. Depending on the options selected, you may need to confirm certain items.
- 6 A second connection attempt will be made and if successful, an authentication dialog will be displayed:



- 7 Enter your username and password. The [viewer window](#) should now open and show the current host computer. *Note: If the Username entry is blanked out then only admin user account is currently defined and only a password is required.*

IMPORTANT: During login, if you see a warning message similar to the one shown here, then **stop** and do not proceed.



This message is displayed if an SC5-IP unit, that your viewer has previously visited, has had a change of security keys. This is not uncommon if a unit is reset for some reason. However, it could also mean that your trusted unit is being spoofed and you may not be connecting to the system that you think you are.

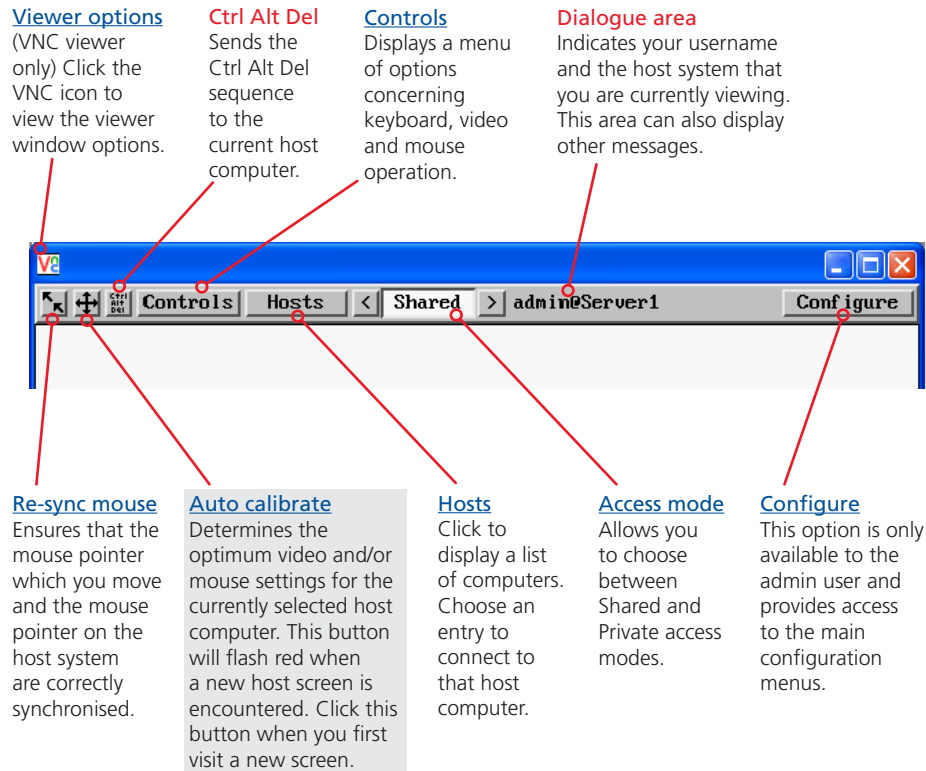
Do not click the Yes button until you have checked with your administrator that the trusted SC5-IP unit has been recently reset for some reason.

Using the viewer window

The viewer window gives you the ability to view and control the SC5-IP and its host computer(s). Its operation is almost identical regardless of whether you used the VNC viewer or your Web browser to display it.

The menu bar

The viewer window presents a menu bar similar to that shown below. Certain items within the toolbar are displayed depending upon your access permissions and/or the SC5-IP configuration.



When using the viewer window

What is the best screen resolution to use?

The best resolution for your computer is one that is larger than the screen of the host computer that you are viewing. This will allow you to see everything without scrolling around. Alternatively, the VNC viewer can be set to scale the image to fit your screen, but remember that some pixel dithering effect will be seen when scaling is used.


How do I navigate around a larger screen?

If the screen that you are viewing has a larger resolution than your viewing window you will need to scroll around to see all items. The viewer window allows you to 'bump scroll' (only in full screen mode). This means that when your mouse cursor bumps against the edge of the screen, the screen image will scroll across automatically.

How do I escape from full screen mode?

Press the F8 button. This button is changeable but is most often set to F8.

Why is the button flashing red?

This happens when a new host screen is viewed (that has not been viewed before). Click the  button to perform an auto calibration for the screen and the mouse. See [Auto calibrate](#) for important information about this feature.

How do I change between host computers?

The best way to change between host computers is to click the 'Hosts' button and then select the required computer by name. See [Host selection](#).

How do I remove traces of moved items from the screen?

When you move an item or window across the screen, sometimes it can leave unsightly trails. These are called *artifacts* and can be particularly prevalent when the connection speed is low. To remove artifacts, click the 'Controls' button and select the 'Refresh screen' option. See [Controls](#).

How do I make the most of a slow connection?

The VNC viewer is slightly better suited to slower connections than the browser viewer because it offers more options. Click the [Options](#) button of the VNC viewer when entering the SC5-IP address during log on.

Adjust the Threshold setting

Ensure that the video [Threshold setting](#) is set higher than the automatic setting suggests. Tweak this setting manually to ensure the best setting.

Fewer colours

Select the [Low \(64 colours\)](#) mode. The Very low option offers hardly any improvement and looks a lot worse.

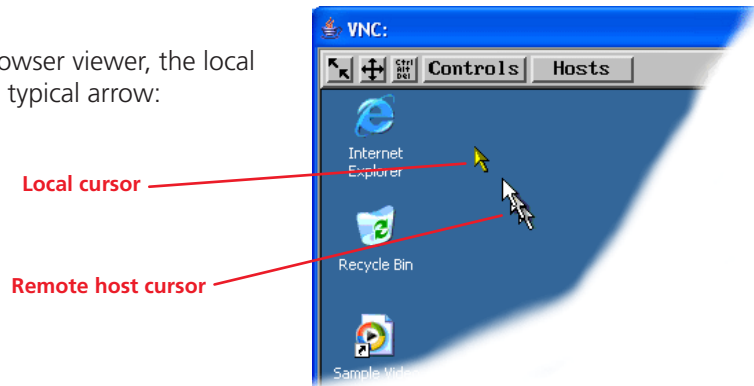
Rate limit mouse events

When selected, this mode greatly reduces the mouse movement data that are sent to the host computer. When you move the local mouse, the remote cursor will catch up roughly once per second.

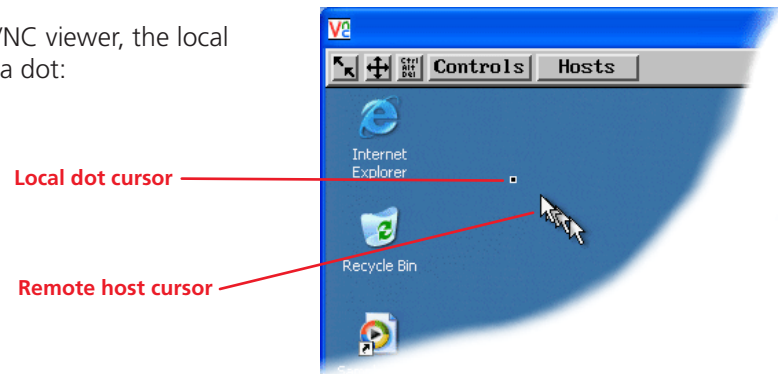
Mouse pointers

Both viewers provide a double mouse cursor to help overcome any delays caused by slow connections. When you move your mouse you will see two mouse cursors, a local one that responds immediately to your movements and a second, slower moving, cursor that represents the current mouse position at the host.

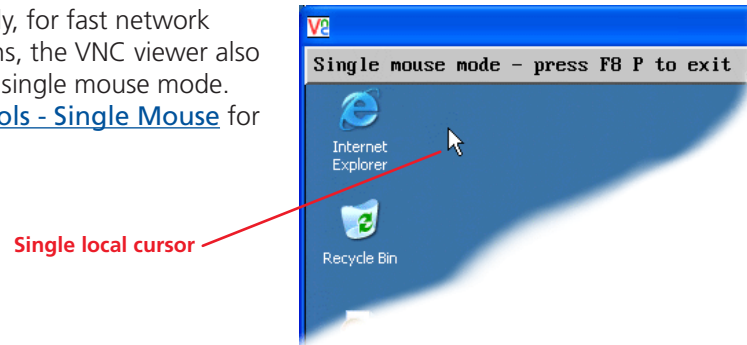
For the browser viewer, the local cursor is a typical arrow:



For the VNC viewer, the local cursor is a dot:



Additionally, for fast network connections, the VNC viewer also provides a single mouse mode. See [Controls - Single Mouse](#) for details.



Host selection

The Hosts button on the menu bar provides the quickest and most efficient way to switch between host computers. This is because the button is close at hand, but also because the screen calibration details for each host are reused when this method of switching is used. The alternative is to use [hotkey combinations](#) or the SC5-IP [on-screen menu](#).

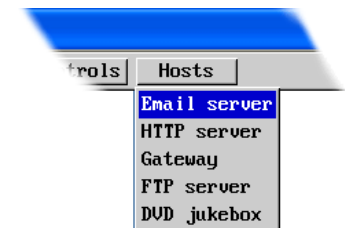
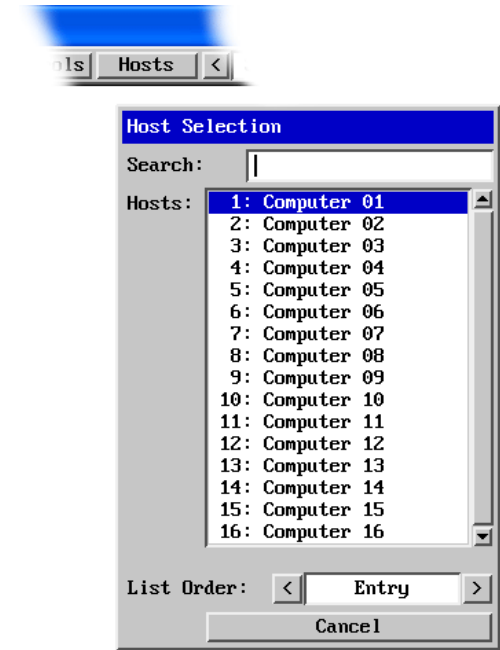
Note: The Hosts button is displayed only when the switching details for two or more computers have been declared within the configuration section by the admin user.

To select a host

- 1 Click the Hosts button to display a list of computers.
Note: If there are ten or less entries, then the list will appear as a simple drop down (as shown below).

- 2 Click the required computer name to view and control it.
You can use the List Order option to determine whether the hosts are listed by their entry number or alphabetically.

See [Appendix 2 - Host configuration](#) for details about programming new hosts into the SC5-IP ('admin' user status required).



Configure

This option is displayed only when you are logged on as the 'admin' user. When selected it provides access to a wide range of SC5-IP settings.

See [Appendix 2 - Configuration pages via viewer](#) for more details.


Auto calibrate

When you visit a host computer for the very first time, your viewer needs to determine the optimum video and mouse settings for that particular computer. The button will remind you to click it by flashing red when a new computer screen is encountered. Performing this step is important because it can help to decrease unnecessary video information being sent across the link, thus improving overall performance.

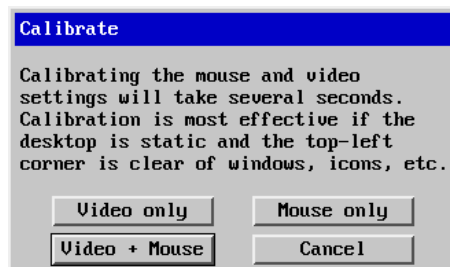
Once this has been done, providing you use the 'Hosts' button to switch between host computers, the video settings for each machine will be re-used.

Note: When performing an auto calibration, ensure that the screen image is static (no moving images) and also try to remove any on-screen displays generated by KVM switches (such as host names or menus). This is because they can affect the calibration process and result in a lower overall performance level. For mouse calibration, ensure that there are no application windows located around the upper left corner of the screen. This is because as the mouse calibration takes place, the cursor may change (to match the application as it skims across the window) and this may confuse the calculation. Also ensure that the host computer does not have the mouse cursor trails option enabled.

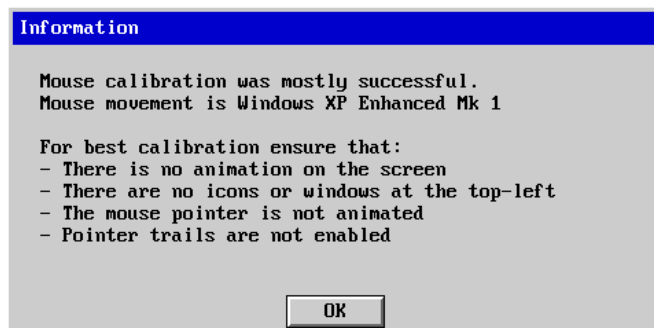
To auto calibrate the screen and/or mouse

- 1 Use the Hosts button to select the required computer.
- 2 Click the  button to display the Calibrate options dialog:
- 3 Click the required action.

A progress indicator will be displayed while the necessary calculations are made.




Upon completion an information dialog will explain the results:



Re-synchronise mouse

If you find that your local mouse pointer and that of the host are not correctly synchronised, use this feature to re-align their movements. This operation is also selectable from the Controls menu.

To re-synchronise the mouse

- 1 Use the Hosts button to select the required computer.
- 2 Click the  button and then click OK in the subsequent pop-up message.

Note: If you find that this doesn't work, you may need to perform a mouse calibration again.

Access mode - shared/private

Up to five users can be simultaneously logged-on (four global users plus one local or remote user) and during normal operation, all are able to see the same view of the currently selected host. If you need to perform a sensitive task that should not be viewed by other users, you can change the access mode to Private. This action blanks the viewer window for all other logged on users.

Note: For the courtesy of other users, this mode should be used sparingly. The admin user has the ability to overrule the private setting.

To change the access mode

- 1 Click one of the arrow buttons adjacent to the Shared/Private indicator.



Controls

When clicked, this button reveals a menu of options concerned with keyboard, video and mouse operation.


Single Mouse Mode

This mode is for fast network connections where the cursor response is sufficient to provide instant visual feedback on the remote screen. When enabled, the cursor is 'captured' within the viewer window until you use the 'escape' hot keys.

To quit from single mouse mode, press F8 and then P. Alternatively, enable and use the mouse button escape sequences - see [Advanced unit configuration](#) for details.

The single mouse mode does not require calibration.

Resync Mouse

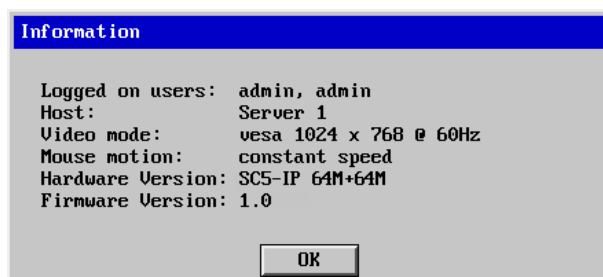
This option has the same effect as the  button on the menu bar and re-synchronises the local and remote mouse pointers.

Refresh Screen

This option refreshes the whole screen image to remove any artifacts from moved screen items. This is useful when using very low refresh rates on slow speed communication links.

Info

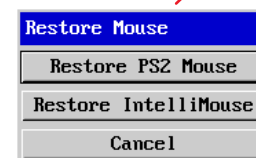
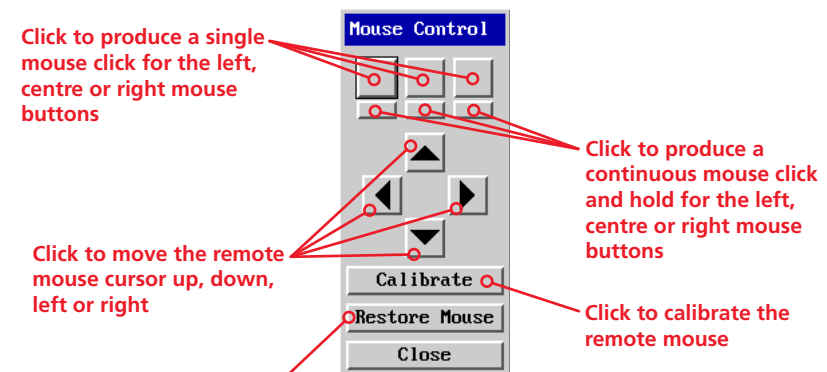
When selected, this option displays an information dialog showing the current logged on users, the current host, its video mode and its mouse motion details.



Mouse Control

This option displays a mouse control dialog and is useful when the remote cursor is failing to respond correctly to your mouse movements, even after using the Resync mouse option.

The mouse control dialog allows you to control the remote mouse cursor using a selection of buttons that you click with your local mouse.

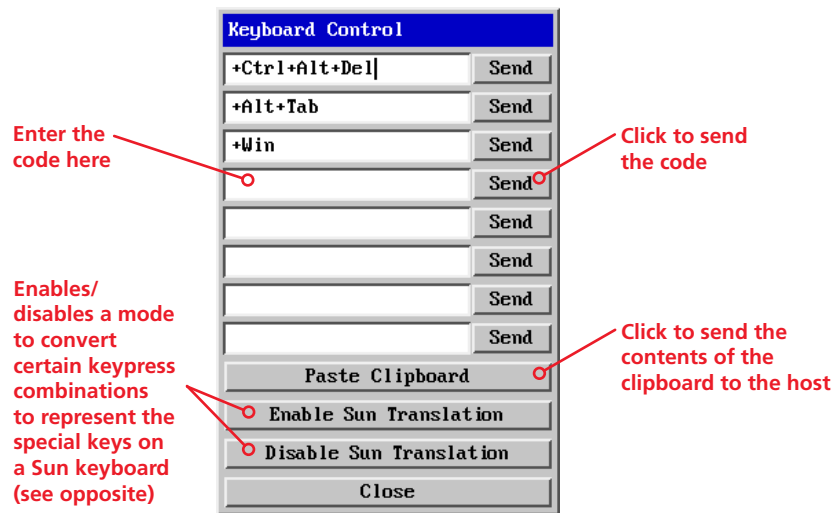


Click to display the Restore mouse dialog where you can reinstate a mouse that has failed to operate correctly.

continued

Keyboard Control

This option displays a keyboard control dialog and is useful for sending keyboard combinations (to the host) that are needed regularly or that are trapped by the SC5-IP.



When entering codes:

- + means press down the key that follows
- means release the key that follows
- +– means press down and release the key that follows
- * means wait 250ms (note: if a number immediately follows the asterisk, then the delay will equal the number, in milliseconds)

It is automatically assumed that all keys specified will be released at the end, so there is need to specify -Ctrl or -Alt if these keys are to be released together.

See [Appendix 8](#) for a list of key sequence codes that can be used.

Examples:

'Ctrl + Alt 12' would be expressed as: +Ctrl+ Alt+1–1+2

+N means press the 'N' key

+Scroll means press the Scroll lock key

+Space means press the space key

Video Settings

see [next page](#)

Enable Sun Translation

When enabled, this mode translates certain keyboard sequences to represent the special keys that are present on Sun keyboard. Use this when using a standard keyboard while connecting to a Sun system.

Notes:

The Enable/Disable status of the Sun translation mode is retained, so this mode selection only needs to be done once per host.

The mode selection only affects the host being viewed, so can be set differently for different hosts.

Standard keyboard

Right-[Ctrl] [F1]
Right-[Ctrl] [F2]
Right-[Ctrl] [F3]
Right-[Ctrl] [F4]
Right-[Ctrl] [F5]
Right-[Ctrl] [F6]
Right-[Ctrl] [F7]
Right-[Ctrl] [F8]
Right-[Ctrl] [F9]
Right-[Ctrl] [F10]
Right-[Ctrl] [1]
Right-[Ctrl] [2]
Right-[Ctrl] [3]
Right-[Ctrl] [4]
Right-[Ctrl] [H]

Sun keyboard

Stop
Again
Props
Undo
Front
Copy
Open
Paste
Find
Cut
Mute
Volume -
Volume +
Power*
Help

* Certain PS/2 keyboards have a power key which will be mapped to perform the same function for a Sun system.



INSTALLATION

CONFIGURATION

OPERATION

FURTHER INFORMATION

INDEX

Video Settings

This dialog provides access to all of the key video settings that determine image quality and link performance.

Threshold

The threshold is effectively a noise filter that differentiates between valid video signals and background noise or interference. This has the effect of reducing unnecessary video signals between the SC5-IP and the remote system, thus improving performance.

Phase

The phase setting adjusts the alignment of the host video output and the remote system video display to achieve the sharpest image.

Horizontal Position

Determines the horizontal position of the host screen image within the viewer window.

Vertical Position

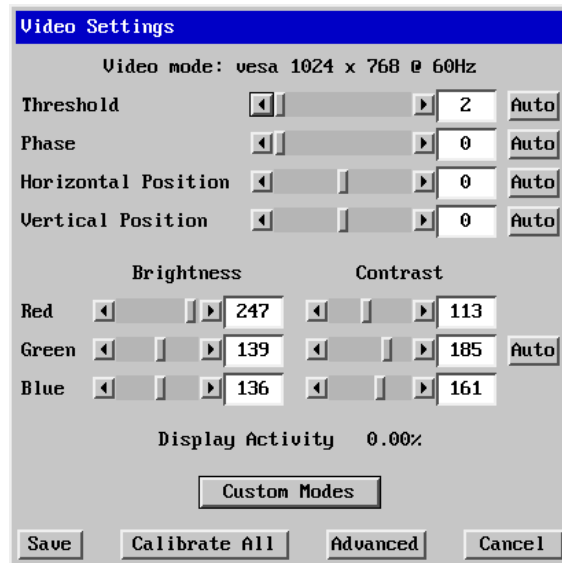
Determines the vertical position of the host screen image within the viewer window.

Custom Modes

See the next page.

Advanced

See the next page.



Brightness & Contrast

The red, green and blue constituents of the brightness and contrast can be set individually. Alternatively, use the Auto button on the right side to automatically optimise these for the current host and connection speed.

Calibrate All

Click to determine the optimum settings for all aspects of video the video connection from the host system.

Display activity

Indicates the level of video activity currently in progress.

Using automatic configurations

- Every setting can be individually subjected to an automatic configuration (click the appropriate 'Auto' button) or can also be manually adjusted.
- Use the 'Calibrate All' button to automatically determine the optimum settings for all items.

Note: Before using the 'Calibrate All' option, if possible, remove on-screen display (OSD) elements generated by the SC5-IP (such as a host name label or menu). These OSD elements use different video rates to those of the host system(s) and can affect the setting of the automatic threshold value. SC5-IP uses an improved calculation procedure to filter out the effect of these elements. However, best results are obtained when the screen contains only host system information.

Note: To maximise performance, the threshold level is automatically increased by 50% when a slow link is detected.

Note: When the SC5-IP is used with one or more other switches, the threshold needs to be higher than 32 due to the significant amounts of 'noise' that these switches introduce. The SC5-IP configuration should detect such noise and adjust the threshold accordingly.

Setting the Threshold manually

Occasionally it can be useful to manually adjust the Threshold setting, in order to achieve a setting that best suits your particular requirements.

- 1 Use the 'Calibrate All' function to ensure that all other settings are optimised.
- 2 Click the Threshold left arrow button to decrement the setting by one and observe the 'Display Activity' indicator.
- 3 Repeat step 2 until the Display Activity indicator suddenly rises to a much higher level (i.e. 50%). This will mean that you have reached the noise boundary. At this point, increment the Threshold value by 2 or 3 points to achieve an optimum setting.



INSTALLATION

CONFIGURATION

OPERATION

FURTHER INFORMATION

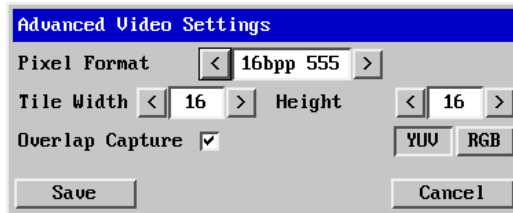
INDEX

Advanced Settings

This option contains video signal settings that do not normally need to be adjusted.

Pixel Format

Determines the colour depth and data required to represent each video pixel.



YUV / RGB

Determines the colour space used by the unit.

Overlap Capture

When enabled, the unit will begin capturing the next frame of video output from the host computer before it has fully completed processing the current frame. In most cases this produces better video performance, however, when moving large objects around the screen (such as an application window), the video image seen at the remote system may exhibit temporary artifacts as the large image moves.

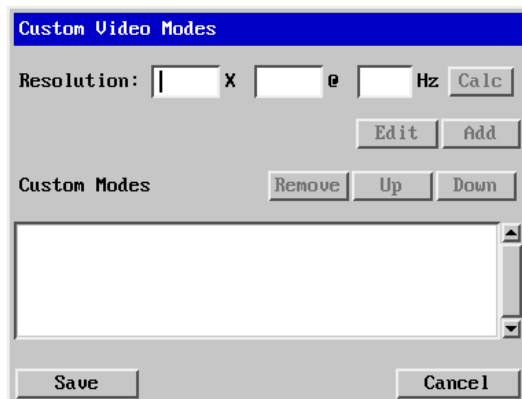
Tile Width and Height

Determines the size of the sample areas into which the source video screen is divided for examination purposes. Smaller sizes result in more areas to sample, larger areas result in more frequent screen area refreshes. 16 is considered to be the optimum size for both the width and height settings.

Custom Video Modes

This option allows you to define non-standard video resolutions and refresh rates to suit your display characteristics.

Enter the horizontal and vertical pixels counts together with the refresh rate and then click the Calc button. Then click the Add button to include the new mode within the list.



If you need to enter a port number

Usually, when you make a network connection to the SC5-IP (either using the VNC viewer or a Web browser) you simply enter the IP address, i.e. 192.168.0.3. However, if a special configuration is necessary, then you may be asked to specify a port number as well as the IP address.

[What is a port?](#)

To enter a port number in a Web browser

- 1 Enter the required IP address in the usual Address box, i.e. http://192.168.0.3
- 2 At the end of the IP address, add a single colon (:) and then enter the port number (in this example, the required port number is 8000), i.e. http://192.168.0.3:8000
- 3 Continue with the standard [Web browser instructions](#).

To enter a port number in VNC viewer

- 1 Enter the required IP address in the usual 'Server' box, i.e. http://192.168.0.3
- 2 At the end of the IP address, add two colons (::) and then enter the port number (in this example, the required port number is 8000), i.e. http://192.168.0.3::8000
- 3 Continue with the standard [VNC viewer instructions](#).

Viewer encryption settings

The web browser viewers and VNC viewers (of level 4.0b5S or higher) offer four encryption options. The resulting actions of certain options depend upon how the SC5-IP to which you are connecting is configured:

- **Always on** - This setting will ensure that the link is encrypted, regardless of the SC5-IP encryption setting.
- **Let server choose** - This setting will follow the configuration of the SC5-IP. If the SC5-IP has a preference to encrypt the link, then it will be so, otherwise the link will not be encrypted.
- **Prefer off** - This setting will configure an un-encrypted link if the SC5-IP will allow it, otherwise it will be encrypted.
- **Prefer on** - If the SC5-IP allows it, this setting will configure an encrypted link, otherwise it will be un-encrypted.

Whenever encryption does take place, the viewer will first need to create the necessary secure key before the connection process can continue.

Supported web browsers

The following web browsers have been tested and found to work correctly with SC5-IP.

Windows

- Internet Explorer 5.50 and above,
with Microsoft [Java] Virtual Machine (release 5.50).
with Java Runtime Environment 1.3 or above.

Linux

- Netscape 4.61 and above,
with Java Runtime Environment 1.1 or above.
- Opera,
with Java Runtime Environment 1.1 or above.



Further information



This chapter contains a variety of information, including the following:

- Troubleshooting and Getting assistance - this page
- Appendices
 - Appendix 1 - [Configuration menus](#)
 - Appendix 2 - [Configuration pages via viewer](#)
 - Appendix 3 - [VNC viewer connection options](#)
 - Appendix 4 - [VNC viewer window options](#)
 - Appendix 5 - [Browser viewer options](#)
 - Appendix 6 - [Addresses, masks and ports](#)
 - Appendix 7 - [Cable specifications](#)
 - Appendix 8 - [Hotkey sequence codes](#)
 - Appendix 9 - [Supported video modes](#)
- [Safety information](#)
- [Warranty](#)
- [WEEE recycling information](#)
- [End user licence agreement](#)
- [Radio frequency energy statements](#)

Troubleshooting

Global network users are unable to contact the SC5-IP

- Check that the correct address is being used by the remote users.
- Check the [network settings](#). Check that the users network address has not been excluded in the [IP access control section](#).
- If the SC5-IP is situated behind a firewall, check that the relevant ports are being allowed [through the firewall](#) and are being correctly routed.
- Check the [front panel indicators](#), the LNK indicator should be on. If the network link is a 100Mbps connection, the 100 indicator should also be on.

The remote cursor is not correctly responding to my mouse movements

- [Recalibrate the mouse](#). When doing so, ensure that the host system does not have mouse cursor trails enabled and that the top left corner of the screen is clear of application windows.

When logging on using VNC viewer, I cannot enter a username

- Either, the VNC viewer is an old version ([download a new one](#)) or only the admin user has been configured on the SC5-IP.

Getting assistance

If you are still experiencing problems after checking the list of solutions in the Troubleshooting section then we provide a number of other solutions:

- LINDY website – www.lindy.com

Check the Support section of our website for the latest solutions and driver files.

- Email
 - in the UK: postmaster@lindy.co.uk
 - in the US: usa@lindy.com
 - in Australia: info@lindy.com.au
 - in Germany: info@lindy.de
 - in France: france@lindy.fr
 - in Italy: italia@lindy.it
 - in Switzerland: info@lindy.ch
 - LINDY International: postmaster@lindy.com
- Fax
 - in the UK: **01642 765274**
 - in the US: **(256) 771-0460**
 - in Australia: **07 3262 9055**
 - in Germany: **0621-4700530**
 - in France: **03 88 20 57 74**
 - in Italy: **031 48 06 52**
 - in Switzerland: **061-3359709**
 - LINDY International: **+44 (0)1642 754029**
- Phone
 - in the UK: **01642 754000**
 - in the US: **(256) 771-0660**
 - in Australia: **07 3262 9033**
 - in Germany: **0621-470050**
 - in France: **0 825 825 111**
 - in Italy: **031 48 40 11**
 - in Switzerland: **061-3359700**
 - LINDY International: **+44 (0)1642 754020**

INSTALLATION

CONFIGURATION

OPERATION

FURTHER
INFORMATION

INDEX

Appendix 1 – Local setup menus

The SC5-IP local setup menus allow a range of settings to be made both to the installation as a whole and to parts of the system accessed by each user.

To access the local setup menus

1 First select the Select Host screen in one of two ways:

- By simultaneously pressing and then releasing **Ctrl** **Alt** **M**, or
- By pressing the middle and right buttons of a three button mouse.

If you are not already logged in, do so now. [What to do if the ADMIN password has been forgotten.](#)

2 Press **F1** to display the Main Menu.

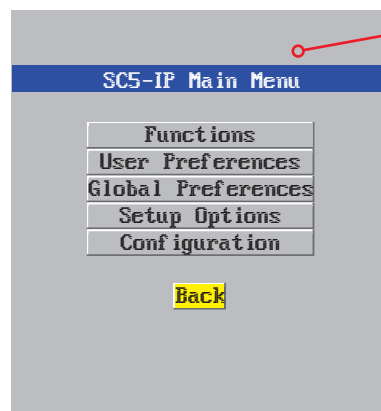
3 Use the following keys:

↑ and **↓** to highlight required options.

Space or arrow buttons to change values.

Esc to quit and save the changes.

The full set of options are only available to the Admin user. All other users will see only the Functions and User Preferences options.



The following items and menus are available in the Main Menu screen:

- [Functions](#)
- [User Preferences](#)
- [Global Preferences](#)
- [Setup Options](#)
- [Configuration](#)

Functions

The Functions menu contains a collection of procedures that affect various aspects of SC5-IP operation.

To get here

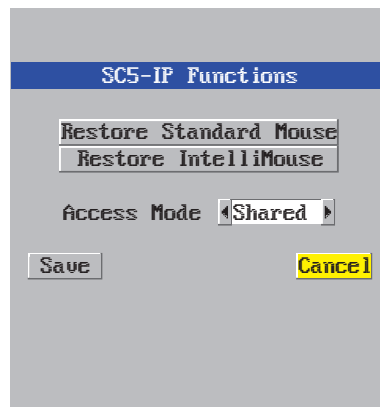
- 1 From a local keyboard, log on as a standard or 'admin' user.
- 2 Press **Ctrl** **Alt** **M** (hotkeys can change).
- 3 Press **F1** to show the Main Menu.
- 4 Select 'Functions' and press **Enter**.

Restore Standard Mouse

This option is used to resume standard mouse operation if it has ceased to operate, for instance, if it has been connected without rebooting the SC5-IP.

Restore Intellimouse

This option is used to resume Microsoft Intellimouse operation if it has ceased to operate, for instance, if it has been connected without rebooting the SC5-IP.



INSTALLATION

CONFIGURATION

OPERATION


FURTHER
INFORMATION

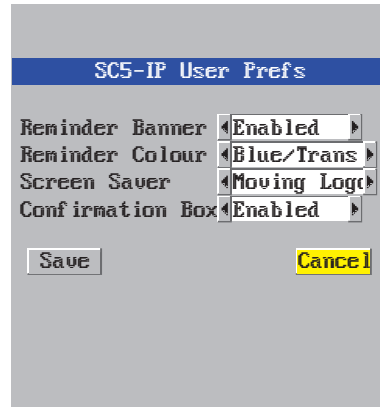
INDEX

User Preferences

The User Preferences are system operating parameters that are independently selectable for each user and affect only their screen.

To get here

- 1 From a local keyboard, log on as a standard or 'admin' user.
- 2 Press **Ctrl** **Alt** **M** (hotkeys can change).
- 3 Press **F1** to show the Main Menu.
- 4 Select 'User Preferences' and press .



Reminder Banner

Settings: Enabled, Disabled

When the reminder banner is enabled, the name of the currently selected computer will appear in a small reminder banner. This is normally located at the top of the screen in a central position but may be moved as required (see [To move the reminder banner](#)).

Reminder Colour

Settings: Blue/White, Blue/Trans, Pink/Trans, White/Trans, White/Red

You can select the colour of the reminder banner. The Blue/Trans, Pink/Trans and White/Trans use a transparent background.

Screen Saver

Settings: Blank, Moving Logo

You can select the type of screen saver. If you select BLANK then the screen will blank completely. If you select Moving Logo then a small logo will bounce around the screen.

Confirmation Box

Settings: Disabled, Enabled

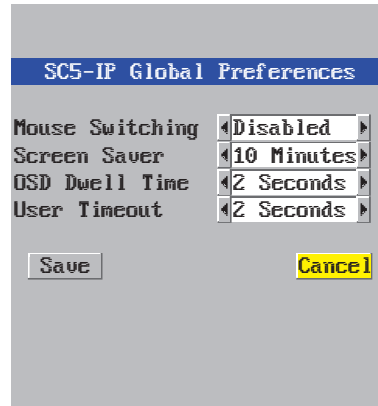
When enabled, a confirmation box is displayed on screen for three seconds after a computer is selected. The confirmation box indicates the current user port and user name, the selected computer and the connection status.

Global Preferences

Global preferences are available only to the Admin user and allow settings to be made that affect all users attached to the SC5-IP.

To get here

- 1 From a local keyboard, log on as the 'admin' user.
- 2 Press **Ctrl** **Alt** **M** (hotkeys can change).
- 3 Press **F1** to show the Main Menu.
- 4 Select 'Global Preferences' and press **Enter**.



Mouse Switching

Settings: Enabled, Disabled

The computer channel can be switched using a three button mouse or IntelliMouse. Pressing the central button or wheel button together with the left hand mouse button will cause the SC5-IP to switch to the next available computer.

When mouse switching is enabled, you can still use the middle button on its own to control applications. Only when its pressed with the left or right button is it interpreted by mouse switching, otherwise it is passed on to the host application. The rotation action of an IntelliMouse wheel is not affected and is always available to the computer application.

Screen Saver

Settings: Disabled; 2, 5, 10, 15 or 20 Minutes

The SC5-IP can be set to blank the screen after no keyboard or mouse activity has been detected for a selected timeout period. If preferred, the user can blank the screen manually by selecting channel '0' using the keyboard hotkeys or by pressing ESC from the login screen.

OSD Dwell Time

Settings: 1, 2, 3, 5, 10 Seconds

After a successful computer channel change the SC5-IP will display a confirmation message for a few seconds. The length of time that this confirmation message dwells on the screen may be changed.

User Timeout

Settings: 1, 2, 5, 10, 30 Seconds, 1, 5, 10 Minutes

When no keyboard or mouse data has been received from an active user port for the user timeout period, the SC5-IP will relinquish the control of that user port in order to allow other users to access the host computer. The new port then becomes the active port until it too times out. To avoid confusion between users it is desirable to set the timeout period to be sufficiently long so that user's work is not needlessly interrupted by other users and sufficiently short to ensure good overall system efficiency.

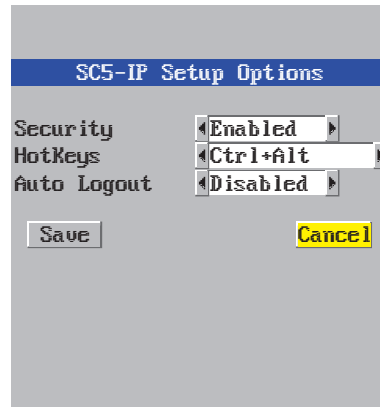


Setup Options

Setup options are available only to the Admin user.

To get here

- 1 From a local keyboard, log on as the 'admin' user.
- 2 Press **Ctrl** **Alt** **M** (hotkeys can change).
- 3 Press **F1** to show the Main Menu.
- 4 Select 'Setup Options' and press **Enter**.



Security

Settings: Disabled, Enabled

With security disabled there is no requirement for users to log-in to the system. All users have full access to all the connected computers and full administration rights. With security enabled, users are required to log-in to the SC5-IP. Each user is allocated access rights to computers by the system administrator and they are only able to see the computers that they have access to on their on-screen menu.

Hotkeys

Settings: Ctrl+Alt, Ctrl+Shift, Alt+Shift, Alt Gr, Left+Right Alt, Left Ctrl+Alt, Right Ctrl+Alt

The keyboard hotkeys are special combinations of keys that, when used together with certain keyboard "command keys", perform special SC5-IP functions. For example, pressing the hotkeys together with the "M" key will cause the on-screen menu to be displayed on your monitor. Other hotkey combinations allow you to query which computer you are connected to and to move the on-screen menu around the screen. You can also use the hotkeys together with the port number to select a particular connected computer.

Auto Logout

Settings: Disabled, Enabled

The SC5-IP enables you to restrict access to your computers on a login basis. If a user forgets to logout when they have finished accessing the SC5-IP then the user console may unintentionally be left with full access to all the computers. The SC5-IP can be set to automatically logout unattended user consoles when the screen saver kicks in. This reduces the risk of security problems by preventing user consoles remaining in a permanent "logged-in" state when there is no keyboard or mouse activity. The automatic logout feature is only enabled when the screen saver feature is active (i.e. not disabled).



INSTALLATION

CONFIGURATION

OPERATION

FURTHER
INFORMATION

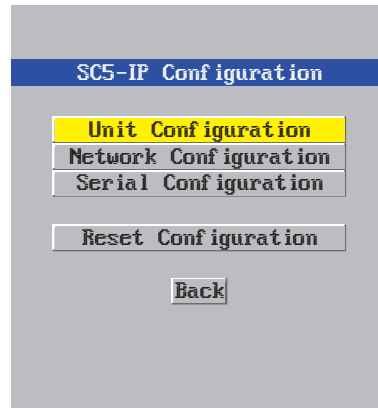
INDEX

Configuration

Available only to the Admin user, the configuration section menu allows you to determine settings that relate directly to the global (IP) user aspects of the unit.

To get here

- 1 From a local keyboard, log on as the 'admin' user.
- 2 Press **Ctrl** **Alt** **M** (hotkeys can change).
- 3 Press **F1** to show the Main Menu.
- 4 Select 'Configuration' and press **Enter**.



- [Unit Configuration](#)
IP admin password, encryption settings, etc.
- [Network Configuration](#)
IP address, net mask, VNC port, etc.
- [Serial Configuration](#)
Options port usage and Baud rate.
- [Reset Configuration](#)
Completely resets the SC5-IP unit.



INSTALLATION

CONFIGURATION

OPERATION

FURTHER
INFORMATION

INDEX

Unit Configuration

This page provides access to a selection of both basic and fundamental settings for the SC5-IP.

To get here

- 1 From a local keyboard, log on as the 'admin' user.
- 2 Press **Ctrl** **Alt** **M** (hotkeys can change).
- 3 Press **F1** to show the Main Menu.
- 4 Select 'Configuration' and press **Enter**.
- 5 Select 'Unit Configuration' and press **Enter**.

The screenshot shows the 'SC5-IP Unit Config' menu. The settings are as follows:

Setting	Value
Hardware	SC5-IP 64M+64M
Firmware	1.00
Keybd Layout	UK
Admin Passwd	[Redacted]
Unit Name	LINDY SC5-IP
Time	00:59:52
Date	15 Jul 2008
Encryption	Always On

At the bottom of the menu are two buttons: 'Save' and 'Cancel'.

Hardware

Indicates the version of the internal circuitry.

Firmware

Indicates the version of the internal software.

Keybd Layout

Use the arrow buttons to match the keyboard layout expected by the host system.

Admin Passwd

Enter the password that will be used to gain administrator access to the SC5-IP. There can only be one admin user and only that user is given access to the configuration menus. The admin password background will be red until a reasonably secure password has been entered, although this is only advisory as any password or no password may be entered.

Unit Name

The name entered here will be displayed on the local menus and the remote VNC/browser windows.

Time and Date

Use the left and right arrow keys to select the correct time and date. The time entry uses the 24 hour clock notation. The internal real time clock will continue to run for roughly one week without power to the unit, after that it will be lost and require resetting. Use the up and down arrow keys to move between each of the sections within the time and date entries.

Encryption

Three options are available: Always on, prefer off, prefer on. The one to choose depends on the specific details of your installation - see [Encryption settings](#) for details. The use of encryption imposes a slight performance overhead of roughly 10% but is highly secure against third party intrusion.



INSTALLATION

CONFIGURATION

OPERATION

FURTHER
INFORMATION

INDEX

Network Configuration

This page allows you to configure the various aspects of the IP port and its relationship with the local network.

To get here

- 1 From a local keyboard, log on as the 'admin' user.
- 2 Press **Ctrl** **Alt** **M** (hotkeys can change).
- 3 Press **F1** to show the Main Menu.
- 4 Select 'Configuration' and press **↓**.
- 5 Select 'Network Configuration' & press **↓**.

SC5-IP Network Config

MAC Address	66:CB:23:00:00:22
Use DHCP	No
IP Address	192.168.1.42
Net Mask	255.255.255.0
Gateway	
VNC Port	5900
HTTP Port	80

Clear IP Access Control

Save Cancel

MAC Address

Media Access Control address – this is the unique and unchangeable code that was hard coded within your SC5-IP unit when it was built. It consists of six 2-digit hexadecimal (base 16) numbers separated by colons. A section of the MAC address identifies the manufacturer, while the remainder is effectively the unique electronic serial number of your particular unit.

Use DHCP

DHCP stands for 'Dynamic Host Configuration Protocol'. Its function is particularly useful when connecting to medium size or larger networks, such as the Internet. When this option is selected, your SC5-IP will attempt to locate a DHCP server on the network. If such a server is located, it will supply three things to the SC5-IP: an IP address, an IP network mask (also known as a Subnet mask) and a Gateway address. These are not usually granted permanently, but on a 'lease' basis for a fixed amount of time or for as long as the SC5-IP remains connected and switched on. [Discover allocations.](#)

IP Address

This is the identity of the SC5-IP within a network. The IP address can be thought of as the telephone number of the SC5-IP. Unlike the MAC address, the IP address can be altered to suit the network to which it is connected. It can either be entered manually or configured automatically using the DHCP option. When the DHCP option is enabled, this entry is unavailable. See [IP addresses.](#)

Net Mask

Also often called the 'subnet-mask', this value is used alongside the IP address to help define a smaller collection (or subnet) of devices on a network. In this way a distinction is made between locally connected devices and ones that are reachable elsewhere, such as on the wider Internet. This process helps to reduce overall traffic on the network and hence speed up connections in general. See [Net masks.](#)

Gateway

This is the address of the device that links the local network (to which the SC5-IP is connected) to another network such as the Internet. Usually this is a network switch or router and it will be used whenever a device to be contacted lies outside the local network.

VNC Port

This is the logical link through which communications with a remote VNC viewer will be channelled (see [What is a port?](#)). The default setting is 5900 which is a widely recognised port number for use by VNC software. However, in certain circumstances it may be advantageous to alter this number - see [Security issues with ports](#) for more details.

Note: The VNC port and HTTP port can be set to the same port number in order to simplify router and firewall configuration. If this is done then the SC5-IP will "listen" for both types of traffic on the single port.

HTTP Port

This is the logical link through which communications with a remote web browser will be channelled. The default setting of 80 is an established standard for web (HTTP – HyperText Transfer Protocol) traffic though this can be changed to suit your local network requirements.

Clear IP Access Control

This option removes all entries from the IP access control feature within the SC5-IP. The IP access control feature (configurable by a global admin user) allows certain network address ranges to be denied access to the SC5-IP. If set incorrectly, it is possible to exclude all network users and so this option provides an emergency recovery point.



INSTALLATION

CONFIGURATION

OPERATION

FURTHER INFORMATION

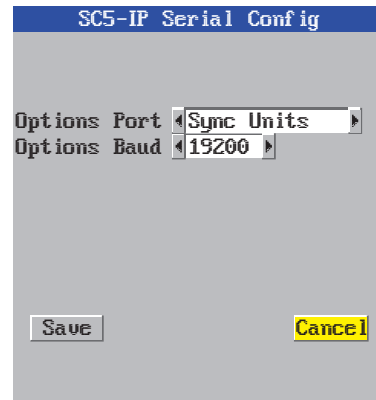
INDEX

Serial Configuration

This page allows you to configure the OPTIONS serial port located at the rear of the SC5-IP.

To get here

- 1 From a local keyboard, log on as the 'admin' user.
- 2 Press **Ctrl** **Alt** **M** (hotkeys can change).
- 3 Press **F1** to show the Main Menu.
- 4 Select 'Configuration' and press **Enter**.
- 5 Select 'Serial Configuration' & press **Enter**.



SC5-IP Serial Config

Options Port **Sync Units**

Options Baud **19200**

Save **Cancel**

Options Port

Settings: Sync Units

Determines the use fro the RS232 serial OPTIONS port at the rear of the unit.
This is fixed at Sync Units.

Options Baud

This option determines the speed of the RS232 serial OPTIONS port. This setting is fixed at 19200.



INSTALLATION

CONFIGURATION

OPERATION

FURTHER
INFORMATION

INDEX

Reset Configuration

This option allows you to completely reset the IP portion of the SC5-IP unit.

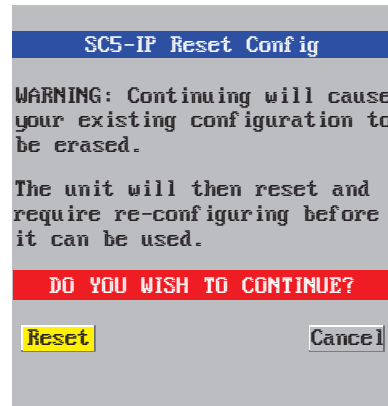
WARNING: This process will remove all network settings and return the unit to use its original state. A complete reconfiguration will be required before the IP features of the unit can be used.

To get here

- 1 From a local keyboard, log on as the 'admin' user.
- 2 Press **Ctrl** **Alt** **M** (hotkeys can change).
- 3 Press **F1** to show the Main Menu.
- 4 Select 'Configuration' and press **↓**.
- 5 Select 'Reset Configuration' and press **↓**.

To reset the SC5-IP configuration

- 1 From a local or remote (not accessible from a global keyboard), log on as the 'admin' user.
- 2 Press **Ctrl** **Alt** **M** (hotkeys can change).
- 3 Press **F1** to select 'More menus'.
- 4 Select 'Configuration'.
- 5 Select 'Reset Configuration'.
- 6 Highlight the 'Reset' option and press **↓**.
- 7 After a short period, you should see the first of five initial configuration screens. See [Initial configuration](#) for details.

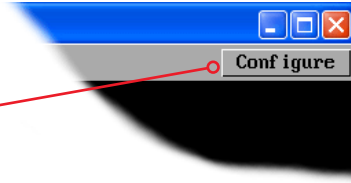


Appendix 2 - Configuration pages via viewer

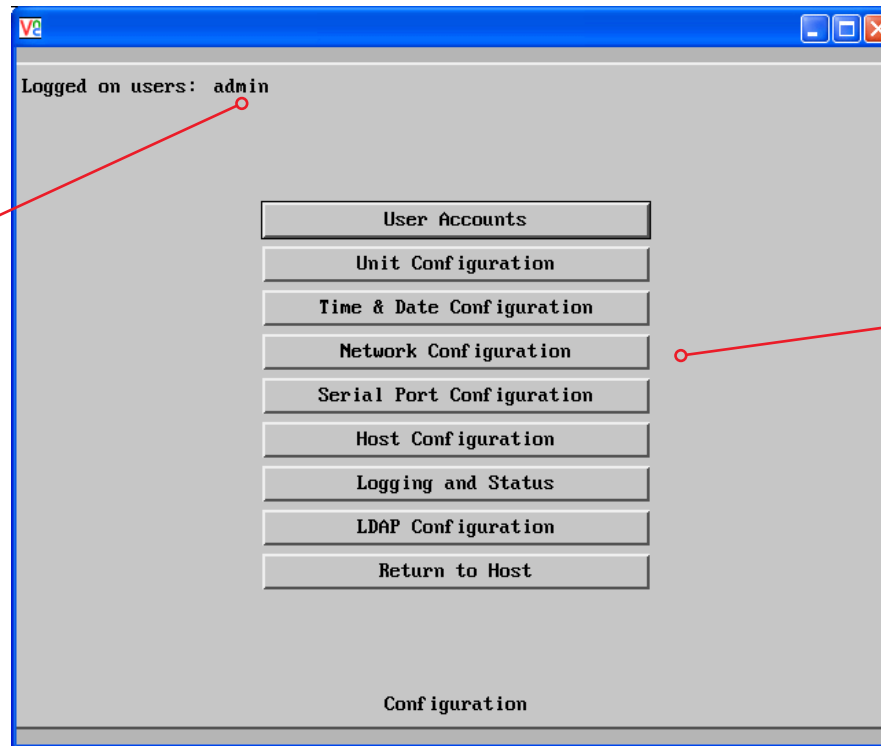
This section covers the configuration pages that are available to global admin users, using either the VNC viewer or the browser methods of access.

To access the remote configuration pages

- 1 Make a [global connection](#) to the SC5-IP unit and login as the admin user.
- 2 Once logged in, click the Configure button in the top right corner of the window.



Main configuration page



Logged on users

Indicates the current users irrespective of whether they are connected locally or via a network.

Click the required option

- [User Accounts](#)
- [Unit Configuration](#)
- [Time & Date Configuration](#)
- [Network Configuration](#)
- [Serial Port Configuration](#)
- [Host Configuration](#)
- [Logging and Status](#)
- [LDAP Configuration](#)

User accounts

This page allows you to manage up to sixteen separate accounts.

The first of the sixteen accounts is the admin account and is the only account with access rights to the configuration menus. The user name and access rights are fixed for the admin account, the only change possible for this account is the password.

There are fifteen user account positions.

User Name	Password	Confirm Pwd	Local	Remote
admin			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
user1	*****	*****	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>

To create a new user account

- 1 Enter the required User Name to activate that position (the Password and access tick box positions will become editable).
- 2 Optionally enter a password for the user account.
- 3 Tick/untick the Local and Remote options that are appropriate to the user.
- 4 Click the Save button to register your changes.

To get here

- 1 Using VNC viewer or a browser, log on as the 'admin' user.
- 2 Click the 'Configure' button in the top right corner.
- 3 Click the 'User Accounts' option.

User Name

All user names must consist of lower case characters or numbers only. No symbols or upper case characters are permissible. The user name can be between 1 and 16 characters in length.

Password

Passwords are case sensitive and can include certain keyboard symbols. The password can be between 1 and 16 characters in length. It is important to note, however, that the password background remains shaded in amber while the SC5-IP considers your entered password to be too easy to guess. A suitable password is best constructed using a mixture of more than 6 letters, numbers and punctuation characters.

Confirm Pwd

Re-enter your password here to confirm that it is correct.

Local

When ticked, the selected user can gain access using the local KVM console directly connected to the SC5-IP unit.

Remote

When ticked, the selected user can gain access via an IP network link, such as a local intranet or the wider Internet (depending on how the SC5-IP is connected).



INSTALLATION

CONFIGURATION

OPERATION

FURTHER
INFORMATION

INDEX

Unit configuration

This page provides access to a selection of both basic and advanced settings for the SC5-IP. Many of the settings displayed here are also accessible through the on-screen menu.

The screenshot shows a window titled 'Unit Configuration' with a blue title bar. At the top, it says 'Logged on users: admin'. Below this, there are several settings:

- Hardware Version:** SC5-IP 64M+64M
- Firmware Version:** 1.00
- Host Keyboard Layout:** A dropdown menu showing 'UK' with left and right arrow buttons.
- Admin Password:** A text input field with a red background, indicating it is required or invalid.
- Unit Name:** A text input field.
- Menu Bar Toggle Hot Key:** A dropdown menu showing 'None' with left and right arrow buttons.
- Display Menu Bar for New Connections:** A checkbox that is checked.
- Encryption:** A dropdown menu showing 'Prefer Off' with left and right arrow buttons.

Below these settings is a button labeled 'Advanced Unit Configuration'. At the bottom of the window are three buttons: 'Save', 'Unit Configuration', and 'Cancel'.

Hardware Version

Indicates the version of the electronic circuitry within the SC5-IP unit.

Firmware Version

Indicates the version of the internal software within the SC5-IP flash memory. This may be updated using the [flash upgrade procedure](#).

Host Keyboard Layout

Use the arrow buttons to match the keyboard layout expected by the host system.

Admin Password

Enter the password that will be used to gain administrator access to the SC5-IP. There can only be one admin user and only that user is given access to the configuration menus.

To get here

- 1 Using VNC viewer or a browser, log on as the 'admin' user.
- 2 Click the 'Configure' button in the top right corner.
- 3 Click the 'Unit Configuration' option.

Unit Name

The name entered here will be displayed on the local menus and the remote VNC viewer/browser windows.

Menu Bar Toggle Hot Key

Determines the function key that can be used to display/hide the menu bar within the VNC screen.

Encryption

Three options are available: Always on, prefer off, prefer on. The one to choose depends on the specific details of your installation - see [Encryption settings](#) for details. The use of encryption imposes a slight performance overhead of roughly 10% but is highly secure against third party intrusion.

[Advanced Unit Configuration](#)



INSTALLATION

CONFIGURATION

OPERATION

FURTHER
INFORMATION

INDEX

Advanced unit configuration

Click this button to display advanced options that do not normally require alteration.

To get here

- 1 Using VNC viewer or a browser, log on as the 'admin' user.
- 2 Click the 'Configure' button in the top right corner.
- 3 Click the 'Unit Configuration' option.
- 4 Click the 'Advanced Unit Configuration' option.

Force VNC Protocol 3.3

IMPORTANT: The use of this option is not recommended. Protocol 3.3 is a legacy version that does not offer any encryption.

Idle Timeout

Determines the period of inactivity on a global connection before the user is logged out. The idle timeout period can be set to any time span, expressed in minutes.

Note: The [Screensaver](#) option serves a similar purpose for local connections.

Protocol Timeout

Sets the time period by which responses should have been received to outgoing data packets. If the stated period is exceeded, then a connection is considered lost and terminated.

Mouse Latency Allowance

This option is used during calibration to account for latency delays (caused as signals pass through a device) introduced by some KVM switches from alternative manufacturers.

During calibration, the SC5-IP waits for 40ms after each mouse movement before sampling the next. If a KVM device adds a significant delay to the flow of data, the calibration process can be lengthened or may fail entirely. The value entered here is added to (or subtracted from) the default 40ms sampling time.

Note: You can enter negative values (down to -40) in order to speed up the calibration process when using fast KVM switches. Use this option with caution as it can adversely affect the calibration process.

Mouse Rate

Defines the rate at which mouse movement data are transmitted to the system. The default option is 20ms, which equates to 50 mouse events per second. This default rate can prove too fast when passed through certain connected KVM switches from alternative manufacturers. In such cases, data are discarded causing the local and remote mouse pointers to drift apart. If this effect is encountered, increase the mouse rate to around 30ms (data are then sent at a slower rate of 33 times per second).

Background Refresh Rate

Use the arrow keys to alter the refresh rate for screen images via remote links. This allows you to tailor the screen refresh to suit the network or modem connection speeds. The options are: Slow, Medium, Fast or Disabled. When the disabled option is selected, the remote users will need to manually refresh the screen.

Note: When a low connection speed is detected, the background refresh is automatically disabled, regardless of the settings of this option.

Single Mouse Mode Mouse Switch

Allows you to select the mouse button combination that can be used to exit from single mouse mode (when active).

Behaviour for admin connections when limit reached

Determines what should occur when four global connections already exist and a fifth, administrator connection attempt is made. Options are: *Replace oldest connection*, *Replace newest connection* and *Don't replace*. Only non-administrator connections can be terminated in this way.

Use VESA GTF

When ticked, the VESA Generalized Timing Formula will be used to help determine the correct input video resolution and timing details. See [Appendix 9](#) for a list of all supported video modes.

Upgrade firmware

Places the unit into upgrade mode. See [Upgrading SC5-IP models](#).



INSTALLATION

CONFIGURATION

OPERATION

FURTHER
INFORMATION

INDEX

Time & date configuration

This page allows you to configure all aspects relating to time and date within the SC5-IP unit.

Logged on users: admin

Time And Date

Timezone specifier (e.g. EST5)

Use NTP

NTP Server IP address

Set Time from NTP Server

Save Time & Date Configuration Cancel

Time and Date

Use the arrow buttons to set the correct current time.

Use NTP

When this option is selected, the SC5-IP will synchronise its internal clocks using information from the (Network Time Protocol) server listed in the *NTP Server IP address* field.

NTP Server IP address

Optionally enter the IP address for a known Network Time Protocol server.

Set Time from NTP Server

Click to immediately use the time and date information from the listed NTP server.

Timezone specifier

Optionally enter a recognised timezone specifier related to the current position of the SC5-IP unit. When an NTP server is used, the specifier will be used to provide the correct real time.

The timezone specifier takes the following form:

std offset dst [offset], start[/ time], end[/ time]

The *std* and *offset* specify the standard time zone, such as GMT and 0, or CET and -1, or EST and 5, respectively.

The *dst* string and *[offset]* specify the name and offset for the corresponding Daylight Saving Time zone; if the *offset* is omitted, it defaults to one hour ahead of standard time.

The remainder of the specification describes when Daylight Saving Time is in effect. The *start* field is when Daylight Saving Time goes into effect and the *end* field is when the change is made back to standard time. The most common format used for the daylight saving time is: *mm.w.d*

Where: *m* specifies the month and must be between 1 and 12. The day *d* must be between 0 (Sunday) and 6. The week *w* must be between 1 and 5; week 1 is the first week in which day *d* occurs, and week 5 specifies the last *d* day in the month.

The *time* fields specify when, in the local time currently in effect, the change to the other time occurs. If omitted, the default is 02:00:00.

Typical examples are:

UK:	GMT0BST,M3.5.0/1,M10.5.0/2
Central Europe:	CET-1CEST,M3.5.0/2,M10.5.0/3
US Eastern:	EST5EDT,M3.2.0/2,M11.1.0/2
US Pacific:	PST5PDT,M3.2.0/2,M11.1.0/2

For further details

- For details of timezone specifier formats, please refer to: http://www.gnu.org/software/libc/manual/html_node/TZ-Variable.html
- For details of the Network Time Protocol (main RFC number: 1305; the SNTP subset used as the basis for the SC5-IP: 4330) <http://www.ietf.org/rfc.html>



INSTALLATION

CONFIGURATION

OPERATION

FURTHER INFORMATION

INDEX

Network configuration

This page allows you to configure the various aspects of the IP port and its relationship with the local network.

Logged on users: admin

MAC address: 00:1E:ED:00:00:02

Use DHCP ☐

IP Address 192.168.0.6

IP Network Mask 255.255.255.0

IP Gateway

UNC Port 5900

HTTP Port (0=disabled) 80

IP Access Control

Add Remove Up Down Edit

+0.0.0.0/0.0.0.0

Save Network Configuration Cancel

MAC address

Media Access Control address – this is the unique and unchangeable code that was hard coded within your SC5-IP unit when it was built. It consists of six 2-digit hexadecimal (base 16) numbers separated by colons. A section of the MAC address identifies the manufacturer, while the remainder is effectively the unique electronic serial number of your particular unit.

Use DHCP

DHCP is an acronym for 'Dynamic Host Configuration Protocol'. Its function is particularly useful when connecting to medium size or larger networks, such as the Internet. When this option is selected, your SC5-IP will attempt to locate a DHCP server on the network. If such a server is located, it will supply three things to the SC5-IP: an IP address, an IP network mask (also known as a Subnet mask) and a Gateway address. These are not usually granted permanently, but on a 'lease' basis for a fixed amount of time or for as long as the SC5-IP remains connected and switched on. [Discover allocations](#).

To get here

- 1 Using VNC viewer or a browser, log on as the 'admin' user.
- 2 Click the 'Configure' button in the top right corner.
- 3 Click the 'Network Configuration' option.

IP Address

This is the identity of the SC5-IP within a network. The [IP address](#) can be thought of as the telephone number of the SC5-IP. Unlike the MAC address, the IP address can be altered to suit the network to which it is connected. It can either be entered manually or configured automatically using the DHCP option. When the DHCP option is enabled, this entry is greyed out.

IP Network Mask

Also often called the [subnet-mask](#), this value is used alongside the IP address to help define a smaller collection (or subnet) of devices on a network. In this way a distinction is made between locally connected devices and ones that are reachable elsewhere, such as on the wider Internet. This process helps to reduce overall traffic on the network and hence speed up connections in general.

IP Gateway

This is the address of the device that links the local network (to which the SC5-IP is connected) to another network such as the wider Internet. Usually the actual gateway is a network switch or router and it will be used whenever a required address lies outside the current network.

VNC Port

This is the logical link through which communications with a remote VNC viewer will be channelled (see [What is a port?](#)). The default setting is 5900 which is a widely recognised port number for use by VNC software. However, in certain circumstances it may be advantageous to alter this number - see 'Security issues with ports' for more details.

HTTP Port

This is the logical link through which communications with a remote web browser will be channelled (see [What is a port?](#)). The default setting of 80 is an established standard for web (HTTP – HyperText Transfer Protocol) traffic though this can be changed to suit your local network requirements.

IP Access Control

This section allows you to optionally specify ranges of addresses which will or won't be granted access to the SC5-IP. If this option is left unchanged, then the default entry of '+0.0.0.0/0.0.0.0' ensures that access from all IP addresses will be permitted. See [Setting IP access control](#) for details.

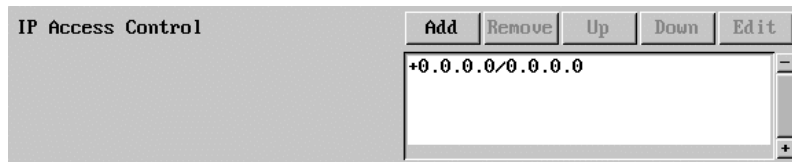


Setting IP access control

The golden rule with this feature is 'Include before you exclude' or to put it another way 'Arrange *allowed* addresses in the list *before* the *denied* addresses'.

This is because the positions of entries in the list are vitally important. Once a range of addresses is denied access, it is not possible to make exceptions for particular addresses within that range. For instance, if the range of addresses from A to F are denied access first, then the address C could not be granted access lower down the list. Address C needs to be placed in the list before the denied range.

IMPORTANT: This feature should be configured with extreme caution as it is possible to deny access to everyone. If such an error occurs, see [Clearing IP access control](#) for details about how to regain access.



In the list, access control addresses prefixed by '+' are allow entries while those prefixed by '-' are deny entries.

To get here

- 1 Using VNC viewer or a browser, log on as the 'admin' user.
- 2 Click the 'Configure' button in the top right corner.
- 3 Click the 'Network Configuration' option.

To define a new IP access control entry

- 1 Click the Add button to display a popup dialog:

Network/Address

Enter the network address that is to be allowed or denied access. If a range of addresses is being specified then specify any one of the addresses within the range and use the Mask entry to indicate the size of the range.

Mask

Enter an IP network mask that indicates the range of addresses that are to be allowed or denied access. For instance, if only a single specified IP address were to be required, the mask entry would be 255.255.255.255 in order to specify a single location. See [Calculating the mask for IP access control](#) for details.

Access

Use the arrow buttons to select either 'Allow' or 'Deny' as appropriate.

- 2 Enter the base [network address](#), the [mask](#) and select the appropriate access setting.
- 3 Click the OK button.

To reorder access control entries

IMPORTANT: When reordering, ensure that any specific allowed addresses are listed higher in the list than any denied addresses. Take care not to invoke any deny access settings that would exclude valid users.

- 1 In the access control list, click on the entry to be moved.
- 2 Click the Up or Down buttons as appropriate.

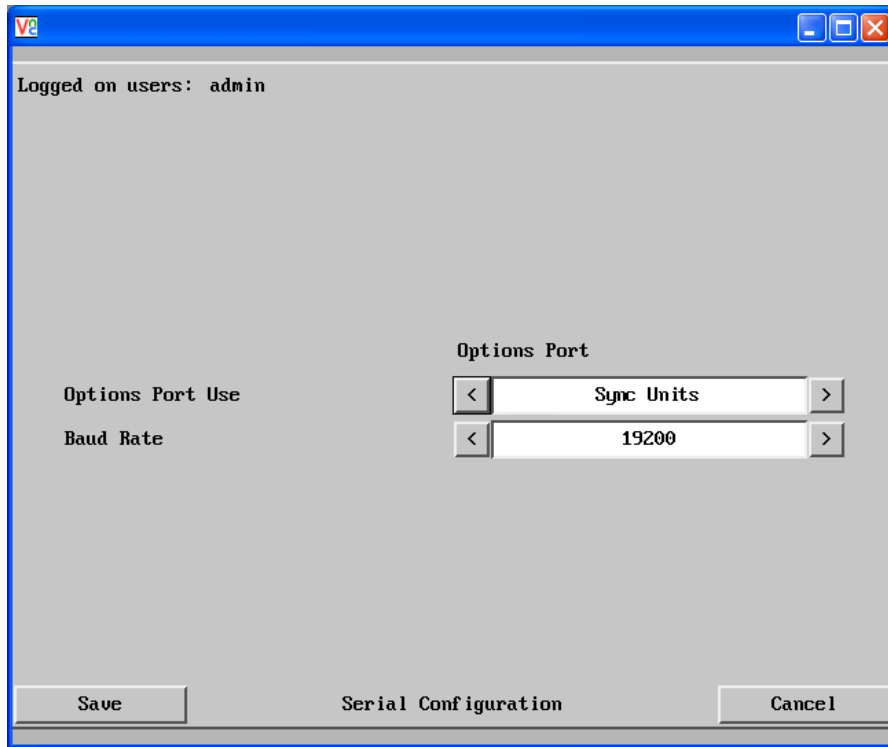
To edit/remove access control entries

- 1 In the access control list, click on the appropriate entry.
- 2 Click either the Edit or Remove button as appropriate.



Serial port configuration

This page provides all access to settings concerned with the serial OPTIONS port that is situated at the rear of the SC5-IP unit.



The screenshot shows a VNC window titled 'Serial Configuration'. At the top left, it says 'Logged on users: admin'. The main area contains two settings: 'Options Port Use' set to 'Sync Units' and 'Baud Rate' set to '19200'. Both settings are in dropdown menus with left and right arrow buttons. At the bottom, there are 'Save' and 'Cancel' buttons, and the title 'Serial Configuration' is centered.

To get here

- 1 Using VNC viewer or a browser, log on as the 'admin' user.
- 2 Click the 'Configure' button in the top right corner.
- 3 Click the 'Serial Port Configuration' option.

Options Port Use

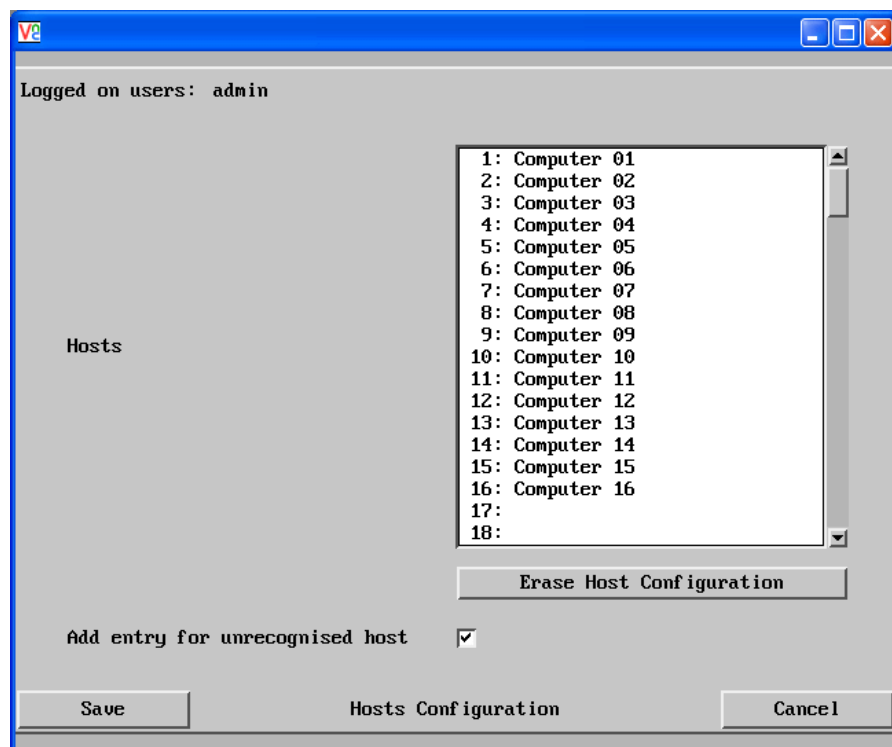
This option determines the use for the RS232 serial OPTIONS port at the rear of the unit. This option is fixed at Sync Units.

Baud Rate

This option determines the speed of the RS232 serial OPTIONS port. The other communication settings are fixed as: No parity, 8 bit word, 1 stop bit.

Host configuration

This page provides the opportunity to configure various details for each of the host systems that may be connected to the SC5-IP. Each entry can be configured with a name, the permitted users and the hot key combinations required to switch to it.



Add entry for unrecognised host

When selected, any systems visited that are not specified in the Hosts list, will be added to the list. It is useful to tick this option when cascaded systems are first added to the installation.

Erase Host Configuration

Removes all hosts from the list.

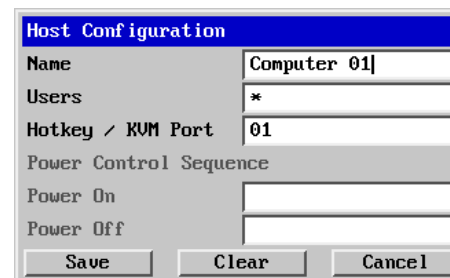
To get here

- 1 Using VNC viewer or a browser, log on as the 'admin' user.
- 2 Click the 'Configure' button in the top right corner.
- 3 Click the 'Host Configuration' option.

To create a new host entry

- 1 Click one of the host entries to reveal a Host configuration dialog.

Note: Host computers connected to a cascaded SC5 unit will appear within the list (providing the 'Add entry for unrecognised host' option is ticked) and you can easily discern them from directly connected systems because their addresses will be four digits, rather than two.



Name

Enter the name that will be displayed in the viewer window when you click the Host button.

Users

Select the users that will be permitted to connect to this host. Either enter * to allow all users or a list of users separated by commas (e.g. admin, nigel, preben, steve).

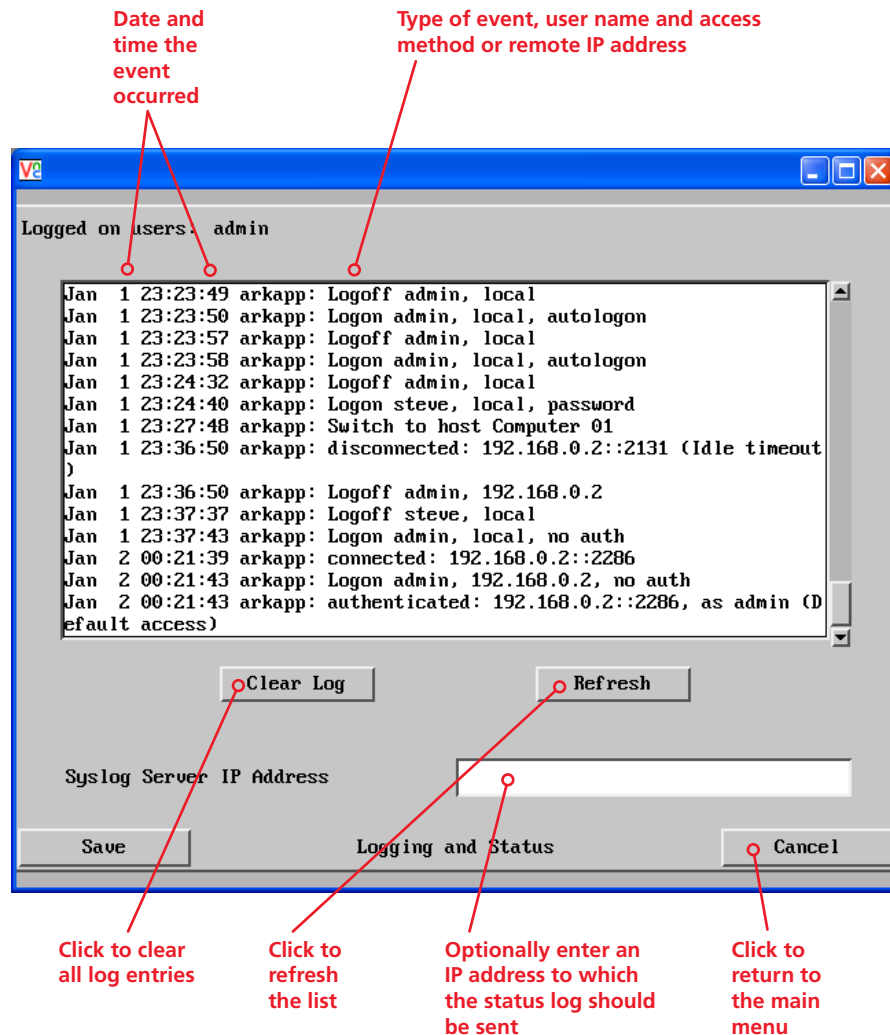
Hotkey / KVM Port

Declare the numeric sequence that is pressed together with the hotkeys (usually Ctrl + Alt) to select this host system, which is the same value as the KVM port number.

- 2 Enter the required information in each field.
- 3 Click the OK button.

Logging and status

This screen provides various details about the user activity on the SC5-IP unit.



To copy and paste the log

You can copy the information listed within the log and paste it into another application.

- 1 While viewing the log screen, press Ctrl and C, to copy the data into the clipboard.
- 2 In a text application (i.e. Word, WordPad, Notepad) press Ctrl and V, or right mouse click and 'Paste'.

Syslog Server IP Address

Logging information can optionally be sent, as it occurs, to a separate system using the standard Syslog protocol. Enter the IP address of a suitable system in the field provided.

For further details

- For details of the Syslog protocol (RFC number: 3164) <http://www.ietf.org/rfc.html>

To get here

- 1 Using VNC viewer or a browser, log on as the 'admin' user.
- 2 Click the 'Configure' button in the top right corner.
- 3 Click the 'Logging and Status' option.

LDAP configuration

The SC5-IP can optionally use the industry standard LDAP (Lightweight Directory Access Protocol) to allow user authentication to occur in conjunction with an externally held database. This screen allows you to configure details related to the creation of an LDAP link to an external directory service, such as an Active Directory server.

Logged on users: admin

Use LDAP ☒

Host Address

Host Port

Base DN

User field

Anonymous Bind ☐

Save LDAP Configuration Cancel

To get here

- 1 Using VNC viewer or a browser, log on as the 'admin' user.
- 2 Click the 'Configure' button in the top right corner.
- 3 Click the 'LDAP Configuration' option.

Use LDAP

Tick this option to enable the Lightweight Directory Access Protocol features of the unit.

Host Address

Enter the IP address of the LDAP server that holds the required directory service.

Host Port

The standard port address for LDAP links is 389 and this should not need to be changed unless special circumstances exist.

Base DN

This field allows you to enter a Distinguished Name for the unit which will be used as the main identifier during (non-anonymous bind) LDAP sessions. An example Base DN value might be: "dc=LINDYSC5IP,dc=com"

User field

Enter the LDAP database field that will be used to match each user name against. The details entered here will depend on the specific LDAP database being used - 'uid' or 'cn' are commonly used values.

Anonymous Bind

If left unchecked then bind requests are sent with username (Base DN) and password (more suitable for Active Directory applications).

If checked, bind requests are anonymous (more suitable for Linux LDAP implementations).



INSTALLATION

CONFIGURATION

OPERATION

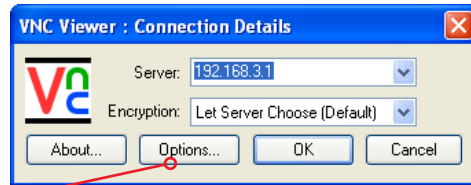
FURTHER
INFORMATION

INDEX

Appendix 3 - VNC viewer connection options

When you are connecting to the SC5-IP using the VNC viewer, a number of options are available.

Click here to access the options



There are six tabbed pages of options:

- Colour/Encoding
- [Inputs](#)
- [Scaling](#)
- [Misc](#)
- [Identities](#)
- [Load/Save](#)

IMPORTANT: If you make any changes to the options given here and wish to retain them for successive connection sessions, you must save the changes. To do this, change to the 'Load/Save' tab and click the 'Save' button within the 'Default' section.

Colour/Encoding

Auto select

When ticked, this option will examine the speed of your connection to the SC5-IP and apply the most suitable encoding method. This option is suggested for the majority of installations.

Preferred encoding

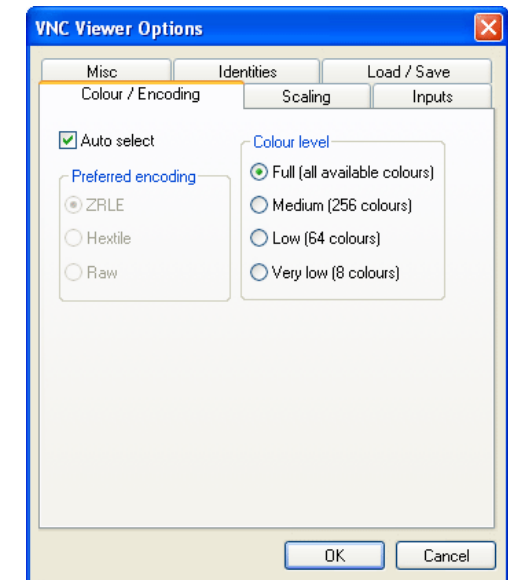
There are three manually selectable encoding methods which are accessible when the Auto select option is unticked.

- **ZRLE** – This is a highly compressed method that is best suited to slow modem connections.
- **Hextile** – This method offers better performance than the ZRLE when used over a high speed network because there is no need for the SC5-IP to spend time highly compressing the data.
- **Raw** – This is a primitive, uncompressed method that is mainly used for technical support issues. You are recommended not to use this method.

Colour level

This section allows you to select the most appropriate colour level for the speed of the connection to the SC5-IP. Where the connection speed is slow or inconsistent there will be a necessary compromise between screen response and colour depth.

- **Full** – This mode is suitable only for fast network connections and will pass on the maximum colour depth being used by the host system.
- **Medium (256 colours)** – This mode reduces the host system output to a 256 colour mode and is more suitable for ISDN and fast modem connections.
- **Low (64 colours)** – This mode is suitable for slower modem connections and reduces the host system output to 64 colours.
- **Very low (8 colours)** – This mode provides very rudimentary picture quality and hardly any speed advantage over the 64 colour setting. You are recommended not to use this mode.



INSTALLATION

CONFIGURATION

OPERATION

FURTHER INFORMATION

INDEX

Inputs

Enable all inputs

When selected, allows keyboard, mouse and clipboard data to be transferred between server and viewer systems.

Disable all inputs (view-only mode)

When selected, prevents control data being passed between server and viewer. Viewer can display the server output, but cannot control it.

Customise

Allows you to select which data can be transferred between server and viewer.

Send pointer events to server

When un-ticked, the VNC viewer will not send mouse movement or click data to the SC5-IP or host system.

Send keyboard events to server

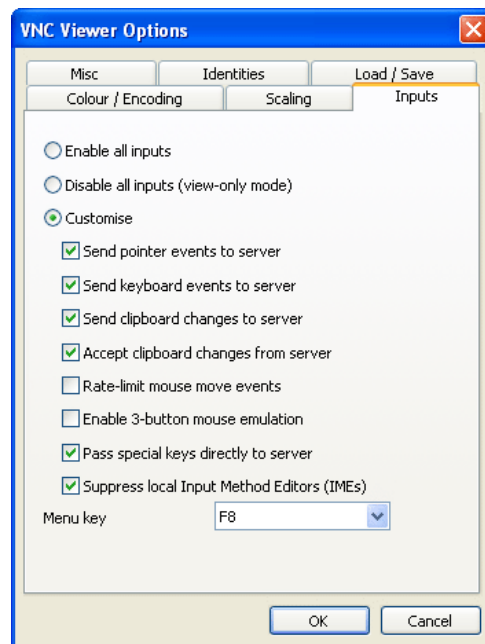
When un-ticked, the VNC viewer will not send keyboard information to the SC5-IP or host system.

Send clipboard changes to server

This feature is restricted to software server versions of VNC and has no effect on SC5-IP installations.

Accept clipboard changes from server

This feature is restricted to software server versions of VNC and has no effect on SC5-IP installations, except for retrieving the activity log as described in the logging and status section.



Rate-limit mouse move events

When ticked, this feature reduces the mouse movement information that is sent to the SC5-IP and host system. This is useful for slow connections and you will notice that the remote cursor will catch up with the local cursor roughly once every second.

Enable 3-button mouse emulation

This feature allows you to use a 2-button mouse to emulate the middle button of a 3-button mouse. When enabled, press the left and right mouse buttons simultaneously to create a middle button action. You are advised to generally use a 3-button mouse.

Pass special keys directly to server

When ticked, 'special' keys (the Windows key, the Print Screen key, Alt+Tab, Alt+Escape and Ctrl+Escape) are passed directly to the SC5-IP rather than being interpreted locally.

Menu key

This feature allows you to select which function key is used to display the VNC viewer options menu. The menu key is only way to exit from the full screen viewer mode.

IMPORTANT: If you make any changes to the options given here and wish to retain them for successive connection sessions, you must save the changes. To do this, change to the 'Load/Save' tab and click the 'Save' button within the 'Default' section.



INSTALLATION

CONFIGURATION

OPERATION

FURTHER
INFORMATION

INDEX

Shared connection (do not disconnect other viewers)

This option does not apply to SC5-IP connections.

Full screen mode

When ticked, the VNC viewer will launch in full screen mode. Use the menu key (usually F8) to exit from full screen mode.

Full screen mode matches server resolution

When ticked, the VNC viewer will attempt to use the screen resolution of the selected host system.

Full screen mode uses all monitors

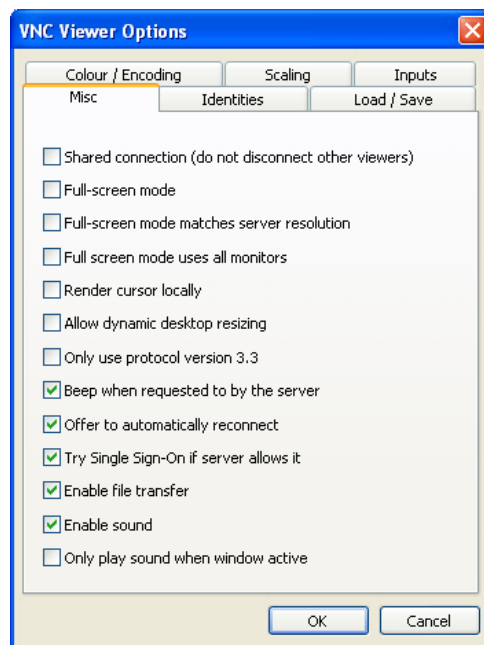
When ticked, the VNC viewer will show the screen image using all available display monitors on multiple display systems.

Render cursor locally

This option does not currently apply to SC5-IP connections.

Allow dynamic desktop resizing

When ticked, the viewer window will be automatically resized whenever the host system's screen resolution is altered.

**Only use protocol version 3.3**

This option does not apply to SC5-IP connections.

Beep when requested to by the server

When ticked, your local system will beep in response to any error beeps emitted by the SC5-IP.

Offer to automatically reconnect

When ticked, the viewer will offer to restore a lost connection with the server.

Try Single Sign-On if server allows it

This option does not apply to SC5-IP connections.

Enable file transfer

When ticked, the VNC viewer will allow file transfers between the IP connected viewer system and the selected host system.

Enable sound

Not supported.

Only play sound when window active

Not supported.

IMPORTANT: If you make any changes to the options given here and wish to retain them for successive connection sessions, you must save the changes. To do this, change to the 'Load/Save' tab and click the 'Save' button within the 'Default' section.



Scaling

No Scaling

No attempt is made to make the screen image fit the viewer window. You may need to scroll horizontally and/or vertically to view all parts of the screen image.

Scale to Window Size

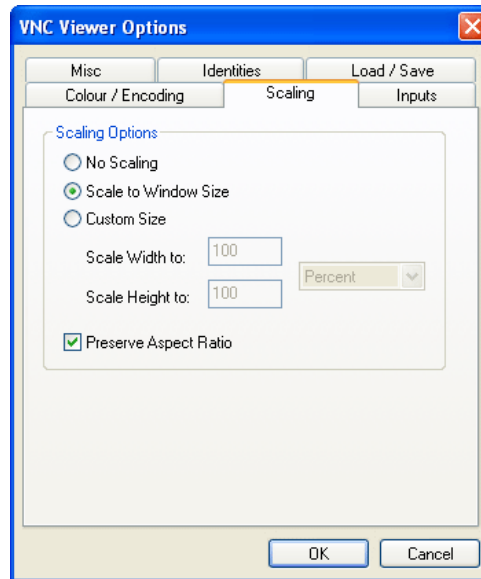
Adjusts the server screen image to suit the size of the viewer window.

Custom Size

Adjusts the server screen image according to the Width and Height settings in the adjacent fields. A drop box to the right of the fields allows you to define the image size by percentage or by pixels, as required.

Preserve Aspect Ratio

When ticked, maintains a consistent ratio between the horizontal and vertical dimensions of the screen image.



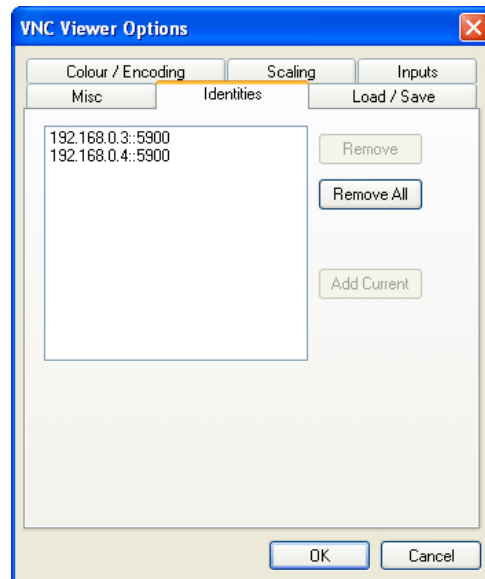
IMPORTANT: If you make any changes to the options given here and wish to retain them for successive connection sessions, you must save the changes. To do this, change to the 'Load/Save' tab and click the 'Save' button within the 'Default' section.

Identities

This feature helps your VNC viewer to confirm that a revisited SC5-IP is genuine and not another device masquerading as an SC5-IP. The list given will retain the identities of all visited units (that have full security enabled).

When you first make a secure connection to the SC5-IP, the security information for that SC5-IP unit is cached within this Identities tab (i.e. the “identity” is known). The next time that you connect to the SC5-IP, its identity is checked against the stored version. If a mismatch is found between the current and the stored identities then a warning will be issued to you.

If an existing SC5-IP is fully reconfigured then it will need to issued with a new identity. In this case the previous identity, listed in this tab, should be removed so that a new identity can be created on the next connection.



Load / Save

Configuration File - Reload

Allows you to load a configuration file saved from this, or another viewer.

Configuration File - Save

Allows you to save the current settings so that they can be copied from one viewer to another.

Configuration File - Save As...

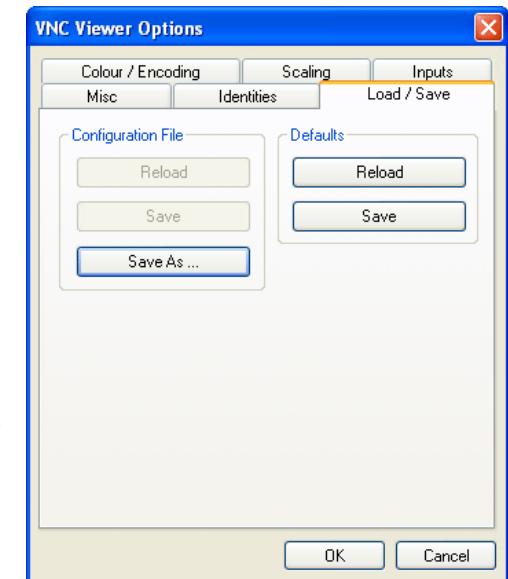
Allows you to save the current settings under a new name so that they can be copied from one viewer to another.

Defaults - Reload

When clicked, all connection options are returned to the default settings that are currently saved.

Defaults - Save

When clicked, saves the current connection options as the default set that will be used in all subsequent VNC connections.



INSTALLATION

CONFIGURATION

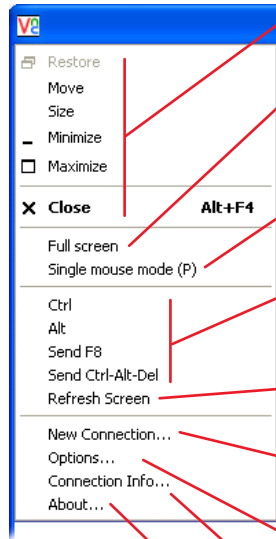
OPERATION

FURTHER
INFORMATION

INDEX

Appendix 4 - VNC viewer window options

Click the VNC icon in the top left corner of the viewer window (or press F8) to display the window options:



Standard window control items

Full screen

Expands the VNC viewer window to fill the whole screen with no visible window edges or toolbar. Press F8 to re-display this menu.

Single mouse mode (P)

Used for fast network connections where a second, "predictor" cursor is not required.

Ctrl, Alt, Send F8, Send Ctrl-Alt-Del

Sends the selected keypress(es) to the SC5-IP and host computer. This is necessary because certain keys and key combinations are trapped by the VNC viewer.

Refresh Screen

Requests data from the server for a complete redraw of the screen image, not just the items that change.

New connection...

Displays the connection dialog so that you can log on to a different SC5-IP or VNC server location.

Options...

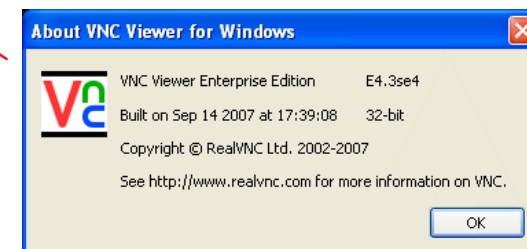
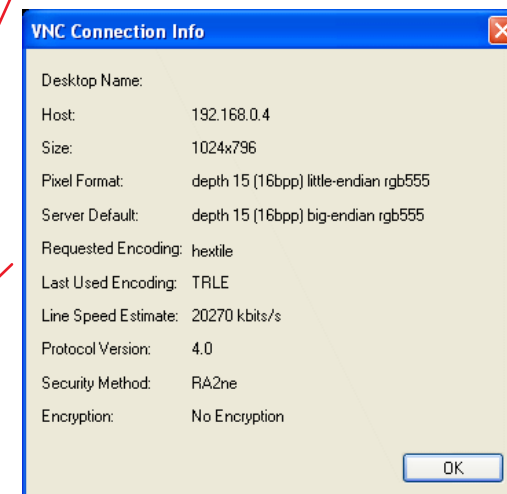
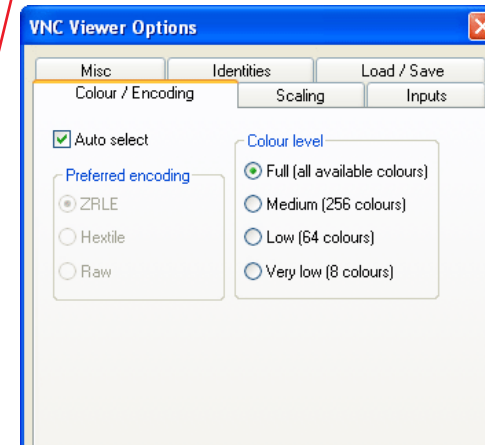
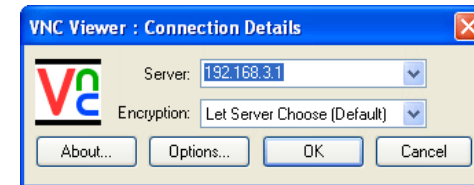
Displays the full range of connection options - see [Appendix 3](#) for more details.

Connection info...

Displays various connection and display details.

About...

Displays information about your VNC viewer.



INSTALLATION

CONFIGURATION

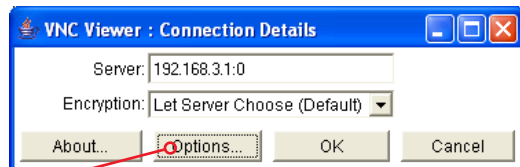
OPERATION

FURTHER INFORMATION

INDEX

Appendix 5 - Browser viewer options

When you are connecting to the SC5-IP using a Web browser, a number of options are available.



Click here to access the options

There are four options pages:

Encoding and colour level

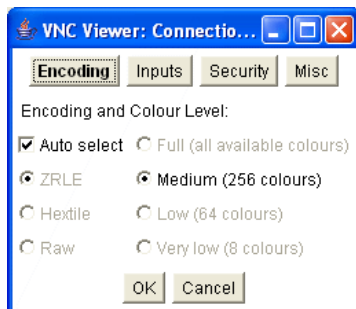
Auto select

When ticked, this option will examine the speed of your connection to the SC5-IP and apply the most suitable encoding method. This option is suggested for the majority of installations.

Preferred encoding

There are three manually selectable encoding methods which are accessible when the Auto select option is unticked.

- **ZRLE** – This is a highly compressed method that is best suited to slow modem connections.
- **Hextile** – This method offers better performance than the ZRLE when used over a high speed network because there is no need for the SC5-IP to spend time highly compressing the data.
- **Raw** – This is a primitive, uncompressed method that is mainly used for technical support issues. You are recommended not to use this method.



Colour level

The colour level is fixed at Medium (256 colours) for almost all browsers.

Inputs

View only (ignore mouse & keyboard)

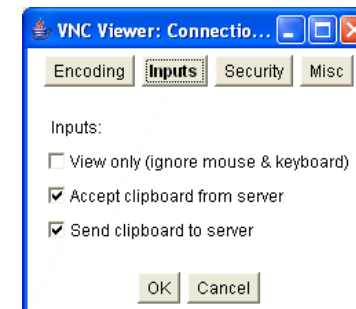
When ticked, the viewer will not send keyboard or mouse information to the SC5-IP or host computer.

Accept clipboard from server

This feature is restricted to software server versions of VNC and has no effect on SC5-IP installations.

Send clipboard to server

This feature is restricted to software server versions of VNC and has no effect on SC5-IP installations.



Security

512 bits (low security)

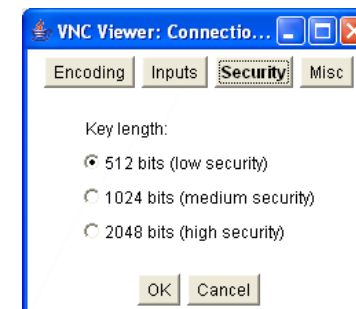
Selects the lowest level of encoding for communications between the browser and the SC5-IP.

1024 bits (medium security)

Selects the middle level of encoding for communications between the browser and the SC5-IP.

2048 bits (high security)

Selects the highest level of encoding for communications between the browser and the SC5-IP.



Misc

Shared (don't disconnect other viewers)

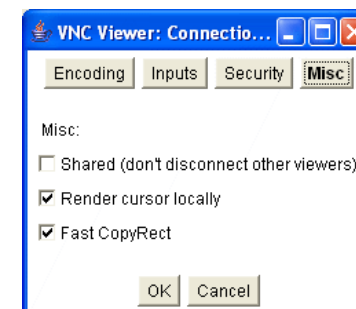
This feature is restricted to software server versions of VNC and has no effect on SC5-IP installations.

Render cursor locally

This feature is restricted to software server versions of VNC and has no effect on SC5-IP installations.

Fast CopyRect

This feature is restricted to software server versions of VNC and has no effect on SC5-IP installations.



INSTALLATION

CONFIGURATION

OPERATION

FURTHER INFORMATION

INDEX

Appendix 6 – Addresses, masks and ports

IP address, network masks and ports are all closely linked in the quest for one device to find another across disparate network links.

IP addresses

As a rough analogy, consider how you use the telephone system. The phone number for LINDY in the UK is **0044 (0)1642 754000**. This number consists of three distinct parts:

- **0044** connects from another country to the UK
- **(0)1642** selects the main telephone exchange in the Thornaby area of Stockton-on-Tees, and
- **754000** is the unique code for LINDY within Thornaby.

The important parts of the whole number depend on where you are. If you were based in the same local area as LINDY, there would be no point in dialling out of the UK, or even out of the area. The only part of the whole number that you are interested in is the final part: 754000.

In a similar way to the various parts of the telephone number, the four sections (or *Octets*) of every IP address have different meanings or “weights”. Consider the following typical IP address:

192.168.142.154

192 is the most global part of the number (akin to the *0044* of the phone number) and **154** is the most local (similar to the *754000* unique local code of the phone number).

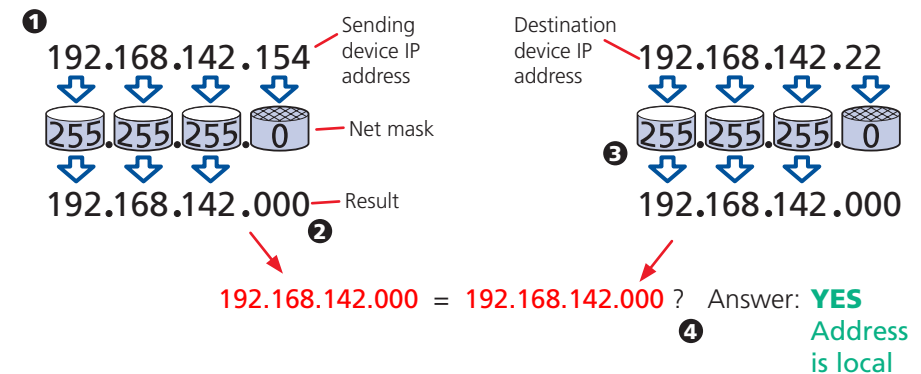
When two network devices communicate with each other, they always “dial the whole number” regardless of their respective locations in a network. However, they still need to know whether the other device is local to them or not, and this is where the net mask comes into play.

Net masks

The net mask (or sub-net mask) informs a device as to its own position within a network. From this it can determine whether any other device is within the same local network or is situated further afield.

Taking the telephone number analogy given in the IP address section, in order to use the telephone system efficiently, it is vital for you to know your location relative to the person you are calling. In this way you avoid dialling unnecessary numbers.

When one network device needs to talk to another, the first thing that it will do is a quick calculation using its own IP address, the other device’s IP address and its own net mask. Suppose a device with address **192.168.142.154** and net mask **255.255.255.0** needed to communicate with a device at address **192.168.142.22**. The sending device would perform several calculations:



1 The net mask is used to determine the local and global parts of the sender's IP address. Where there is 255 in the mask, the corresponding address slips through, where there is a 0, it is blocked.

2 Where the net mask was 0, the corresponding part of the result is also zero - this section is now known to be the local part of the IP address.

3 The same process is carried out for the destination address, again using the sender's net mask. Now the local parts of both addresses have been equalised to zero, because their values are not important in determining whether they are both in the same local network.

4 The results of the two net mask operations are now compared, if they match, the destination is local. If not, then the sender will still use the same full destination IP address but will also flag the message to go via the local network gateway and out into the wider world.

The reason for doing this? It makes the network, as a whole, much more efficient. If every message for every recipient was shoved straight out onto the Internet, the whole thing would grind to a halt within seconds. Net masks keep local traffic just that - local.

[Want to know more?](#)

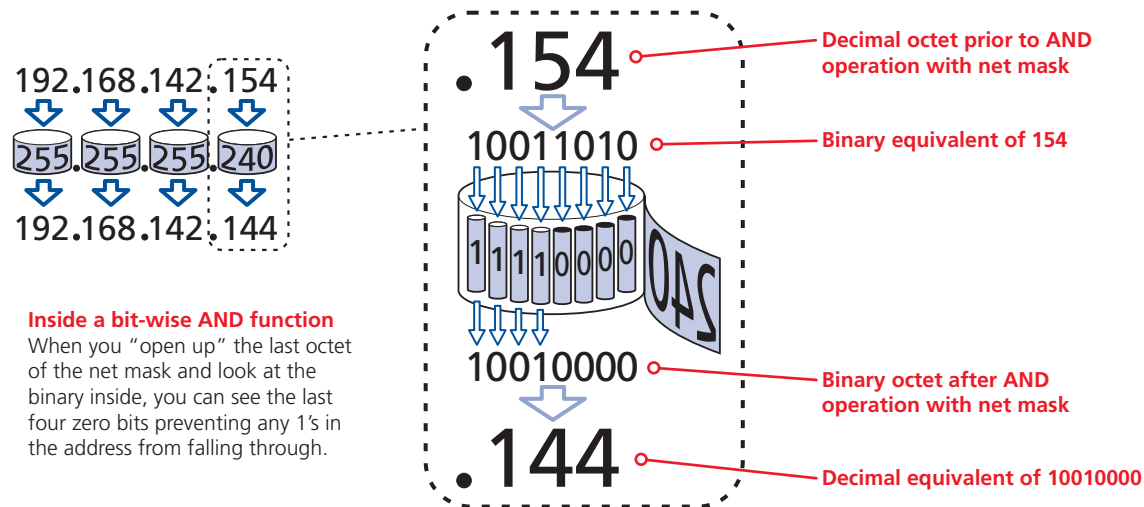
Net masks - the binary explanation

To really understand the operation of a net mask it is necessary to delve deeper into the life blood of computers – *binary*; this is native digital, where everything is either a 1 (one) or 0 (zero), on or off, yes or no.

The net mask operation described on the [previous page](#) is known as a 'bit-wise AND function'. The example of 255.255.255.0 is handy because the last octet is completely zero and is "clean" for illustrative purposes. However, actual net mask calculations are carried out, not on whole decimal numbers, but bit by bit on binary numbers, hence the term 'bit-wise'. In a real local network, a net mask might be 255.255.255.240. Such an example would no longer be quite so clear, until you look at the net mask in its binary form:

11111111.11111111.11111111.11110000

In this case, the four zeroes at the end of the net mask indicate that the local part of the address is formed by only the last four bits. If you use the diagram from the previous example and insert the new net mask, it will have the following effect on the final result:



Thus, when 154 is *bit-wise ANDed* with 240, the result is 144. Likewise, any local address from 192.168.142.144 through to 192.168.142.159 would produce exactly the same result when combined with this net mask, hence they would all be local addresses. However, any difference in the upper three octets or the upper four bits of the last octet would slip through the mask and the address would be flagged as not being local.

Calculating the mask for IP access control

The IP access control function uses a standard IP address and a net mask notation to specify both single locations and ranges of addresses. In order to use this function correctly, you need to calculate the mask so that it accurately encompasses the required address(es).

Single locations

Some of the simplest addresses to allow or deny are single locations. In this case you enter the required IP address into the 'Network/Address' field and simply enter the 'Mask' as **255.255.255.255** (*255 used throughout the mask means that every bit of the address will be compared and so there can only be one unique address to match the one stated in the 'Network/Address' field*).

All locations

The other easy setting to make is ALL addresses, using the mask **0.0.0.0**. As standard, the IP access control section includes the entry: **+0.0.0.0/0.0.0.0**. The purpose of this entry is to *include* all IP addresses. It is possible to similarly *exclude* all addresses, however, take great care not to do this as you instantly render all network access void. There is a [recovery procedure](#) should this occur.

Address ranges

Although you can define ranges of addresses, due to the way that the mask operates, there are certain restrictions on the particular ranges that can be set. For any given address you can encompass neighbouring addresses in blocks of either 2, 4, 8, 16, 32, 64, 128, etc. and these must fall on particular boundaries. For instance, if you wanted to define the local address range:

192.168.142.67 to 192.168.142.93

The closest single block to cover the range would be the 32 addresses from:

192.168.142.64 to 192.168.142.95.

The mask needed to accomplish this would be: **255.255.255.224**

When you look at the mask in binary, the picture becomes a little clearer. The above mask has the form: **11111111.11111111.11111111.11100000**

Ignoring the initial three octets, the final six zeroes of the mask would ensure that the 32 addresses from .64 (01000000) to .95 (01011111) would all be treated in the same manner. See [Net masks - the binary explanation](#) for details.

When defining a mask, the important rule to remember is:

There must be no 'ones' to the right of a 'zero'.

For instance, (ignoring the first three octets) you could not use a mask that had **11100110** because this would affect intermittent addresses within a range in an impractical manner. The same rule applies across the octets. For example, if you have zeroes in the third octet, then all of the fourth octet must be zeroes.

The permissible mask values (for all octets) are as follows:

Mask octet	Binary	Number of addresses encompassed
255	11111111	1 address
254	11111110	2 addresses
252	11111100	4 addresses
248	11111000	8 addresses
240	11110000	16 addresses
224	11100000	32 addresses
192	11000000	64 addresses
128	10000000	128 addresses
0	00000000	256 addresses

If the access control range that you need to define is not possible using one address and one mask, then you could break it down into two or more entries. Each of these entries could then use smaller ranges (of differing sizes) that, when combined with the other entries, cover the range that you require.

For instance, to accurately encompass the range in the earlier example:

192.168.142.67 to 192.168.142.93

You would need to define the following six address and mask combinations in the IP access control section:

Network/address entry	Mask entry	
192.168.142.67	255.255.255.255	defines 1 address (.67)
192.168.142.68	255.255.255.252	defines 4 addresses (.68 to .71)
192.168.142.72	255.255.255.248	defines 8 addresses (.72 to .79)
192.168.142.80	255.255.255.248	defines 8 addresses (.80 to .87)
192.168.142.88	255.255.255.252	defines 4 addresses (.88 to .92)
192.168.142.93	255.255.255.255	defines 1 address (.93)



INSTALLATION

CONFIGURATION

OPERATION

FURTHER INFORMATION

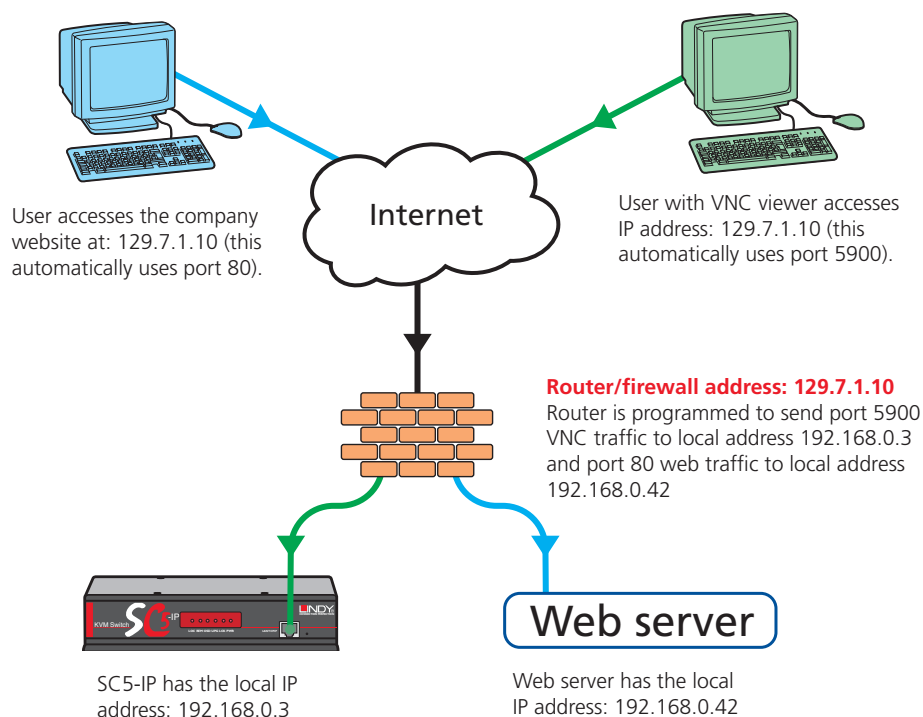
INDEX

Ports

If you accept the analogy of [IP addresses](#) being rather like telephone numbers, then think of ports as extension numbers. In a company of any size, you generally wouldn't expect the accounts department to share the same telephone with the technical department. Although their calls may all be related to the same company, they concern very different aspects of that company.

It is the same with IP network connections. Although you have only one network link into your computer and only one IP address (phone number), you are probably performing many different tasks through that one link, often at the same time. Thus, when you browse the web your outgoing requests and the incoming information are all channelled through port 80. When you send an email, it travels through port 25 and when you transfer files you are, without knowing it, using port 20.

At the "border crossing" between the wider Internet and every local network attached to it, there is a router that is usually combined with a firewall. One of its main tasks is to direct incoming traffic to the correct place within its local network. A key piece of information to help it do this is the port number:



Security issues with ports

The settings of port numbers become important when the SC5-IP is situated behind a network firewall. In order for a remote VNC viewer or web browser to make contact with your SC5-IP, it is necessary for the firewall to allow communication through a particular numbered port to occur.

One specific function of firewalls is to restrict access to ports in order to prevent malicious attackers using them as a route into your network. Every new port that is opened offers a new possibility for hackers and so the number of accessible ports is purposefully kept to a minimum. In such cases, it may be advantageous to change one or both SC5-IP ports to use the same number. The other alternative is to place the SC5-IP unit outside the firewall and take full advantage of its secure operation features – see [Networking issues](#) for details.

IMPORTANT: The correct configuration of routers and firewalls requires advanced networking skills and intimate knowledge of the particular network. We cannot provide specific advice on how to configure your network devices and strongly recommend that such tasks are carried out by a qualified professional.



INSTALLATION

CONFIGURATION

OPERATION

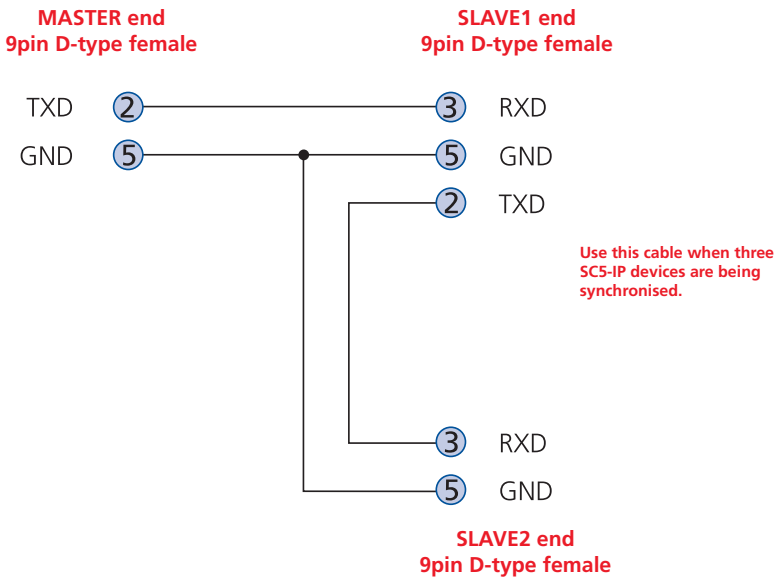
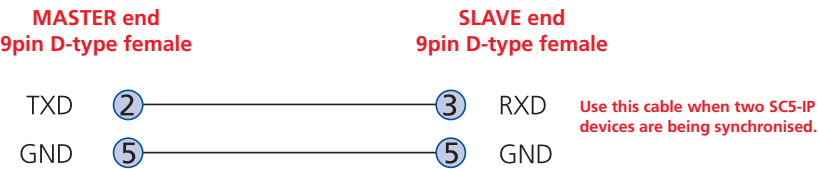
FURTHER
INFORMATION

INDEX

Appendix 7 – Cable and connector specifications



Multi-head synchronisation cable



INSTALLATION
CONFIGURATION
OPERATION
FURTHER INFORMATION
INDEX

Appendix 8 – Hotkey sequence codes

These codes are used when defining hotkey switching sequences (macros) for host computers and allow you to include almost any of the special keys on the keyboard.

Permissible key presses

Main control keys (see 'Using abbreviations')

Backspace | Tab | Return | Enter | Ctrl | Alt | Win | Shift | LShift | RShift
LCtrl | RCtrl | LAlt | AltGr | RAlt | LWin | RWin | Menu | Escape | Space
CapsLock | NumLock | PrintScreen | Scrolllock

Math operand keys (see 'Using abbreviations')

Add (Plus) | Subtract (Minus) | Multiply

Central control keys (see 'Using abbreviations')

Insert | Delete | Home | End | PageUp | PageDown
Up | Down | Left | Right | Print | Pause

Keypad keys (see 'Using abbreviations')

KP_Insert | KP_Delete | KP_Home | KP_End | KP_PageUp
KP_PageDown | KP_Up | KP_Down | KP_Left | KP_Right | KP_Enter
KP_Add | KP_Subtract | KP_Divide | KP_Multiply
KP_0 to KP_9

Function keys

F1 | F2 | F3 | F4 | F5 | F6 | F7 | F8 | F9 | F10 | F11 | F12

ASCII characters

All characters can be entered using their ASCII codes, from 32 to 126 (i.e. A,B,C, ... 1,2,3 etc.) with the exception of the special characters '+', '-', '+-' and '*' which have special meanings, as explained below.

Codes with special meanings

- + means press down the key that follows
- means release the key that follows
- +– means press down and release the key that follows
- * means wait 250ms (note: if a number immediately follows the asterisk, then the delay will equal the number, in milliseconds)

Note: Hotkey sequences are not case sensitive.

Creating macro sequences

Hot key macro sequences can be up to 256 characters long. All keys are assumed to be released at the end of a line, however, you can also determine that a key is pressed and released within a sequence. Any of the following three examples will send a command that emulates a press and release of the Scroll Lock key:

+SCROLL-SCROLL
+-SCROLL
+SCROLL-

Example:

+-SCROLL+-SCROLL+1+ENTER

Press and release scroll twice, press 1 then enter then release all keys (equivalent definition is +SCROLL-SCROLL+SCROLL-SCROLL+1+ENTER-1-ENTER)

Using abbreviations

To reduce the length of the key definitions, any unique abbreviation for a key can be used. For example: "scroll", "scr" and even "sc" all provide an identifiable match for "ScrollLock" whereas "en" could not be used because it might mean "Enter" or "End" ("ent" would be suitable for "Enter").

Note: Hotkey sequences and abbreviations are not case sensitive.

For information about where to enter these codes, please see the section [Keyboard control](#).



Appendix 9 – Supported video modes

The following video modes are supported and can be automatically configured by the SC5-IP units. If a recognised video mode cannot be found, the SC5-IP will gradually change some of the key parameters to discover whether a video lock can be achieved. Support for VESA GTF (Generalized Timing Formula) is available and can be enabled via the [Advanced Unit Configuration](#) screen.

The half width video modes capture every other pixel. These are not generally recommended for normal use but may be used for emergency access to high resolution, high frequency system screens. Half width screens can be expanded to normal width using the scaling features of the viewer.

vesa 720 x 400 @ 85Hz	sun 1152 x 900 @ 66Hz
vesa 640 x 480 @ 60Hz	sun 1152 x 900 @ 76Hz
vesa 640 x 480 @ 72Hz	sun 1280 x 1024 @ 67Hz
vesa 640 x 480 @ 75Hz	apple 640 x 480 @ 67Hz
vesa 640 x 480 @ 85Hz	apple 832 x 624 @ 75Hz
vesa 800 x 600 @ 56Hz	apple 1152 x 870 @ 75Hz
vesa 800 x 600 @ 60Hz	1920 x 1200 @ 60Hz**
vesa 800 x 600 @ 72Hz	
vesa 800 x 600 @ 75Hz	
vesa 800 x 600 @ 85Hz	
vesa 1024 x 768 @ 60Hz	
vesa 1024 x 768 @ 70Hz	
vesa 1024 x 768 @ 75Hz	
vesa 1024 x 768 @ 85Hz	
vesa 1152 x 864 @ 75Hz	
vesa 1280 x 960 @ 60Hz	
vesa 1280 x 1024 @ 60Hz	
vesa 1280 x 1024 @ 75Hz	
vesa 1600 x 1200 @ 60Hz	
vesa 720 x 400 @ 70Hz*	

* Not actually a VESA mode but a common DOS/BIOS mode

** This mode is displayed as a half width video mode via a VNC viewer.



INSTALLATION

CONFIGURATION

OPERATION

FURTHER
INFORMATION

INDEX

Warranty

LINDY warrants that this product shall be free from defects in workmanship and materials for a period of three years from the date of original purchase. If the product should fail to operate correctly in normal use during the warranty period, LINDY will replace or repair it free of charge. Any faulty items are to be returned to LINDY at the owner's expense. No liability can be accepted for damage due to misuse or circumstances outside LINDY's control. Also, LINDY will not be responsible for any loss, damage or injury arising directly or indirectly from the use of this product. LINDY's total liability under the terms of this warranty shall in all circumstances be limited to the replacement value of this product. This warranty goes on top of any applicable legal regulation and does not limit any customer rights compared to the legal regulations.

Safety information

- For use in dry, oil free indoor environments only.
- Both the SC5-IP and its power supply generate heat when in operation and will become warm to the touch. Do not enclose them or place them locations where air cannot circulate to cool the equipment. Do not operate the equipment in ambient temperatures exceeding 40 degrees Centigrade. Do not place the products in contact with equipment whose surface temperature exceeds 40 degrees Centigrade.
- Warning - live parts contained within power adapter.
- No user serviceable parts within power adapter - do not dismantle.
- Plug the power adapter into a socket outlet close to the module that it is powering.
- Replace the power adapter with a manufacturer approved type only.
- Do not use the power adapter if the power adapter case becomes damaged, cracked or broken or if you suspect that it is not operating properly.
- If you use a power extension cord with the SC5-IP, make sure the total ampere rating of the devices plugged into the extension cord does not exceed the cord's ampere rating. Also, make sure that the total ampere rating of all the devices plugged into the wall outlet does not exceed the wall outlet's ampere rating.
- Do not attempt to service the SC5-IP yourself.

General Public License (Linux)

The SC5-IP runs an embedded version of the Linux operating system, licensed under the GNU General Public License. To obtain the source code for the open-source components of the system visit:

<http://www.adventiq.com/products/ARQ3/gpl.html>



INSTALLATION

CONFIGURATION

OPERATION

FURTHER
INFORMATION

INDEX

WEEE (Waste of Electrical and Electronic Equipment), Recycling of Electronic Products



United Kingdom

In 2006 the European Union introduced regulations (WEEE) for the collection and recycling of all waste electrical and electronic equipment. It is no longer allowable to simply throw away electrical and electronic equipment. Instead, these products must enter the recycling process.

Each individual EU member state has implemented the WEEE regulations into national law in slightly different ways. Please follow your national law when you want to dispose of any electrical or electronic products.

More details can be obtained from your national WEEE recycling agency.

Deutschland

Die Europäische Union hat mit der WEEE Direktive umfassende Regelungen für die Verschrottung und das Recycling von Elektro- und Elektronikprodukten geschaffen. Diese wurden im deutschen Elektro- und Elektronikgerätegesetz – ElektroG in deutsches Recht umgesetzt. Dieses Gesetz verbietet vom 24.März 2006 an das Entsorgen von Elektro- und Elektronikgeräten über die Hausmülltonne!

B2B Geräte wie dieses sowie LINDY LCD Terminal und LINDY 19" KVM Switches nimmt LINDY kostenlos zurück und führt sie einem geordneten Recycling entsprechend den gesetzlichen Vorgaben zu. Bitte nehmen Sie hierzu Kontakt mit LINDY auf, die Kontaktadressen finden Sie stets auf der LINDY Website www.lindy.com

B2C-Geräte müssen den lokalen Sammelsystemen bzw. örtlichen Sammelstellen zugeführt werden! Dort werden sie kostenlos entgegen genommen. Die Kosten für den weiteren Recyclingprozess übernimmt die Gesamtheit der Gerätehersteller.

France

En 2006, l'union Européenne a introduit la nouvelle réglementation (DEEE) pour le recyclage de tout équipement électrique et électronique.

Chaque Etat membre de l'Union Européenne a mis en application la nouvelle réglementation DEEE de manières légèrement différentes. Veuillez suivre le décret d'application correspondant à l'élimination des déchets électriques ou électroniques de votre pays.

Italia

Nel 2006 l'unione europea ha introdotto regolamentazioni (WEEE) per la raccolta e il riciclo di apparecchi elettrici ed elettronici. Non è più consentito semplicemente gettare queste apparecchiature, devono essere riciclate. Ogni stato membro dell' EU ha tramutato le direttive WEEE in leggi statali in varie misure. Fare riferimento alle leggi del proprio Stato quando si dispone di un apparecchio elettrico o elettronico.

Per ulteriori dettagli fare riferimento alla direttiva WEEE sul riciclaggio del proprio Stato.



INSTALLATION

CONFIGURATION

OPERATION

FURTHER INFORMATION

INDEX

End user licence agreement

PLEASE READ THIS AGREEMENT CAREFULLY. THIS AGREEMENT CONCERNS ENHANCED VNC VIEWER SOFTWARE ("the SOFTWARE") FOR USE WITH THE SC5-IP PRODUCT ("the PRODUCT"). THE SOFTWARE IS PROVIDED TO ENABLE YOU TO OPERATE THE PRODUCT. BY USING ALL OR ANY PORTION OF THE SOFTWARE YOU ACCEPT ALL THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT ACCEPT ALL THE TERMS AND CONDITIONS OF THIS AGREEMENT THEN DO NOT USE THE SOFTWARE. BY USING ANY UPDATED VERSION OF THE SOFTWARE WHICH MAY BE MADE AVAILABLE, YOU ACCEPT THAT THE TERMS OF THIS AGREEMENT APPLY TO SUCH UPDATED SOFTWARE.

1. Intellectual Property Rights

The Software and its structure and algorithms are protected by copyright and other intellectual property laws, and all intellectual property rights in them belong to RealVNC Limited ("RealVNC"), a United Kingdom Limited Company, or are licensed to it. You may not reproduce, publish, transmit, modify, create derivative works from, publicly display the Software or part thereof. Copying or storing or using the Software other than as permitted in Clause 2 is expressly prohibited unless you obtain prior written permission from RealVNC.

2. Permitted and Prohibited Uses

- 2.1 During the term of this Agreement and as long as you comply with the terms of this agreement, you may use the Software only with the Product for your personal use or for the internal use of your business. You may make as many copies of the Software as you require for your own internal business purposes only and for archival purposes. You are expressly prohibited from distributing the Software in any format, in whole or in part, for sale, or for commercial use or for any unlawful purpose.
- 2.2 You may not rent, lease or otherwise transfer the Software or allow it to be copied. Unless permitted by law, you may not reverse engineer, decompile or disassemble the Software.

3. Warranty

REALVNC DOES NOT WARRANT ANY RESULTS OBTAINED USING THE SOFTWARE. TO THE EXTENT PERMITTED BY LAW, REALVNC DISCLAIMS ALL OTHER WARRANTIES ON THE SOFTWARE, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT OF THIRD PARTY RIGHTS AND FITNESS FOR PARTICULAR PURPOSE.

4. Limitation on Liability

UNDER NO CIRCUMSTANCES SHALL REALVNC BE LIABLE FOR ANY CONSEQUENTIAL INDIRECT OR INCIDENTAL DAMAGES WHATSOEVER INCLUDING LOST PROFITS OR SAVINGS ARISING OUT OF THE USE OF THE SOFTWARE, THE SERVICE OR THE INFORMATION, RELIANCE ON THE DATA PRODUCED OR INABILITY TO USE THE SOFTWARE, THE SERVICE OR THE INFORMATION EVEN IF REALVNC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. BECAUSE SOME STATES AND COUNTRIES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU. NOTHING IN THIS AGREEMENT LIMITS LIABILITY FOR DEATH OR PERSONAL INJURY ARISING FROM A PARTY'S NEGLIGENCE OR FROM FRAUDULENT MISREPRESENTATION ON THE PART OF A PARTY

5. Export Control

The United States and other countries control the export of Software and information. You are responsible for compliance with the laws of your local jurisdiction regarding the import, export or re-export of the Software, and agree to comply with such restrictions and not to export or re-export the Software where this is prohibited. By downloading the Software, you are agreeing that you are not a person or entity to which such export is prohibited.

6. Term and Termination

This licence shall continue in force unless and until it is terminated by RealVNC by e-mail notice to you, if it reasonably believes that you have breached a material term of this Agreement.

In the case above, you must delete and destroy all copies of the Software in your possession and control and overwrite any electronic memory or storage locations containing the Software.

7. General Terms

- 7.1 The construction, validity and performance of this Agreement shall be governed in all respects by English law, and the Parties agree to submit to the exclusive jurisdiction of the English courts.
- 7.2 If any provision of this agreement is found to be invalid by any court having competent jurisdiction, the invalidity of such provision shall not affect the validity of the remaining provisions of this agreement, which shall remain in full force and effect.
- 7.3 No waiver of any term of this agreement shall be deemed a further or continuing waiver of such term or any other term.
- 7.4 This agreement constitutes the entire agreement between you and RealVNC.



INSTALLATION

CONFIGURATION

OPERATION

FURTHER
INFORMATION

INDEX

Radio Frequency Energy

A Category 5 (or better) twisted pair cable must be used to connect the units in order to maintain compliance with radio frequency energy emission regulations and ensure a suitably high level of immunity to electromagnetic disturbances.

All other interface cables used with this equipment must be shielded in order to maintain compliance with radio frequency energy emission regulations and ensure a suitably high level of immunity to electromagnetic disturbances.

European EMC directive 89/336/EEC

This equipment has been tested and found to comply with the limits for a class A computing device in accordance with the specifications in the European standards EN55022 and EN55024. These limits are designed to provide reasonable protection against harmful interference. This equipment generates, uses and can radiate radio frequency energy and if not installed and used in accordance with the instructions may cause harmful interference to radio or television reception. However, there is no guarantee that harmful interference will not occur in a particular installation. If this equipment does cause interference to radio or television reception, which can be determined by turning the equipment on and off, the user is encouraged to correct the interference with one or more of the following measures: (a) Reorient or relocate the receiving antenna. (b) Increase the separation between the equipment and the receiver. (c) Connect the equipment to an outlet on a circuit different from that to which the receiver is connected. (d) Consult the supplier or an experienced radio/TV technician for help.

FCC Compliance Statement (United States)

This equipment generates, uses and can radiate radio frequency energy and if not installed and used properly, that is, in strict accordance with the manufacturer's instructions, may cause interference to radio communication. It has been tested and found to comply with the limits for a class A computing device in accordance with the specifications in Subpart J of part 15 of FCC rules, which are designed to provide reasonable protection against such interference when the equipment is operated in a commercial environment. Operation of this equipment in a residential area may cause interference, in which case the user at his own expense will be required to take whatever measures may be necessary to correct the interference. Changes or modifications not expressly approved by the manufacturer could void the user's authority to operate the equipment.

Canadian Department of Communications RFI statement

This equipment does not exceed the class A limits for radio noise emissions from digital apparatus set out in the radio interference regulations of the Canadian Department of Communications.

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de la classe A prescrites dans le règlement sur le brouillage radioélectriques publié par le ministère des Communications du Canada.



INSTALLATION

CONFIGURATION

OPERATION

FURTHER
INFORMATION

INDEX

© 2009 LINDY Electronics Limited & LINDY Elektronik GmbH
 All trademarks are acknowledged.
 Release 1.0h
 February 2009



Documentation by: www.ctxd.com

INSTALLATION

CONFIGURATION

OPERATION

FURTHER
INFORMATION

INDEX

Great Britain & N. Ireland

LINDY Electronics Ltd
 Sadler Forster Way
 Teesside Industrial Estate
 Thornaby
 Stockton-on-Tees
 TS17 9JY
 United Kingdom
 Email: postmaster@lindy.co.uk
 Tel: 01642 754000
 Fax: 01642 765274

International & Eire

LINDY International Ltd.
 Sadler Forster Way
 Teesside Industrial Estate
 Thornaby
 Stockton-on-Tees
 TS17 9JY
 United Kingdom
 Email: postmaster@lindy.com
 Tel: +44 (0) 1642 754020
 Fax: +44 (0) 1642 754029

North America

LINDY Computer Connection Technology, Inc.
 16214 Phillips Road
 Athens, AL 35613
 USA
 Email: usa@lindy-usa.com
 Tel: (256) 771-0660
 Fax: (256) 771-0460

Germany

LINDY-Elektronik GmbH
 Markircher Str. 20
 68229 Mannheim
 Deutschland
 Email: info@lindy.de
 Tel: 0621 - 470050
 Fax: 0621 - 4700530

France

LINDY FRANCE SA
 6 Rue RAPP
 CS31015
 67451 MUNDOLSHEIM
 CEDEX
 France
 Email: france@lindy.fr
 Tel: 0 825 825 111
 Fax: 03 88 20 57 74

Italia

LINDY Italia Srl
 Via Varesina, 126/B
 22079 - Villa Guardia (CO)
 Italia
 Email: italia@lindy.it
 Tel: 031 48 40 11
 Fax: 031 48 06 52

Schweiz/Suisse/Svizzera

LINDY-Elektronik AG
 Florenzstrasse 9
 CH 4023 Basel
 Email: info@lindy.ch
 Tel. 061 - 3359700
 Fax 061 - 3359709

Index

A

- Access
 - local and remote users 32
- Access control
 - configuration 65
 - mask calculation 79
- Access mode
 - shared & private 42
- Account
 - creation for users 60
- Address
 - explanation 77
- Addressing
 - cascaded computers 15
 - DNS 28
 - network issues 27
- ADMIN
 - forgotten password 22
 - password 21
- Admin password
 - initial setup 19
 - local setting 55
- Advanced options 54
- Advanced unit configuration 62
- Artifacts
 - on screen 40
- Assistance
 - from Lindy 48
- Auto calibrate 42
- Autoscanning 22
- Auto select 70,76

B

- Baud rate
 - local setting 57
 - remote setting 66
- Binary
 - net masks 78
- Brackets 6
 - fitting 7
- Browser
 - connection 39
 - viewer options 76

C

- Cable specifications 81
- Calibrate
 - mouse 42
 - screen 42
- Calibrate all
 - video settings 45
- CAM
 - connection 11
- Cascade connections
 - addressing 15
 - introduction 13
 - tips for success 14
- Clear IP access control
 - local setting 56
- Colour level 70
- Computer
 - connection 11
 - ports 5
 - selecting 32
- Computer Access Module
 - connection 11

- Configuration 18
 - initial IP 24
 - menus 20,49
 - overall steps 18
 - pages 21,59
 - saving and restoring 22
- Confirmation box 35
- Connections 8
 - Computer Access Module 11
 - computer system 11
 - global user 11
 - host computer 9
 - keyboard 9
 - local user 9
 - multiple video head 16
 - network port 10
 - power supply 12
- Connector specifications 81
- Control menus 40
- Controls
 - viewer options 43

D

- Date
 - local setting 55
- DHCP
 - discovering allocations 28
 - during initial setup 19
 - local setting 56
 - remote setting 64
- DNS addressing 28

E

- Encryption key 19
- Encryption settings 25
 - viewer 47
- End user licence 86

F

- Firewall 27
- Firmware
 - current version 61
 - recovery procedure 30
 - upgrade 30
- Force encryption 55
- Front panel
 - controls and indicators 31
- Full screen mode
 - escape from (F8) 40
- Functions 50,54

G

- Gateway
 - local setting 56
 - remote setting 64
- Global preferences 52,54
- Global user
 - access 37
 - connection 11

H

- Hextile 70,76
- Host computer
 - changing between 40,41
 - configuration 67
 - connecting 9
 - connection 11
 - selection 41

- Hotkeys
 - changing 21
 - codes and macros 82
 - selecting computers 32
- HTTP port
 - initial setup 19
 - local setting 56
 - remote setting 64
 - when altered 27

I

- Identities
 - VNC Viewer 74
- Indicators 5,31
- Initial configuration 18
- IP access control 64,65
 - calculating mask 79
 - clearing 23
- IP address
 - explanation 77
 - local setting 56
 - remote setting 64
- IP gateway 64
- IP network mask 64
- IP port
 - configuration via viewer 24
 - connecting 10

K

- Keyboard codes
 - sending 44
- Keyboard layout
 - local setting 55
 - remote setting 61



INSTALLATION

CONFIGURATION

OPERATION

FURTHER
INFORMATION

INDEX

L

Local connection 32
Local network
 connection 26
Local user
 connection 9
 port 5
Logging 68
Logging in and out
 section 34,35
Log on 38

M

MAC address 56,63,64
Mask
 explanation 77
 for IP access control 79
Menu bar
 viewer window 40
Menu key
 changing 71
Mounting 7
Mouse
 calibration 42
 control 43
 pointers 41
 resync 42,43
Multiple video head
 connections 16

N

Net mask 56
 explanation 77
Network configuration 56,64
Networking issues 26
Network port
 connection 10

O

Octets
 ip address 77
Operation 31
Options port
 baud rate 66
 configuration 57

P

Parts
 supplied and extra 6
Password
 admin 21
 admin - setting 55
 forgotten 22
 initial setup 19
 remote logon 38
 setting for users 60
Port number
 entering 47
Power supply
 connecting 12
Preferred encoding 70
Private
 access mode 42

R

Rack mounting 7
Raw 70,76
Recover
 upgrade failure 30
Refresh screen 43
Reminder banner 35

Remote configuration
 advanced unit configuration 62
 host configuration 67
 logging and status 68
 network configuration 64
 serial port configuration 66
 setting IP access control 65
 unit configuration 61
 user accounts 60
Resync mouse 43
Router 27
Routing status 35

S

Safety information 84
Saving
 configuration settings 22
Scaling
 VNC Viewer 73
Screen
 best resolution 40
 calibration 42
 navigation 40
 refresh 43
Screensaver
 local setting 55
Security
 enabling 21
 ensuring 29
 general steps 21
Selecting
 cascaded computers 35
 computers 32
 with hotkeys 32
 with mouse buttons 34
 with on-screen menu 33

Serial port
 configuration 66
Server
 configuration 67
Server IP
 local setting 57
Setup options 50,53
Shared
 access mode 42
Single mouse mode 41,43
Slow connections
 optimising for 40
Supplied items 6
Syslog 68,69

T

Threshold
 adjustment 45
Time
 local setting 55
Time & date configuration 63
Troubleshooting 48

U

Unit Configuration 55,61
Unit name
 local setting 55
 remote setting 61
Upgrade
 firmware 30
 recover after failure 30
Use DHCP
 local setting 56
User accounts 60
User preferences 51,53

V

Video modes 83
Video settings 43
Viewer window 40
VNC port
 initial setup 19
 local setting 56
 remote setting 64
 when altered 27
VNC viewer
 connection 38
 connection options 70
 download 38
 window options 75

W

Warranty 84
Web browser
 connection 39
 viewer options 76

Z

ZRLE 70,76



INSTALLATION

CONFIGURATION

OPERATION

FURTHER
INFORMATION

INDEX