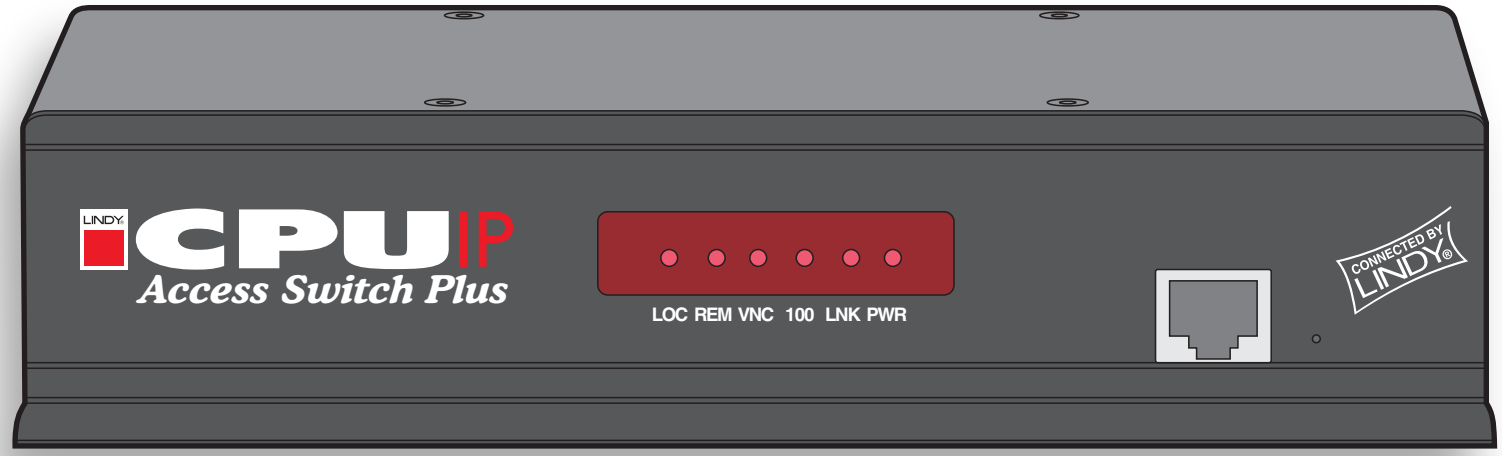
CPU IP Access Switch Plus

User Guide



CONTENTS

Contents

Introduction

CPU IP Access Switch Plus features - front and rear 4
What's in the box 5
What you may additionally need 5

Installation

Mounting 6
Connections 7
Host computer or KVM switch 7
Local keyboard, video monitor and mouse 8
IP network port 8
Modem/ISDN port 9
Power supply connection 9
Power control port 10

Configuration

Initial configuration 11
Part 1 – Local configuration 11
Encryption settings 13
Hot plugging and mouse restoration 14
Resetting the configuration 15
Part 2 – Remote configuration 16
Networking issues 17
Positioning CPU IP in the network 17
Placing CPU IP behind a router or firewall 17
Placing CPU IP alongside the firewall 19
Power switching configuration 20
Performing a flash upgrade 21

Operation

Connecting to the CPU IP 22
Local connection 22
Remote connections 23
Remote connection by VNC viewer 24
Remote connection by Web browser 24
Using the viewer window 25
The menu bar 25
When using the viewer window 25
Mouse pointers 26
Host selection 26
Configure 26
Auto calibrate 27
Re-synchronise mouse 27
Access mode - shared/private 27
Power control 27
Controls 28
Connecting via dial up (modem or ISDN) link 30
Downloading VNC viewer from the CPU IP 30
If you need to enter a port number 30
Viewer encryption settings 31
Supported web browsers 31

Contents - page 2

Further information

Troubleshooting 32
Getting assistance 32
Appendix 1 - Local configuration menus 33
Unit configuration 34
Network configuration 35
Modem configuration 36
Reset configuration 37
Clear IP access control 38
Appendix 2 - VNC viewer connection options 39
Colour/Encoding 39
Inputs 40
Misc 40
Identities 41
Defaults 41
Appendix 3 - VNC viewer window options 42
Appendix 4 - Browser viewer options 43
Encoding and colour level 43
Inputs 43
Security 43
Misc 43
Appendix 5 - Remote configuration menus 44
User accounts 45
Unit configuration 46
Advanced unit configuration 47
Network configuration 48
Setting IP access control 49
Serial port configuration 50
Modem port 50
Power control port 50
Host configuration 51
Logging and status 52
Appendix 6 – Addresses, masks and ports 53
IP addresses 53
Net masks 53
Net masks - the binary explanation 54
Calculating the mask for IP access control 55
Ports 56
Security issues with ports 56
Appendix 7 – Cable and connector specifications 57
RS232 serial mouse to PS/2 converter cable 57
CPU IP to power switch cable 57
Power switch to power switch daisy chain cable 57
Appendix 8 – Hotkey sequence codes 58
Other products in the CPU Switch range 59
Warranty 59
Safety information 59
Radio Frequency Energy 60

Index

Introduction

Thank you for choosing the CPU IP Access Switch Plus from LINDY. This intelligent product delivers straightforward setup, secure operation and the ability to fully control one or more computers from almost anywhere.

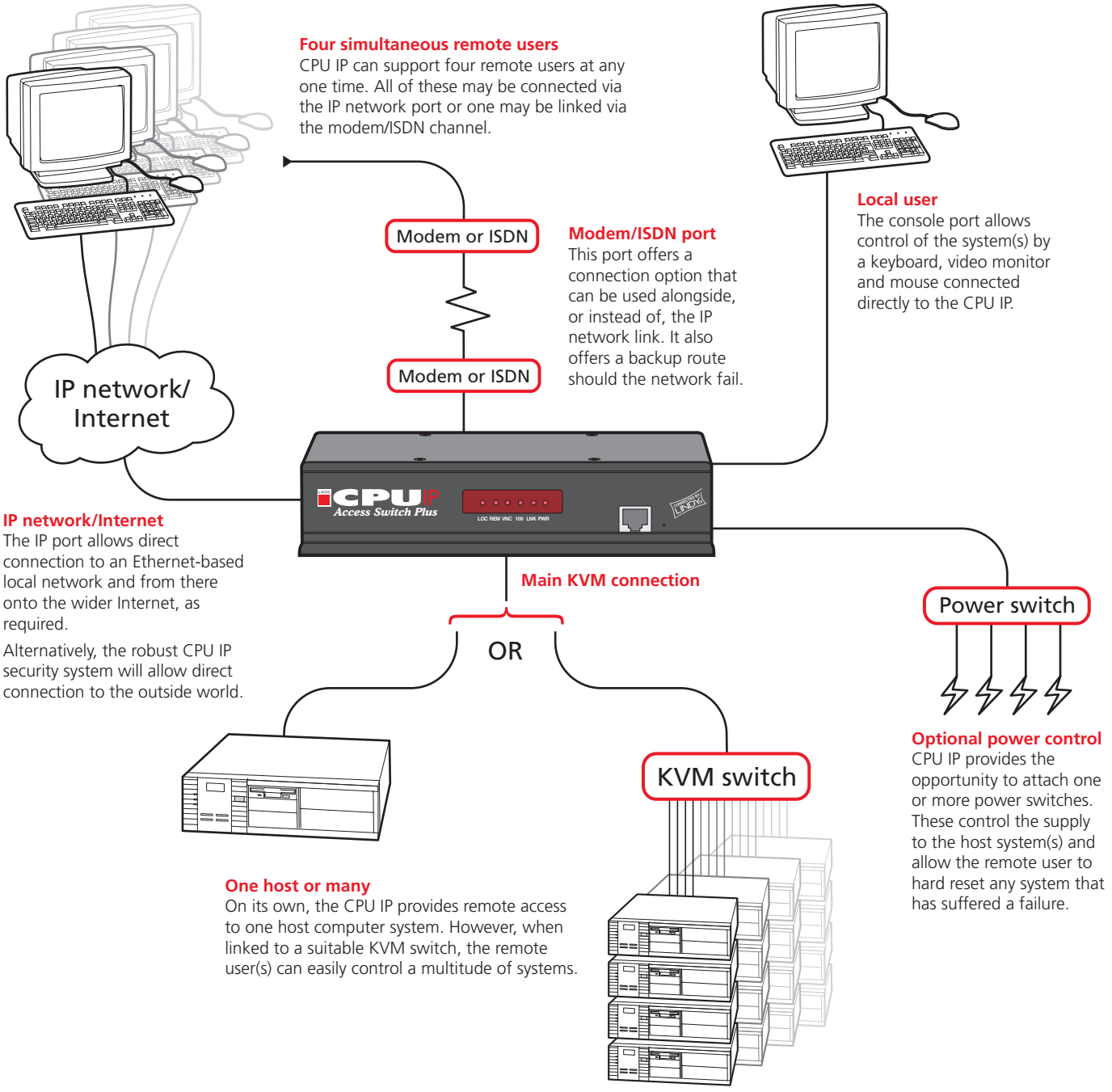
Remote control via a network connection is nothing new and software-only solutions to facilitate this are commonplace. However, they all present two major drawbacks: a) Special software must be used on all of the computers involved, especially the host, and b) if that host ceases to operate, the remote user is powerless to intervene.

The CPU IP is different and requires only the remote system(s) to run a small utility. The host system can run its usual operating system completely unchanged and needs only to be connected (via its keyboard, video and mouse ports) to the compact CPU IP box.

It is this external connection to the CPU IP that keeps the remote user in control. Even in the midst of a system crash, the remote user can still view the host's condition as if sitting next to it. Additionally, when the power switch option is employed, a host system can be remotely rebooted, no matter how badly it has locked-up.

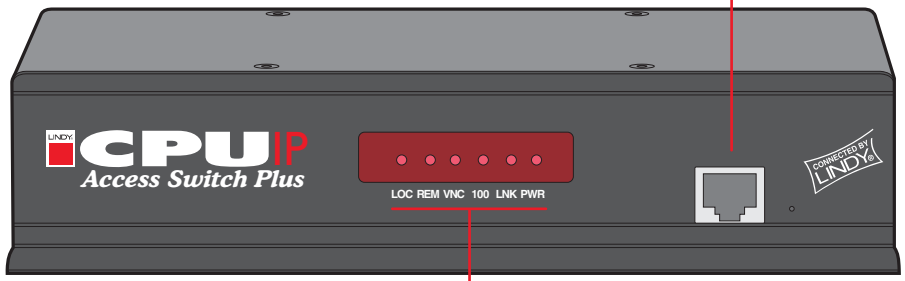
The CPU IP really starts to excel when it is hooked to a suitable KVM switch. Then its robust, secure and adaptable operation is available across a multitude of systems.

Note: Throughout this manual the LINDY CPU IP Access Switch Plus is referred to simply as the CPU IP.



CPU IP Access Switch Plus features - front and rear

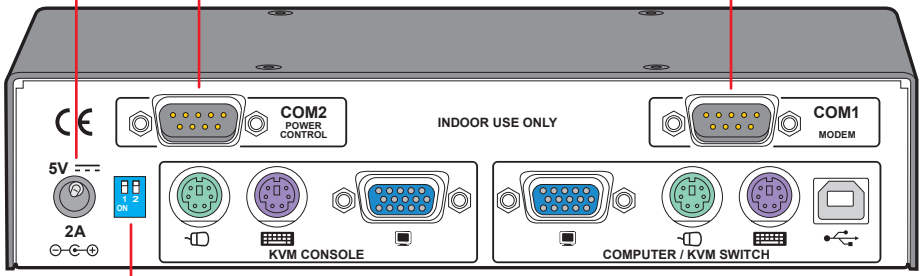
Considering its capabilities, the CPU IP is supplied within a remarkably compact casing. Measuring just 198mm x 120mm x 43mm, it occupies just half of a single (1U) rack space and provides most of its connectors at the rear face. The smart front face features the IP network port and the operation indicators.



IP network port
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 is being received from the local console.
- **REM** Keyboard or mouse data is being received from a remote viewer.
- **VNC** Indicates that a remote viewer is connected and active.
- **100** Indicates the Ethernet network speed (10/100Mbs).
- **LNK** Network link and activity indication.
- **PWR** Power indicator.



Power input
Connect the supplied power adapter here.

Power control port
Optionally use this port to control one or more power switches. These allow the remote user to take full control of the host system(s).

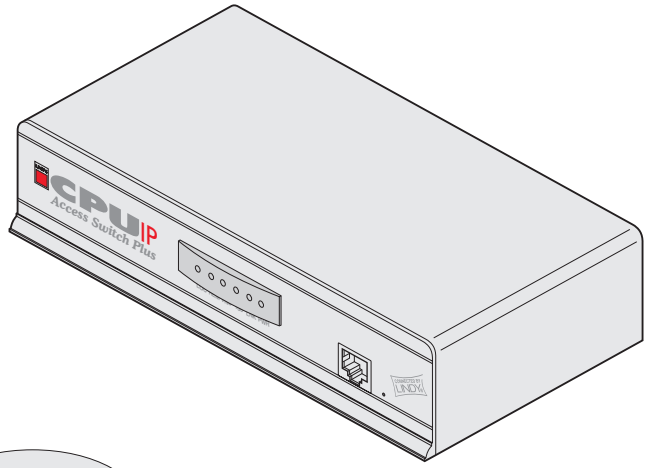
Modem port
Optionally use this port to attach either a standard modem or an ISDN adapter. This feature provides an alternative, direct-dial, remote link into the CPU IP.

Configuration switches
Used for flash upgrades and total reset functions. They are not required under normal circumstances.

KVM console
Connect a keyboard, video monitor and a mouse to these three connectors. These allow you to perform the initial configuration of the CPU IP. Additionally, you can use these to locally control the connected computer(s).

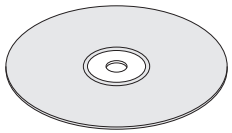
Computer/KVM Switch
Link these connectors to the keyboard, video and mouse ports of the device to be remotely controlled, either a single computer or a KVM switch. The USB port on the right is for future expansion and is not currently used.

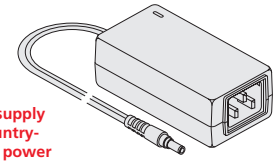
What's in the box



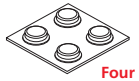
CPU IP Access Switch Plus

CD-ROM

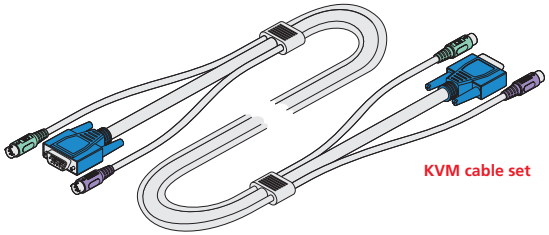




Power supply and country-specific power lead

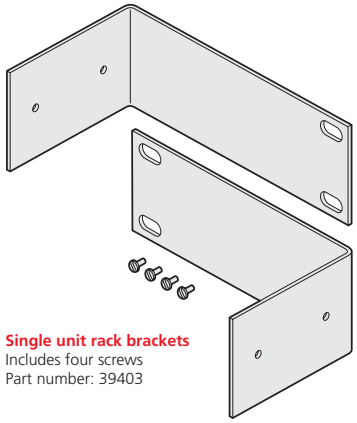


Four Self-adhesive rubber feet

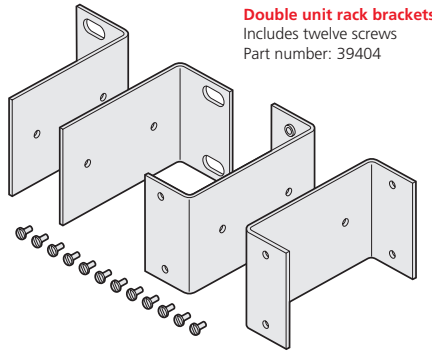


KVM cable set

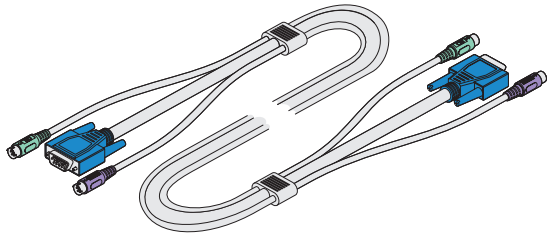
What you may additionally need



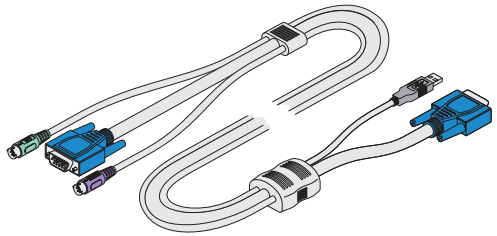
Single unit rack brackets
Includes four screws
Part number: 39403



Double unit rack brackets
Includes twelve screws
Part number: 39404



KVM cables
One set per connected computer
Part numbers: 33711 - 33718
(*cable lengths available: 1, 2, 3, 5, 10, 15 or 20 metres*)



Multi-platform KVM converter cable
Required to connect with computers that use a USB port to connect their keyboard and mouse
Part number: 42867

PS/2 to AT-style keyboard converter
(part number: 70130)

PS/2 to 9-pin serial mouse converter
(part number: 70058)

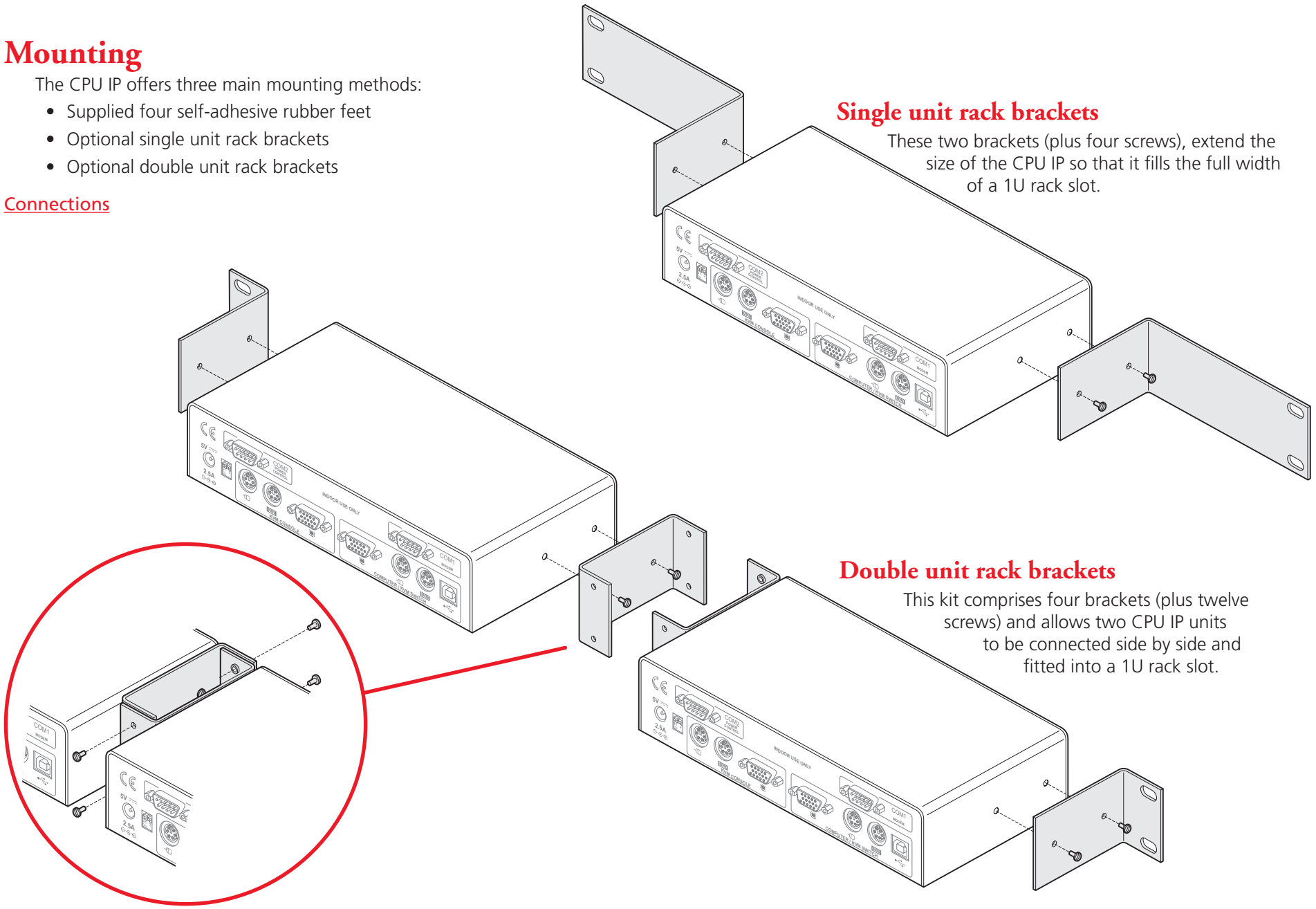
Installation

Mounting

The CPU IP offers three main mounting methods:

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

Connections



Single unit rack brackets

These two brackets (plus four screws), extend the size of the CPU IP so that it fills the full width of a 1U rack slot.

Double unit rack brackets

This kit comprises four brackets (plus twelve screws) and allows two CPU IP units to be connected side by side and fitted into a 1U rack slot.

Connections

Installation of the CPU IP involves a number of basic connections to some or all of the following items:

- Host computer or KVM switch ⇨
- Local keyboard, video and mouse
- IP network port
- Modem/ISDN port
- Power input
- Power control port

Host computer or KVM switch

The CPU IP can either connect directly to a single host computer or to range of hosts via one or more KVM switches.

To connect a host computer or KVM switch

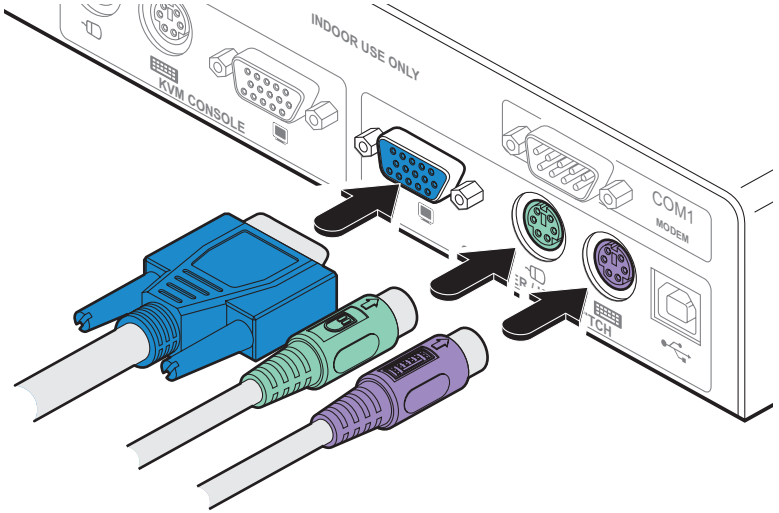
1 Ensure that power is disconnected from the CPU IP and the computer or KVM switch to be connected.

(Note: If it is not possible to switch off devices prior to connection, then a 'Hot plug' procedure is available – see the Hot plugging and mouse restoration section for more details).

2 Connect the plugs at one end of a KVM cable set to the keyboard, video and mouse sockets of the computer or KVM switch (for mouse plug conversion information – see Appendix 7).

Monitor (video)			Blue
Keyboard			Purple
Mouse		or	Mid green

3 Connect the plugs at the other end of the KVM cable set to the corresponding sockets, collectively labelled as 'COMPUTER/KVM SWITCH', at the rear of the CPU IP.



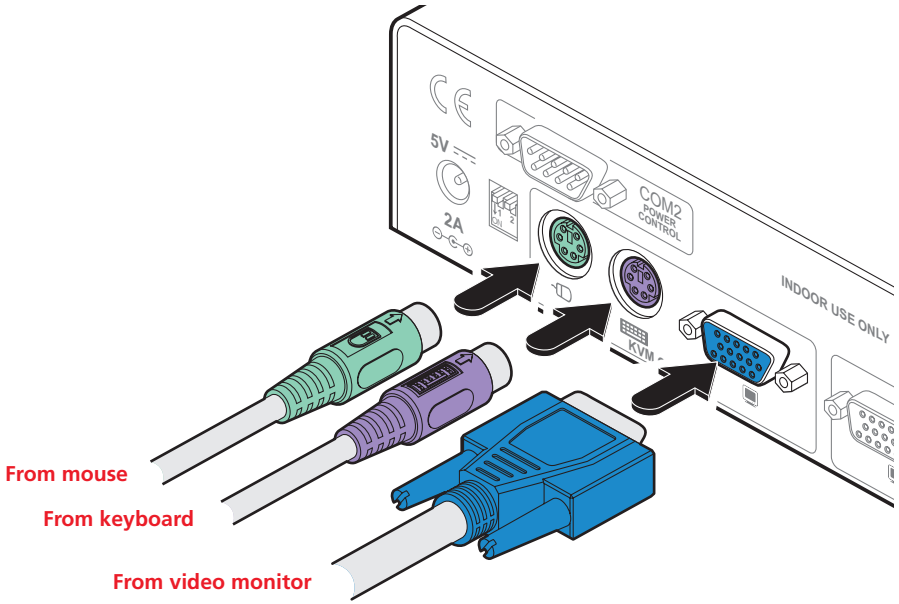
Local keyboard, video monitor and mouse

A locally connected keyboard, video monitor and mouse are required during the initial configuration. These are also useful during normal use to allow quick local control of any connected host computers.

To connect a local keyboard, video monitor and mouse

1 Position a suitable keyboard, video monitor and mouse in the vicinity of the CPU IP such that their cables will easily reach.

2 Connect the keyboard, video monitor and mouse plugs to the sockets, collectively labelled as 'KVM CONSOLE', at the rear of the CPU IP.



IP network port

The CPU IP provides an autosensing Ethernet IP port that can operate at 10 or 100Mbps, according to the network speed. The CPU IP is designed to reside quite easily at any part of your network:

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

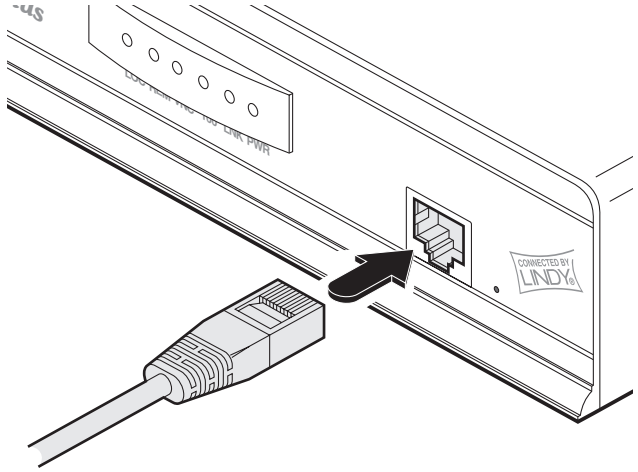
Wherever in the network the CPU IP is situated, you will need to determine certain configuration issues such as address allocation and/or firewall adjustment to allow correct operation. Please refer to Networking issues within the Configuration chapter for more details.

IMPORTANT: When the CPU IP is accessible from the public Internet or dial up connection, you must ensure that sufficient security measures are employed.

To connect the IP network port

1 Depending upon where in the network the CPU IP is being connected, run a category 5e or 6 cable from the appropriate hub or router to the CPU IP.

2 Connect the plug of the category 5e or 6 cable into the IP port on the front panel of the CPU IP.



3 Configure the network settings as appropriate to the position of the CPU IP within the network - see Networking issues for details.

Modem/ISDN port

The CPU IP provides a serial port specifically for you to connect either a modem or ISDN terminal adapter. This can be used as a primary, secondary or backup access port for remote systems, as best suits your overall configuration.

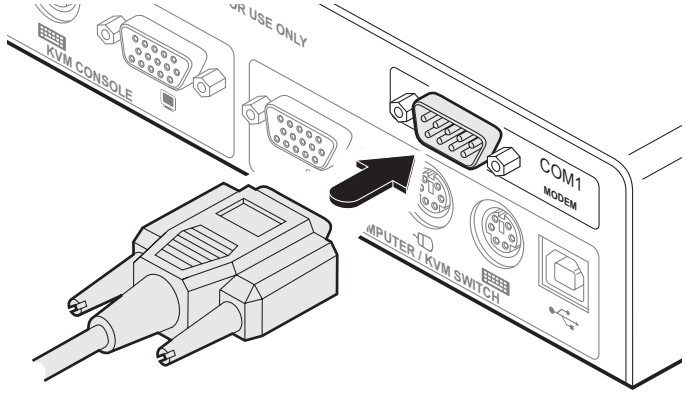
IMPORTANT: When the CPU IP is accessible from the public Internet or dial up connection, you must ensure that sufficient security measures are employed.

To connect a modem or ISDN port

1 If possible, disconnect power from the CPU IP and the modem or ISDN adapter.

2 Connect a suitable serial modem (non-crossover) cable to the serial port on the modem/ISDN adapter.

3 Connect the other end of the serial cable to the port labelled COM1 at the rear of the CPU IP.



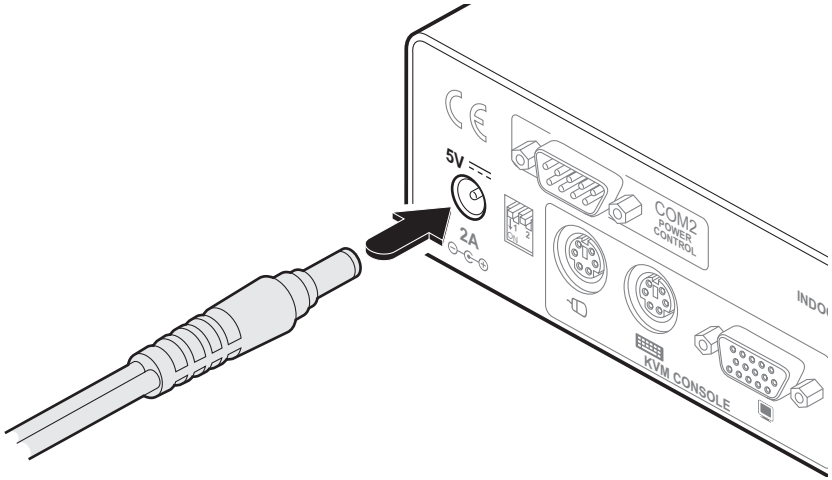
Note: The default serial port speed is 115200K and a standard Hayes-compatible auto-answer string is sent during startup. The default startup string is 'ATZHS0=1'. Both the serial port speed and startup string settings can easily be altered during the local or remote configuration - see Initial configuration for more details. The other serial settings are fixed at: No parity, 8 bit word and 1 stop bit.

Power supply connection

The CPU IP is supplied with a single power supply and an appropriate country-specific IEC power lead. There is no on/off switch so operation begins as soon as the power supply is connected.

To connect the power supply

1 Connect the low voltage output connector from the power supply unit to the power socket on the rear panel of the CPU IP.



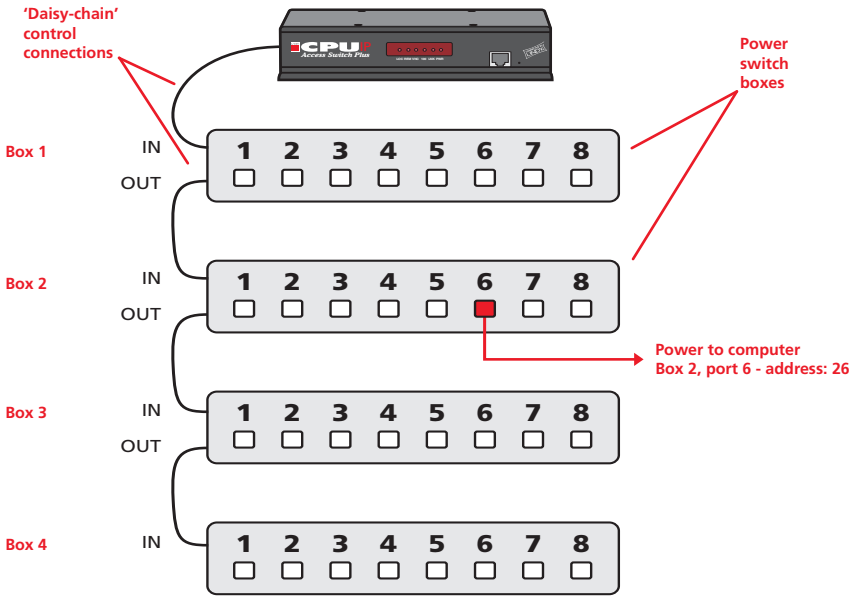
2 Connect the IEC connector of the supplied country-specific power lead to the socket of the power supply.

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

Power control port

The CPU IP provides a serial port for connection to one or more optional power control units. This allows you to control the mains power being supplied to the connected host(s) so that an authorised remote user can, if necessary, perform a complete cold reboot on a failed host system.

The control connector of the first power switch is connected, via serial cable, to the rear panel of the CPU IP. Any additional power switches are then connected via a 'daisy-chain' arrangement to the first power switch. Each power switch box is then given a unique address and access to each power port (4 or 8 ports on each power switch box) is gained using a combination of the switch box address and the port number.



The power ports are connected to the power inputs of each computer and the power switch box(es) are then connected to a mains power supply.

IMPORTANT: Power switching devices have a maximum current rating. It is essential to ensure that the total current drawn by the equipment connected to the power switching device does not exceed the current rating of the power switching device. You must also ensure that the current drawn from any mains socket does not exceed the current rating of the mains socket.

Setting up, configuring and using power switching requires three main steps:

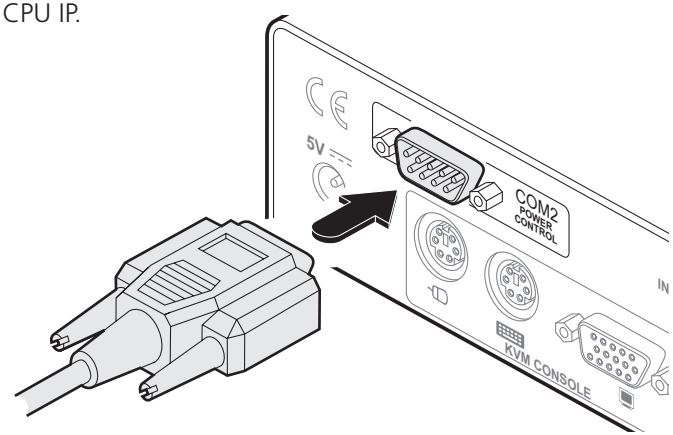
- Connect and address the switch boxes ⇨
- Configure the power strings
- Operate remote power switching

To connect and address the switch boxes

Note: The CPU IP can be powered on during this procedure, however, the switch boxes should be switched off.

1 Mount up to four switch boxes in positions where they are close to the computers that they will control and not too distant from the CPU IP (preferably within 2.5 metres).

2 Use a serial cable with an RJ10 and a 9-pin D-type connector (see Appendix 7 for specification). Connect the RJ10 plug to the socket marked 'IN' on the first switch box. Connect the other end to the socket marked 'COM2' on the CPU IP.



3 For each of the remaining switch boxes (if used), use a serial cable with RJ10 connectors at both ends (see Appendix 7 for specification). Connect one end to the socket marked 'OUT' of the previous box and the other end to the socket marked 'IN' of the next box.

4 Set the addressing switches on each switch box using the micro switches according to the switch box manual.

5 Connect IEC to IEC power leads between each port and the power input socket of each computer that requires power switching. Carefully note to which power ports, on which boxes, each computer is connected. If server systems have multiple power inputs, then each input must be connected via separate ports, which can be on the same, or different boxes.

6 Connect each box to a suitable mains power input.

Now proceed to the configuration stage covered in the Power switching configuration section within the Configuration chapter.

Configuration

Initial configuration

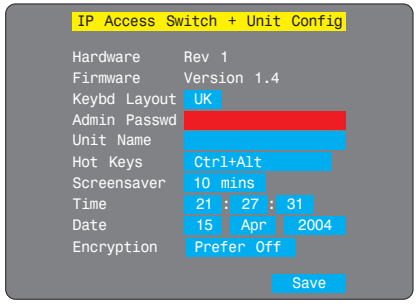
The initial configuration occurs as two distinct parts:

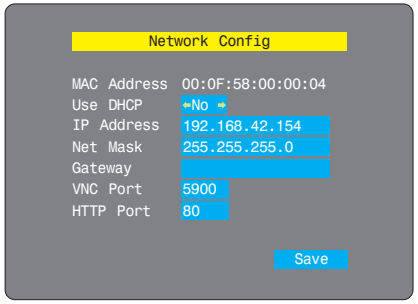
Part 1 – Local configuration
This part of the configuration takes place using the locally connected keyboard and video monitor. It allows you to set up key basic details, network essentials, modem/ISDN parameters and security key creation.

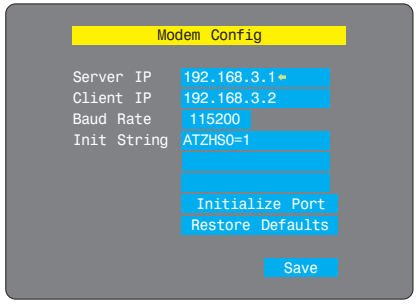
Part 2 – Remote configuration
This part of the configuration takes place using a remote connection (network or dial-up modem/ISDN). It allows fine tuning of the part 1 configuration items plus the creation of multiple user accounts and host details. Go to Part 2 - Remote configuration.

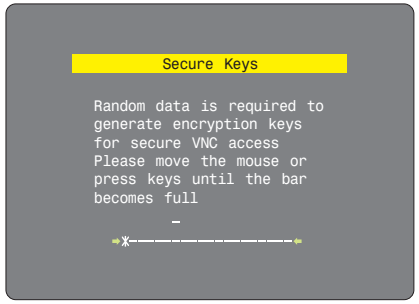
Part 1 – Local configuration

When you switch on the CPU IP unit for the first time it will take you (using the locally connected keyboard and video monitor) through a set up sequence consisting of four main screens:









Unit config screen

Allows you to determine a mixture of basic and fundamental setup details such as the keyboard layout, admin password, time and date.

Network config screen

Requires you to configure the various key aspects of the IP network port addressing.

Modem config screen

Allows you to optionally alter the current settings for the serial port that is used to connect a modem or ISDN terminal adapter. The IP addresses are used to emulate a two-port network connection and are suitable for most situations.

Secure keys screen

This screen uses your mouse movements or keyboard inputs to create random data. This unpredictable information is then combined with several other factors to develop the basis of the encryption keys that are used to establish secure remote links.

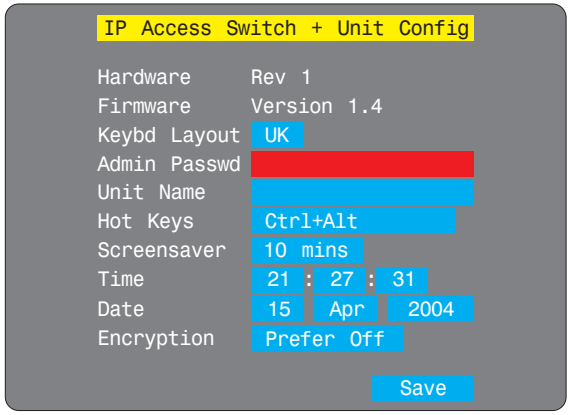
Controlling the local configuration menus
The local menus use only the keyboard. Use the keyboard arrow keys to move the green highlight indicator to the required position. Then, either type the required information or use the left and right arrows to change multiple choice items, as appropriate.

Problems?
The CPU IP asks for an unknown admin password
The CPU IP does not display the configuration sequence

continued

To perform the initial local configuration

1 Edit the Unit config screen. The key elements here are:



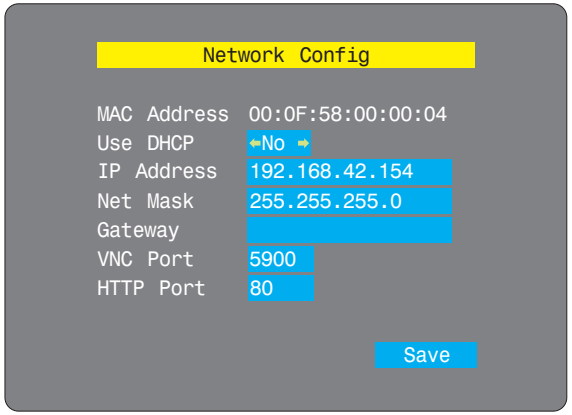
Admin password
Enter a password of at least six characters that has a mix of letters and numerals. The background colour provides an indication of password suitability and is initially red to indicate that the password is not sufficient. When a password with reasonable strength has been entered it changes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

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

Encryption
Arrange this setting according to your security requirements. See Encryption settings for a description of the issues and the settings.

When all items are correct, select the Save option to display the next screen.

2 Edit the Network config screen. The key elements here are:

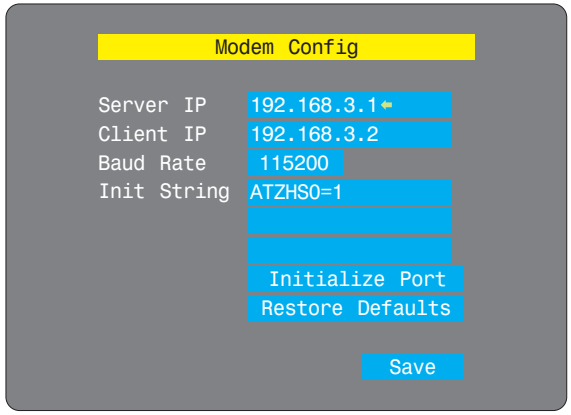


Use DHCP/IP address/Net Mask/Gateway
You need to either set the DHCP option to 'Yes' or manually enter a valid IP address, Net mask and Gateway. See Networking issues for more details.

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.

When all items are correct, select the Save option to display the next screen.

3 If necessary, edit the Modem config screen.

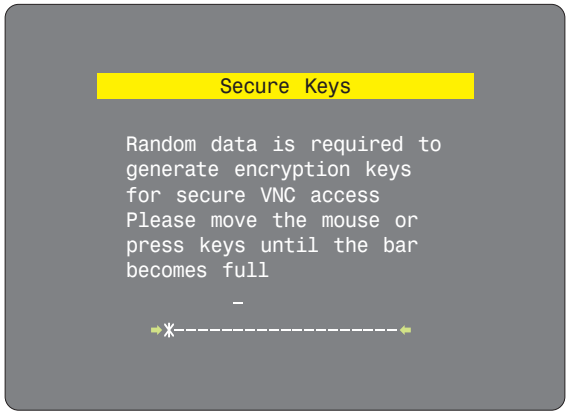


The default items here are perfectly adequate for the majority of modem and ISDN terminal adapter installations.

The Server IP and Client IP addresses are used to form an isolated two-device PPP network connection via the dial up link. Their settings are not related to any other 'real' network settings within the CPU IP.

When all items are correct, select the Save option to display the next screen.

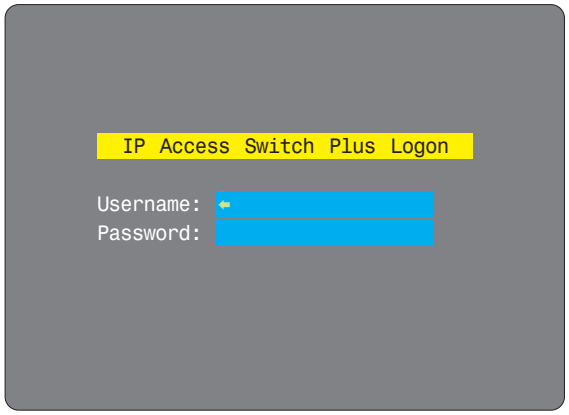
4 Move the mouse and enter changing key sequences within this screen.



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 is accepted as part of the new encryption key. When the bar is full, the final encryption keys for your CPU IP will be created – this process takes roughly 30 to 40 seconds.

continued

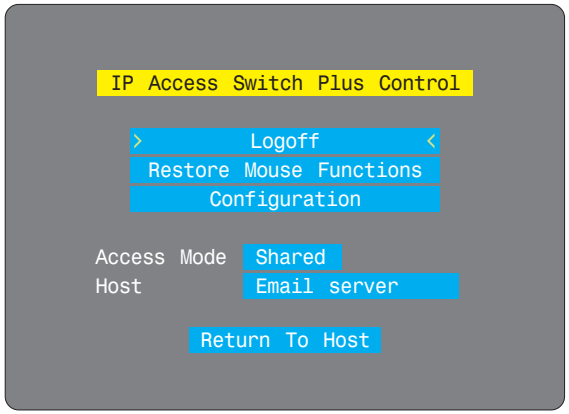
5 Once the secure keys have been calculated the CPU IP will restart and present a standard logon screen.



At this stage the username will be 'admin' and the password will be whatever you entered in the first setup screen.

Once the username and password have been accepted, the screen should now show the host computer screen (or, if none is connected, a blank image).

6 To view the options menu: Press Ctrl Alt C. More about hotkeys. (if the standard hotkeys were altered, use the new hotkeys plus C)



Logoff
Select to close your current session and display the screensaver.

Restore mouse functions
Select to revive a mouse that has ceased to function correctly. See Hot plugging and mouse restoration for details.

Configuration
Select to gain access to the Unit, Network and Modem configuration screens. Within here you can also reset the CPU IP to its initial state.

Access mode
Allows you to choose between Shared mode (where all other logged on users can see your operations) and Private mode (where the screens of all other users are blanked).

Host
Indicates the currently selected host computer and allows you to select others. This item will be blank unless host details have been set within the remote configuration.

Return to host
Quits the menu and returns to the host screen.

Encryption settings

The CPU IP offers a great deal of flexibility in its configuration and this extends equally to its encryption settings. Due to the variety of situations in which it might be used and the range of viewer applications that need to view it, a number of settings are available that might not make perfect sense at first glance. However, these settings should allow you to configure the CPU IP and the viewers to operate as required.

Factors to consider when setting these options might be:

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

CPU IP encryption settings

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

Hot plugging and mouse restoration

It is strongly recommended that you switch off a host computer before attempting to connect it to the CPU IP. However, if this is not possible then you need to 'hot plug' the computer while it is still running. There is not normally a danger of damage to the computer, however, when mouse communications are interrupted, often they fail to re-initialise when reconnected. The CPU IP provides a feature to reinstate mouse communications once the necessary connections have been made.

There are two main types of data formats used by current PC mice, these are the older 'PS/2' format and the more recent 'IntelliMouse®' format introduced by Microsoft. These use slightly different data arrangements and it is important to know which type was being used before you hot-plugged the computer to the CPU IP. The previous setting depends both on the type of mouse and the type of driver, as various combinations of PS/2 and IntelliMouse are possible. Using the incorrect restore function may produce unpredictable results and require the computer to be re-booted.

Which restore setting do I use?

The general rule is that unless both the mouse *and* the driver are *both* IntelliMouse compatible then you need to restore the mouse as 'PS/2'. An IntelliMouse can operate in either mode, whereas a PS/2 mouse cannot.

Recognising an IntelliMouse-style mouse

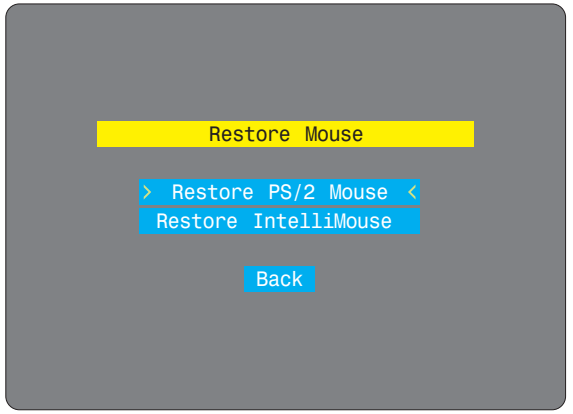
The IntelliMouse format was introduced to support, among other features, the scroll wheel function. If the mouse has a scroll wheel, then it is likely to support the IntelliMouse format. If it is a Microsoft-branded mouse, then it will usually state that it is an IntelliMouse on its underside label.

Recognising an IntelliMouse driver

Before hot plugging to the CPU IP (or afterwards using only keyboard control), access the Windows Control Panel of the computer and select either the *Mouse* option (on Windows NT, 2000 and XP) or the *System* option (on Windows 95, 98, ME). Look for the name of the driver, which will usually include the words *PS/2* or *IntelliMouse*.

To restore mouse operation when hot plugging:

1. Using a KVM cable set, carefully make the keyboard, monitor and mouse connections between the host computer and the ports collectively labelled COMPUTER/KVM SWITCH on the CPU IP.
2. Using a keyboard and monitor directly connected to the CPU IP, log on and then press Ctrl Alt C to view the options menu. More about hotkeys
3. Select the 'Restore mouse functions' option to display:



4. Select one of the following options:
   - *Restore Standard Mouse* – if PS/2 mode is required, or
   - *Restore IntelliMouse* – if IntelliMouse mode is required.
5. Select the 'Return to host' option.
6. Move the mouse a short distance and check for appropriate on-screen cursor movement. If the mouse cursor darts erratically around the screen, then cease moving the mouse. This is an indication that the chosen restore function is incorrect. Try again using the other restore function.

   Note: The restore functions predict the likely mouse resolution settings but may not restore the exact speed or sensitivity settings that were originally set.

Resetting the configuration

The CPU IP asks for an unknown admin password

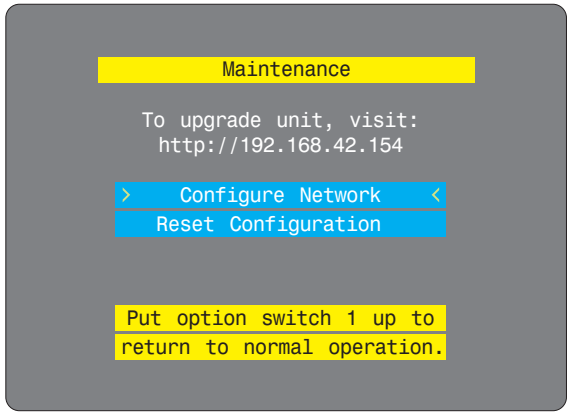
This may occur if the CPU IP has been previously configured. If the existing admin password cannot be discovered, then your only recourse is to perform a factory reset.

To invoke a configuration reset by switch

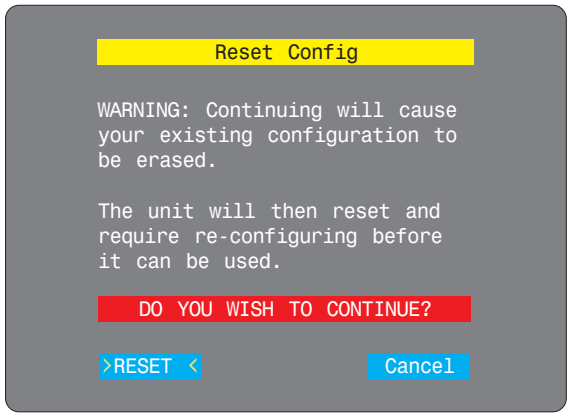
1 Remove power from the CPU IP unit.

2 At the rear of the CPU IP, adjacent to the power input socket, click mini switch 1 to its ON (down) position.

3 Re-apply power to the CPU IP. On the locally connected monitor you should see a Maintenance menu:



4 Select the 'Reset configuration' option.
A warning screen will be displayed. Select the RESET option and press ↵.



5 Remove power, return the mini switch 1 to its OFF position and then re-apply power. The locally connected monitor should display the first screen of the initial configuration sequence.

The CPU IP does not display the configuration sequence

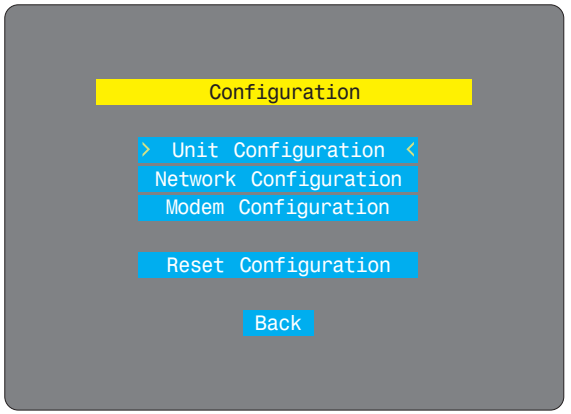
If the CPU IP has been previously configured it may not automatically display the first of the setup screens. In this case you have two options, either:

- Access the Unit, Network and Serial configuration screens separately, or
- Reset the configuration:

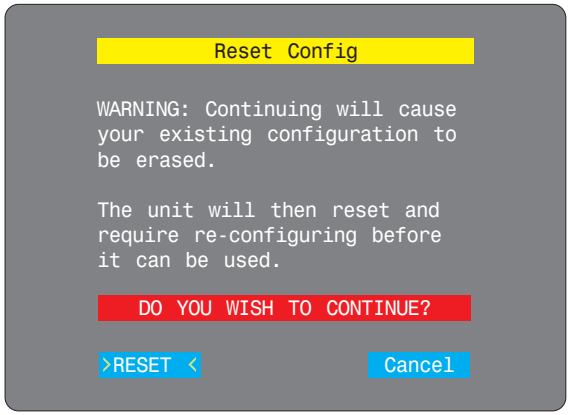
To invoke a configuration reset by main menu

1 Using the locally connected keyboard and screen, log on as the admin user.

2 Select the 'Configuration' option.



3 Highlight the 'Reset configuration' option and press ↵.
A warning screen will be displayed, select the RESET option and press ↵.



4 The CPU IP will reset and then display the first of the four initial configuration screens.

Part 2 – Remote configuration

The second part of the configuration requires you to log into the CPU IP from a system via either a network connection or a dial-up connection (via modem or ISDN). In either case there are two types of access applications that you can use:

- The VNC viewer – a small application supplied on the CD-ROM or downloadable from the RealVNC website or even downloadable from the CPU IP itself.

or

- A standard browser that supports Java – As soon as a web browser makes contact, the CPU IP downloads 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.

To perform the remote configuration

1. Use either the VNC viewer or a standard web browser to make remote contact with the CPU IP – see 'Connecting to the CPU IP' for more details.
2. If the username entry is not blanked out, enter 'admin'. Then enter the password that was set during the local configuration stage (if no password was set, then just press ↵). Once logged in, the CPU 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 configuration menu ⇩

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

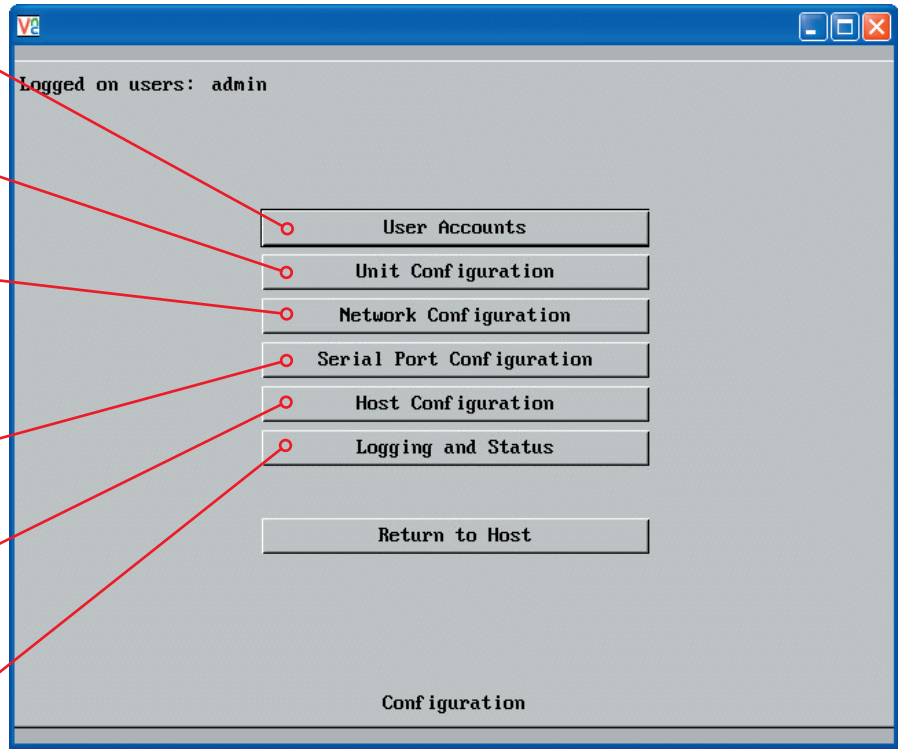
Unit configuration
Allows you to alter both basic and fundamental settings within the CPU IP.

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 modem and power control serial ports.

Host configuration
Allows you to configure user access, hot key switching and power control codes for up to 32 host systems that may be connected to the CPU IP via KVM switch units.

Logging and status
Provides various details about the user activity on the CPU IP.



Shaded items signify options that are not available at the local configuration stage.

Many of the options within the configuration menu duplicate those that were set (or are available) in the local configuration. However, there are numerous other settings that are only available here.

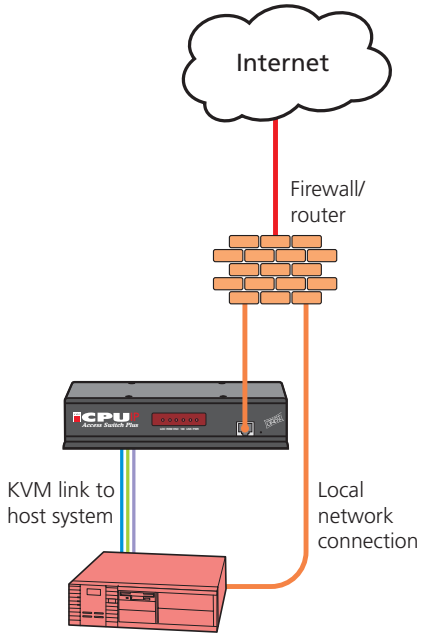
For more information about each menu option, please see Appendix 5 - Remote configuration menus in the 'Further information' chapter.

Networking issues

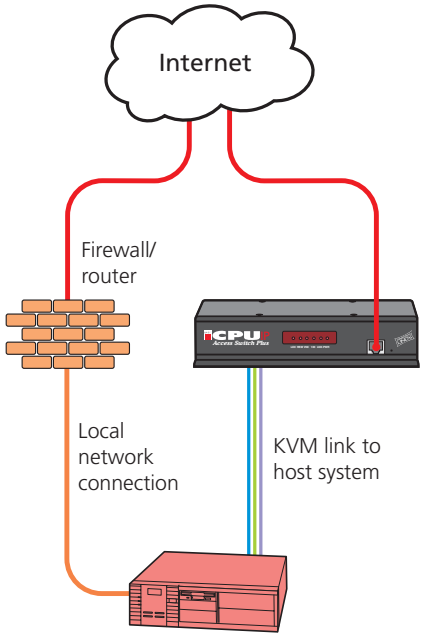
Thanks to its robust security the CPU IP offers you great flexibility in how it integrates into an existing network structure. The CPU IP is designed to reside either on an internal network, behind a firewall/router or alternatively with its own direct Internet connection.

Positioning CPU IP in the network

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



CPU IP situated behind the firewall



CPU IP situated alongside the firewall

IMPORTANT: When the CPU IP is accessible from the public Internet or dial up connection, you must ensure that sufficient security measures are employed.

Placing CPU IP behind a router or firewall

A possible point of contention between the CPU 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 CPU 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. LINDY 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 CPU 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 CPU IP correctly using only its network address. The firewall/router must be informed to transfer traffic, requesting these port numbers, through to the CPU IP.

When a web server is also on the local network

Port 80 is the standard port used by web (HTTP) servers. If the CPU 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 CPU IP must 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 CPU 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

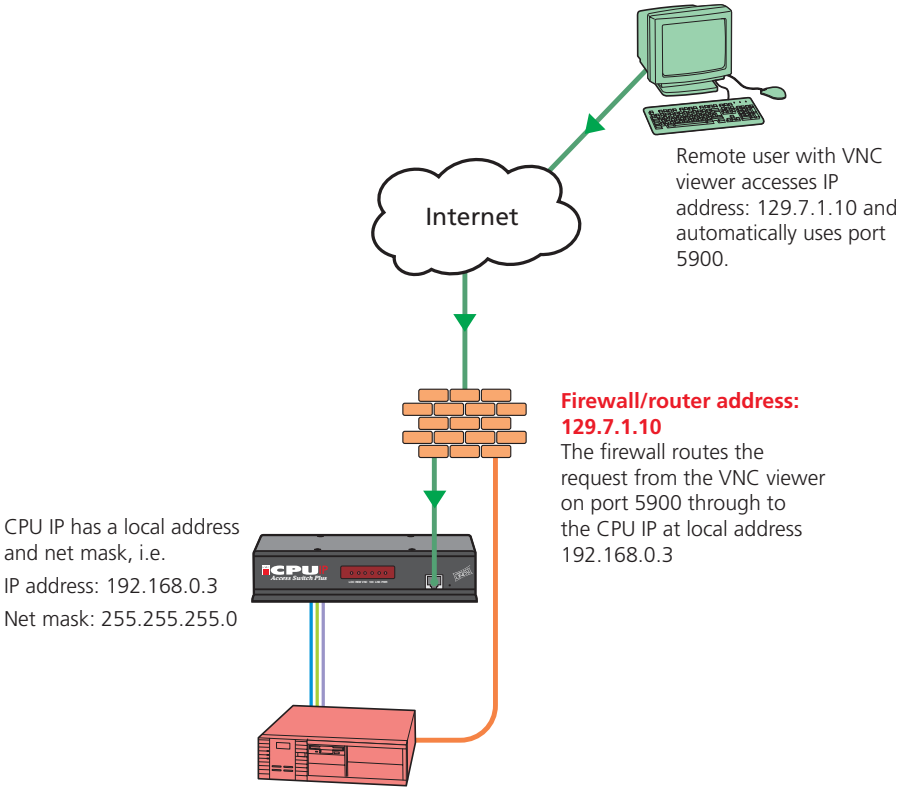
(Note the *double* colons that separate the IP address and port number).

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

Addressing

When the CPU IP is situated within the local network, you will need to give it an appropriate local IP address and IP network mask. 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 CPU 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 CPU IP via a network connection. To discover the allocated IP address:

1. In either the local or remote Network configuration screens, set the 'Use DHCP' option to 'Yes' and select 'Save'. Once the page is saved, the CPU 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 CPU 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 CPU IP's 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.

Placing CPU IP alongside the firewall

CPU 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. Therefore, you can position the CPU IP alongside the firewall and control hosts that are also IP connected within the local network.

IMPORTANT: If you make the CPU IP accessible from the public Internet or from a modem, 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 or limiting remote access to dial up connections only.

Ensuring sufficient security

The security capabilities offered by the CPU 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 or by remote configuration.
- Ensure that you have selected secure passwords with at least 8 characters and a mixture of upper and lower case and numeric characters.
  By remote configuration.
- 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 CPU IP to only those that you will need to use. To restrict IP access.
- Do NOT Force VNC protocol 3.3. Remote configuration.
- Add a further level of inherent security by restricting access only via modem or ISDN dialup.
- Ensure that the computer accessing the CPU 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 CPU IP from public computers.

Security can be further improved by using the following suggestions:

- Use a KVM switch with On-Screen-Display driven security access and an auto-logout (after inactivity) feature to provide a second level of security.
- Place the CPU IP behind a firewall and use port the numbers to route the VNC network traffic to an internal IP address.
- Review the activity log from time to time to check for unauthorized 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 CPU 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 CPU 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

Power switching configuration

Power switch configuration comprises two main steps:

- Configure the COM2 serial port to the same speed as used by the power switch box(es) - see Serial port configuration for details.
- Configure power ON and OFF strings for each relevant host computer.

For each power port there needs to be a valid 'Power ON string' and similarly an appropriate 'Power OFF string'. In each case, the strings are a short sequence of characters that combine a box address, a port number, a power on or off value and finally a checksum number so that the power unit can guard against data errors.

If a particular computer has more than one power input (and thus requires an equivalent number of power ports to control them), collections of strings can be combined to switch all of the required ports together as a group.

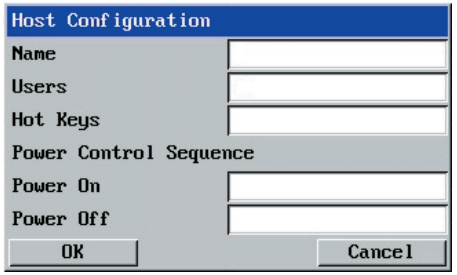
To configure the power sequences for each host computer

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.

4 Click one of the 32 host entry slots to display a Host configuration dialog:



5 If necessary, configure other parameters (Name, Users, Hot Keys - MORE).

6 Enter the **Power control sequences** in the Power On and Power Off fields ⇨

7 Click OK to close the dialog and then click the Save button in the main Host Configuration window to store the details.

Power control sequences

Note: The settings given below are for the LINDY power switch - other power switches may require different settings. Please refer to your power switch documentation for details about codes required by other power switches.

The structure of each power sequence (OFF and ON) is as follows:

\w\x\y\z

Where:

w is the switch box address (first box is 80, second box is 81, etc.),

x is '31' for ON or '32' for OFF,

y is the power port number (from 1 to 8, or 9 to switch all ports),

z is a checksum value - calculate this using the other values (subtract 80H from the switch box address and then perform an exclusive OR function between this and the other two values).

Note: All values are expressed in hexadecimal.

Thus for the first switch box, the codes that you would use in the Power On and Power Off fields would be as follows:

Port(s)	Power On	Power Off
1	\80\31\01\30	\80\32\01\33
2	\80\31\02\33	\80\32\02\30
3	\80\31\03\32	\80\32\03\31
4	\80\31\04\35	\80\32\04\36
5	\80\31\05\34	\80\32\05\37
6	\80\31\06\37	\80\32\06\34
7	\80\31\07\36	\80\32\07\35
8	\80\31\08\39	\80\32\08\3A
All	\80\31\09\38	\80\32\09\3B

For details about operating this feature, see Power control within the Operation chapter.

To control two ports simultaneously

You can control two power ports using a single sequence. This is done using the same command structure as shown above, plus a delay command. Immediately following a port command, insert the characters '*' before the next command. For instance, to switch on ports 1 and 2 in the first power switch, the command line would be:

\80\31\01\30*****\80\31\02\33

For more help with power switch addressing, please contact LINDY support.

Performing a flash upgrade

CPU IP is fully reconfigurable via flash upgrade.

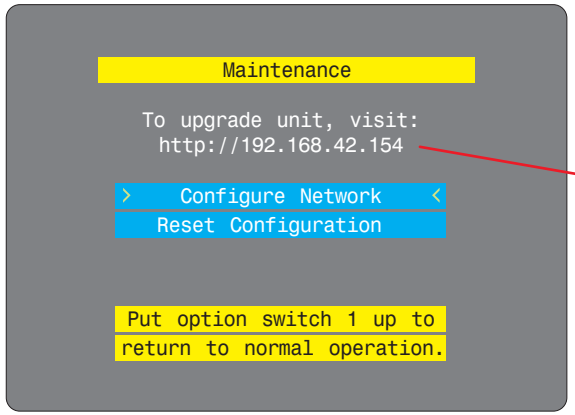
To perform a flash upgrade

1 Using a remote connection, log on as the admin user and access the Unit configuration page to determine the current firmware version of the CPU IP unit.

2 Please contact LINDY Support to get the latest firmware revision.

3 Power down the CPU IP unit. At the rear of the unit, adjacent to the power input socket, click mini switch 1 to its ON (down) position.

4 Re-apply power to the CPU IP. On the locally connected monitor you should see a Maintenance menu:

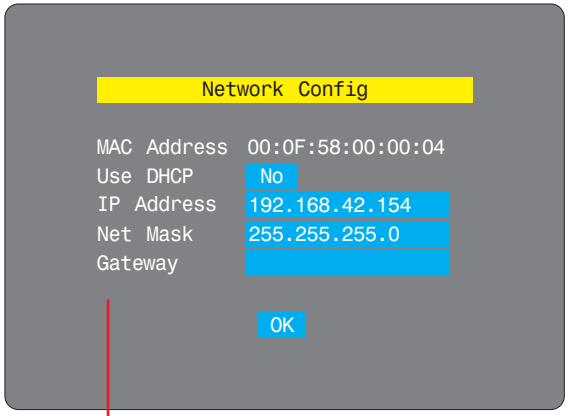


Current network address of the CPU IP

The Maintenance menu should display the current network address of the CPU IP.

- If the current network address is incorrect then select the 'Configure network' option to change it:

Configure network option



5 Use the web browser (not the VNC viewer) on the previously used remote system, connect to the network address shown in the local Maintenance menu.

6 Follow the on screen instructions to upload the firmware file (previously obtained from LINDY) to the CPU IP.

IMPORTANT: Wait until the upgrade is complete.

7 When the upload is complete and confirmed on screen, log off the remote system and then power down the CPU IP.

8 At the rear of the unit, return the mini switch 1 to its OFF position and then re-apply power.

MAC address
Media Access Control address – this is the unique and unchangeable code that was hard coded within your CPU 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
When this option is selected, your CPU IP will attempt to locate a DHCP server on the network. If such a server is located, it will supply three things to the CPU IP: an IP address, an IP network mask (also known as a Subnet mask) and a Gateway address.

IP address
This is the identity of the CPU IP within a network. It can either be entered manually or configured automatically using the DHCP option. When the DHCP option is enabled, this entry is greyed out.

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.

Gateway
This is the address of the device that links the local network (to which the CPU 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.

Operation

Connecting to the CPU IP

The CPU IP offers you three ways to connect:

- Local connection,
- Remote connection by network link,
- Remote connection by direct dial up (modem or ISDN) link,

...and two types of viewer:

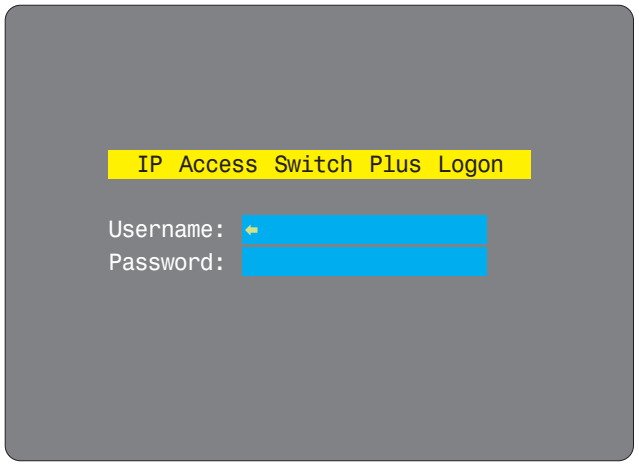
- VNC viewer,
- Standard web browser.

Local connection

The keyboard, video monitor and mouse connected directly to the CPU IP offer password protected access to the host computer(s).

To make a local connection:

1 Using the keyboard connected directly to the CPU IP, press any key to exit the screensaver and display the logon prompt.

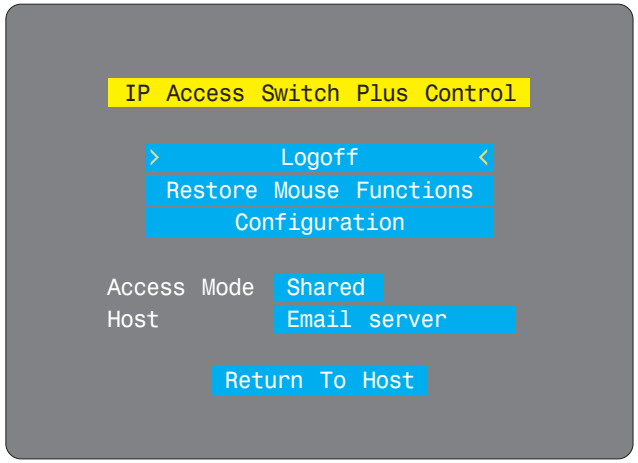


2 Enter your username and password. Providing you have the correct permissions, the screen will display the currently selected host computer.

To view the local control menu

1 Press and hold the hotkeys (usually Ctrl and Alt), then press C and finally release all three keys.

Note: The Ctrl and Alt keys when pressed in combination are called 'hotkeys' and they signal to the CPU 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 C combination fails to work, then please contact the system administrator for details.



The local control menu contains numerous options, the most useful of which are:

- **Access mode** - Allows you to select a 'Private' mode in order to prevent other logged on users from viewing your actions on the host computer. Use → and ← to change between modes.
  Note: For the courtesy of other users, this mode should be used sparingly. The admin user has the ability to overrule the private setting.
- **Host** - Where more than one host computer is available via the CPU IP, this option allows you to easily switch between them. Use → and ← to change between host computers.
- **Return to host** - Quits the control menu and displays the host computer screen.

Local connection (continued)

To avoid the 'hall of mirrors' effect

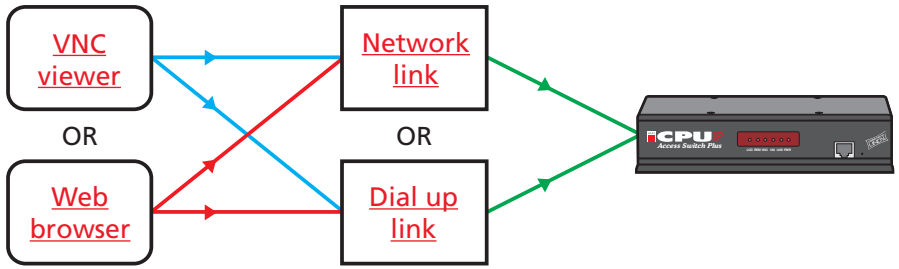
IMPORTANT: Never configure a system so that your viewer is viewing itself.

When controlling a host computer using the locally connected keyboard, video monitor and mouse, it is possible to use the VNC viewer or a browser (if the host computer is networked) to create a remote link back to itself. This will set up a 'hall of mirrors' effect, where the computer is viewing itself into infinity.

While technically possible, the CPU IP unit is not designed to withstand this treatment and could sustain damage.

Remote connections

From a remote system, you connect to the CPU IP using a viewer and a link. There are two types of viewer and two types of link, which can be used in any combination.



Remote connection by VNC viewer

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

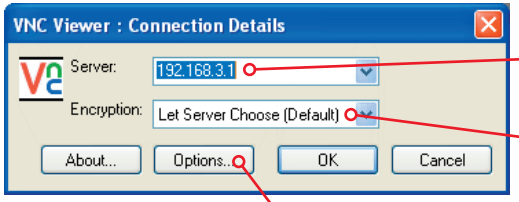
- from the CPU IP installation CD
- from the CPU IP itself
- from the LINDY website
- from the RealVNC website

To connect using the VNC viewer

1 Locate and select the VNC viewer icon ⇨ 

- If you are using a dial up link.

A connection details dialog will be displayed:



Enter the CPU IP address here and click OK

If required, select the encryption mode - MORE [+]

Options button
Provides a range of viewer and connection settings - MORE [+]

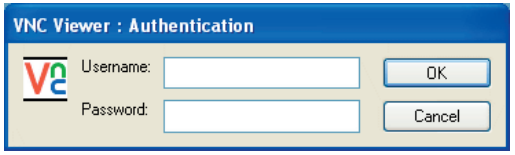
2 In the 'Server:' entry, type the address of the CPU IP as follows:

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.*

Remote connection by Web browser

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

To connect using your Web browser

1 Launch your standard Web browser as usual.

- If you are using a dial up link.

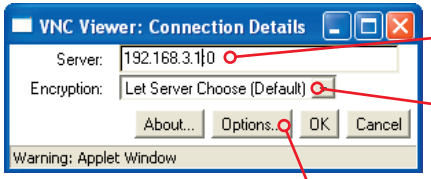
2 In the Address section, type the address of the CPU IP as follows:

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. 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:



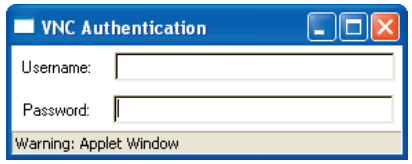
The previously entered CPU IP address will be shown here

If required, select the encryption mode - MORE [+]

Options button
Provides a range of viewer and connection settings - MORE [+]

4 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.

5 A second connection attempt will be made and if successful, an authentication dialog will be displayed:



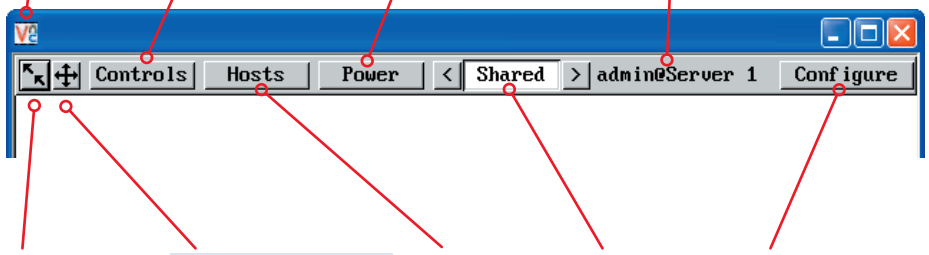
6 Enter your username and password. The viewer window should now open and show the current host computer. *Note: If the Username entry is blanked out then only admin user account is currently defined and only a password is required.*

Using the viewer window

The viewer window gives you the ability to view and control the CPU 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 CPU IP configuration.



Viewer options
(VNC viewer only) Click the VNC icon to view the viewer window options

Controls
Displays a menu of options concerning keyboard, video and mouse operation.

Power
Click to access the power on/off options for the current host computer.

Dialogue area
Indicates your username and the host system that you are currently viewing. This area can also display other messages.

Re-sync mouse
Ensures that the mouse pointer which you move and the mouse pointer on the host system are correctly synchronised.

Auto calibrate
Determines the optimum video and mouse settings for the currently selected host computer. This button will flash red when a new host screen is encountered. Click this button when you first visit a new screen.

Hosts
Click to display a list of hosts. Choose an entry to connect to that host computer.

Access mode
Allows you to choose between Shared and Private access modes.

Configure
This option is only available to the admin user and provides access to the main configuration menus.

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, as described next.

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 CPU 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.

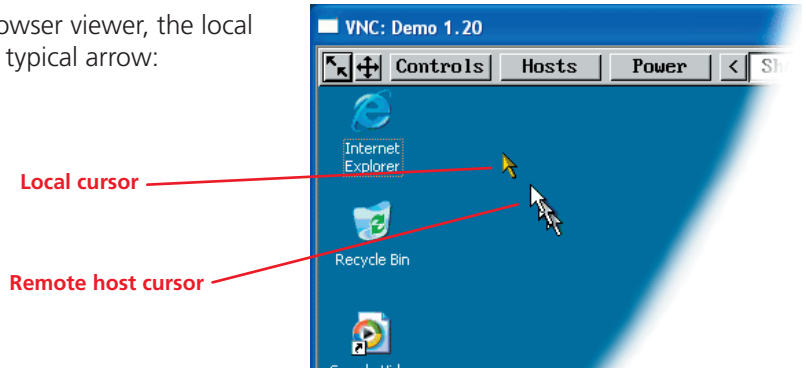
Fewer colours
Select the Low (64 colours) mode. The Very low option offers hardly any improvement and looks a lot worse.

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.

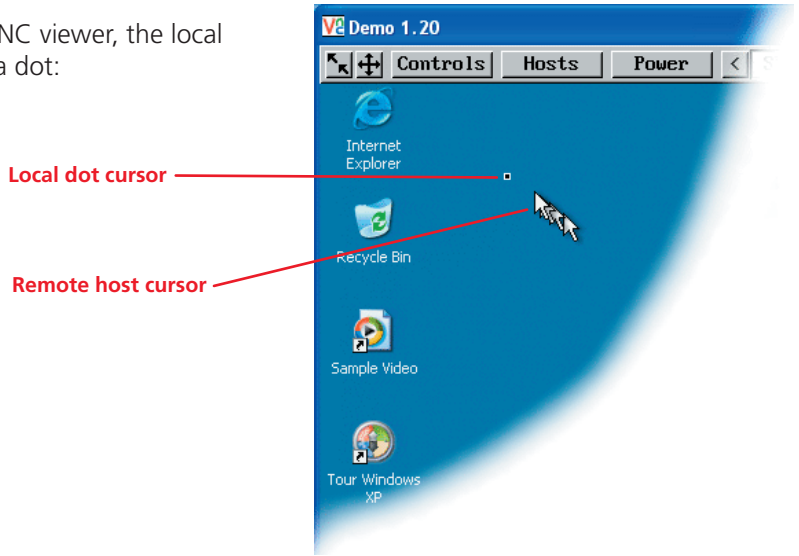
Mouse pointers

Both viewers use 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:



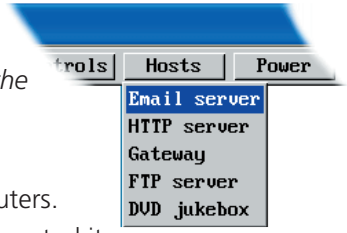
For the VNC viewer, the local cursor is a dot:



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 KVM switch hotkey combinations or the KVM switch on screen display.

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.
2. Click the required computer name to view and control it.

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 CPU IP settings.

See Appendix 5 - Remote configuration menus 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 by flashing red when it encounters a new computer screen. 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 that there are no on-screen displays generated by KVM switches (such as host names or menus). This is because they may confuse the calculation and can result in a lower overall performance level. For the mouse calibration part, 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 system does not have the mouse cursor trails option enabled.

To auto calibrate the screen and 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.

   The screen will appear to freeze for approximately 10 to 60 seconds as the necessary calculations are made. Operation will return as soon as the calculations are complete.

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 remote users plus one local 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.

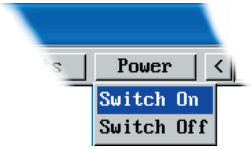
Power control

When configured (and where you have access rights) this option allows you to control the mains power input to the currently selected host computer.

Note: This option is generally used to power cycle remote systems that have failed to respond. Before switching a system off, ensure that all attempts have first been made to power it down through normal means.

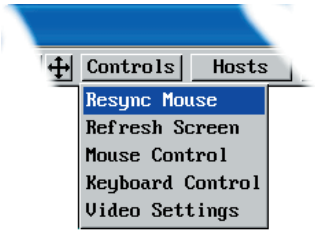
To switch a system on or off

1. Use the Hosts button to select the required computer.
2. Click the Power button and then select the Switch on or Switch off option, as appropriate.



Controls

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



Resync mouse

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

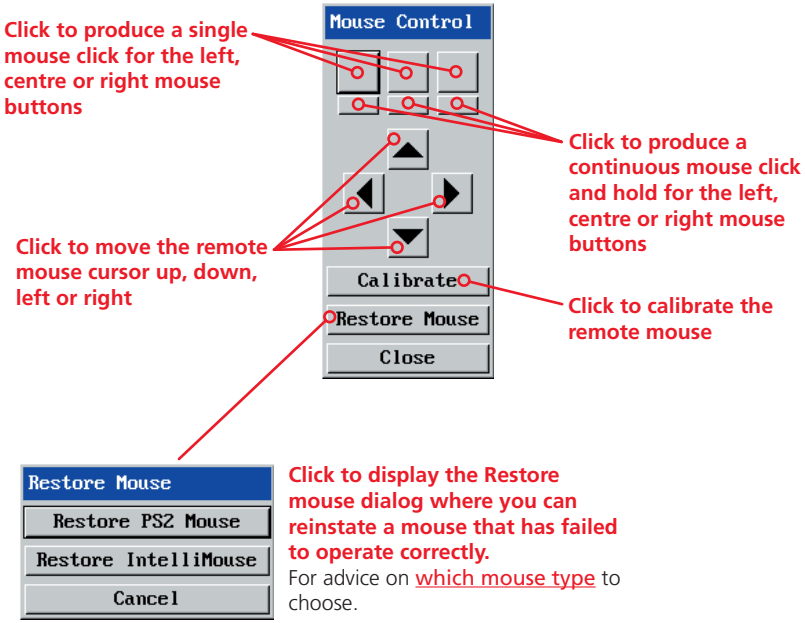
Refresh screen

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.

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.

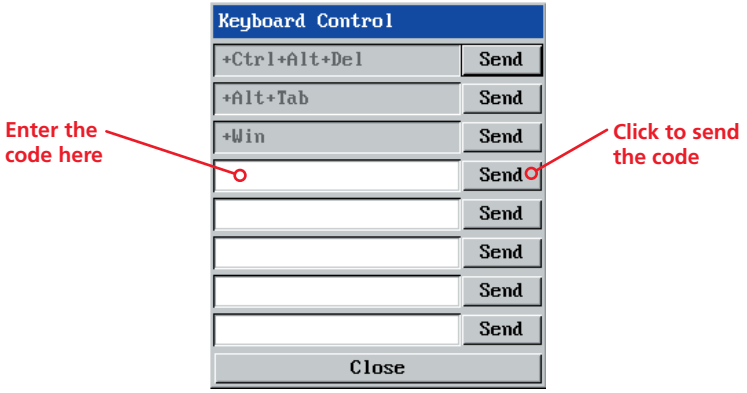
The mouse control dialog allows you to control the remote mouse cursor using a selection of buttons that you click with your local mouse.



Click to display the Restore mouse dialog where you can reinstate a mouse that has failed to operate correctly.
For advice on which mouse type to choose.

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 CPU IP.



When entering codes:

+ means press and hold down the named key,

– means release the named key.

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

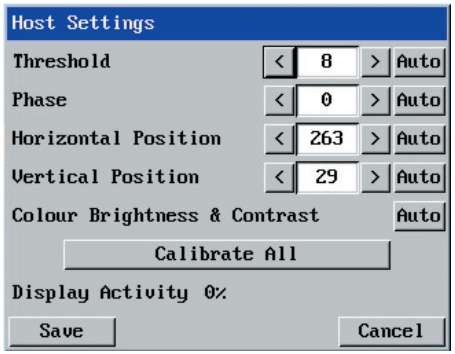
see next page

Video settings

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



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

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

Colour, brightness & contrast
Provides an automatic setting button to optimise these three important video constituents 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.

All settings can be individually subjected to an auto configuration (click the appropriate 'Auto' button) and most 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, ensure that there are no on-screen display elements generated by any connected KVM switch (such as a host name label or menu). Due to the differing video rates of these items compared to the video image from the host itself this can confuse the calibration process into giving a much higher Threshold rate than is necessary, thus worsening the screen artefacts.

Setting the Threshold manually
Occasionally it can be useful to manually adjust the Threshold setting, such as when there is a KVM switch OSD banner that cannot be easily removed from the display.

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.

Connecting via dial up (modem or ISDN) link

When you use a modem or ISDN link to make the connection, the CPU IP uses standard network protocols to create a private two-device network. This approach ensures consistency and allows you to use exactly the same VNC viewer or browser to view the hosts systems. This is achieved using PPP (Point to Point Protocol) and means that you need to use a dial-up networking method to initiate the connection. Such software is standard with operating systems such as Windows, Linux and Mac OS.

To initiate a dial up link

1. Using a system that has a modem or ISDN adapter installed, locate the dial-up networking option on your system. Please refer to your system documentation for more information.
2. Using the dial-up networking option, enter the telephone/ISDN number where the CPU IP can be contacted.
3. Initiate the call and when the link is made, continue with either the standard VNC viewer or browser connection.

   Note: For the viewer network connection address, you must use the IP address that the admin user has set as the Server address (or PPP server IP address) within the Modem configuration screen.

Downloading VNC viewer from the CPU IP

The CPU 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 CPU IP is situated (in the form: http://192.168.0.3) and make the link.
3. In the opening CPU 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 CPU IP using the VNC viewer application.

If you need to enter a port number

Usually, when you make a network connection to the CPU 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 115900), i.e. http://192.168.0.3::115900
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 CPU IP to which you are connecting is configured:

- Always on - This setting will ensure that the link is encrypted, regardless of the CPU IP encryption setting.
- Let server choose - This setting will follow the configuration of the CPU IP. If the CPU 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 CPU IP will allow it, otherwise it will be encrypted.
- Prefer on - If the CPU 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 CPU 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 - see below
- Getting assistance - see right
- Appendices
  - Appendix 1 - Local configuration menus
  - Appendix 2 - VNC viewer connection options
  - Appendix 3 - VNC viewer window options
  - Appendix 4 - Browser viewer options
  - Appendix 5 - Remote configuration menus
  - Appendix 6 - Addresses, masks and ports
  - Appendix 7 - Cable specifications
  - Appendix 8 - Hotkey sequence codes
- Safety information
- Warranty
- End user licence agreement
- Radio frequency energy statements

Troubleshooting

Remote network users are unable to contact the CPU 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 CPU 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 CPU 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:

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

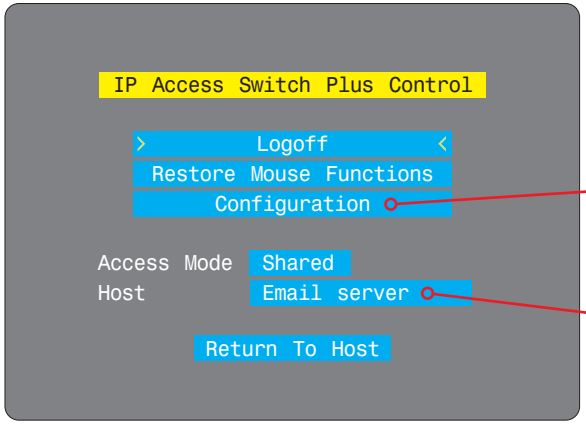
Appendix 1 - Local configuration menus

This section covers the control menus that are available when you are using the locally connected keyboard, video monitor and mouse.

To access the local configuration menus

- On the locally connected keyboard, simultaneously press Ctrl Alt C.

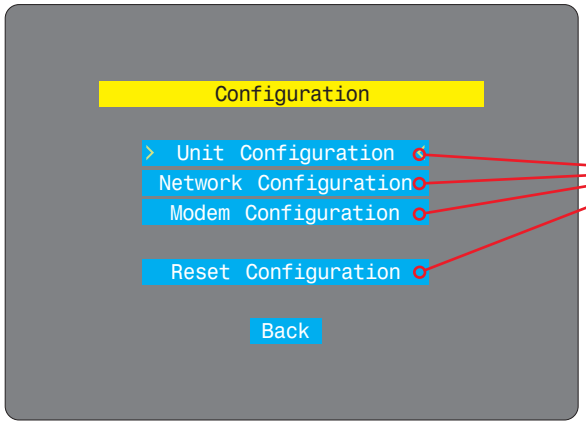
  Note: If the standard hotkeys (CTRL + ALT) have been changed, then you need to use those keys together with C to access the menus.



If you are not logged on as the 'admin' user then the Configuration menu will not be available.

Use the Host entry to switch to the required host computer (when a KVM switch is used).

Select the 'Configuration' option to display:

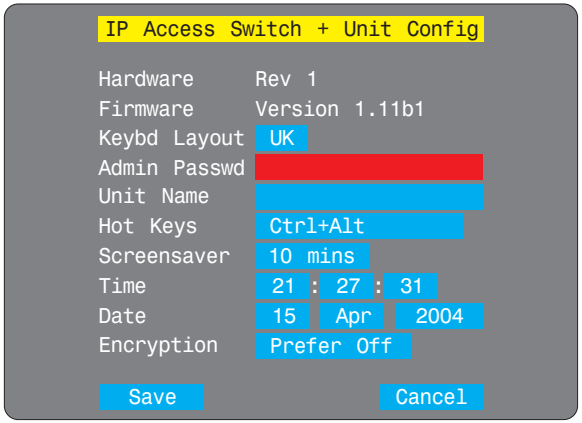


Select the required option:

- Unit configuration
- Network configuration
- Modem configuration
- Reset configuration

Unit configuration

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



To get here

1. Use the local keyboard and log on as the 'admin' user.
2. Press Ctrl Alt C (hotkeys may be different).
3. Select 'Configuration'.
4. Select 'Unit configuration'.

Keybd 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 CPU 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.

Hot keys

Use the left and right arrow keys to select an appropriate hot key sequence for the locally connected keyboard. This sequence is used in combination with other keypresses to access the on-screen menus and to change between hosts. The options are: Ctrl+Alt (default), Ctrl+Shift, Alt+Shift, Alt Gr, Left + Right Alt, Left Ctrl + Alt or Right Ctrl + Alt.

Screensaver

Use the left and right arrow keys to select an appropriate period of inactivity on the local keyboard or mouse before a screensaver is displayed and the user is logged out. This setting applies to local users only and once the screensaver is displayed, for security purposes the user is required to log in again. The timeout period can be selected between 5 minutes and 1 day (24 hours), it cannot be disabled. *Note: The Idle timeout option serves a similar purpose for remote connections.*

Time and date

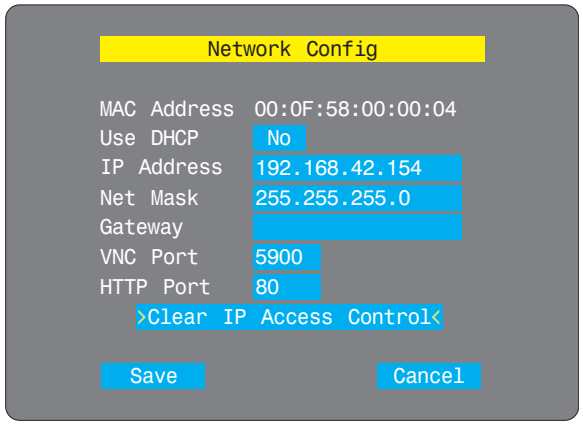
Use the left and right arrow keys to select the correct time and date. The time entry uses the 24 hour clock notation. The internal real time clock will continue to run for roughly one week without power to the CPU IP, after that it will be lost and require resetting. Use the up and down arrow keys to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

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. Use the local keyboard and log on as the 'admin' user.
2. Press Ctrl Alt C (hotkeys may be different).
3. Select 'Configuration'.
4. Select 'Network configuration'.

MAC address

Media Access Control address – this is the unique and unchangeable code that was hard coded within your CPU 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 CPU IP will attempt to locate a DHCP server on the network. If such a server is located, it will supply three things to the CPU 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 CPU IP remains connected and switched on. Discover allocations.

IP address

This is the identity of the CPU IP within a network. The IP address can be thought of as the telephone number of the CPU 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.

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.

Gateway

This is the address of the device that links the local network (to which the CPU 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 CPU IP will "listen" for both types of traffic on the single port.

HTTP port

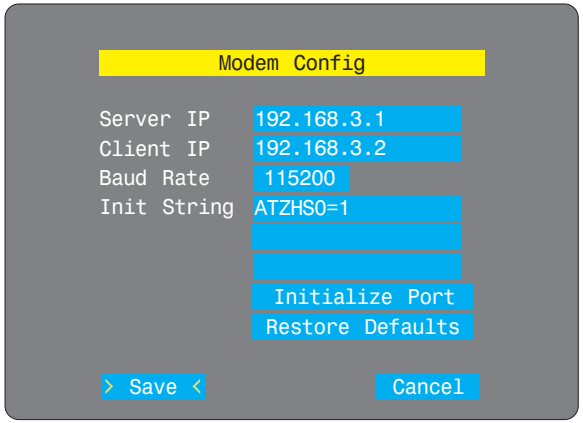
This is the logical link through which communications with a remote web browser will be channelled. The default setting of 80 is an established standard for web (HTTP – HyperText Transfer Protocol) traffic though this can be changed to suit your local network requirements.

Clear IP access control

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

Modem configuration

This page allows you to configure the COM1 serial port located at the rear of the CPU IP.



To get here

1. Use the local keyboard and log on as the 'admin' user.
2. Press Ctrl Alt C (hotkeys may be different).
3. Select 'Configuration'.
4. Select 'Modem configuration'.

Server IP / Client IP
When a user dials into the CPU IP via a modem or ISDN adapter, the CPU IP sets up a temporary two-device network using PPP (Point to Point Protocol). For this purpose, both devices must have 'dummy' IP addresses so that they can communicate correctly. These two addresses can be almost anything expressed in the quad octet format (i.e. 192.168.3.1.). However, it is advisable not to make them the same as the real IP addresses used by either the remote system or the CPU IP.

Baud rate
This option configures the speed of the serial connection between the CPU IP and a connected modem or ISDN terminal adapter. The default setting is 115200. The other communication settings are fixed as: No parity, 8 bit word, 1 stop bit.

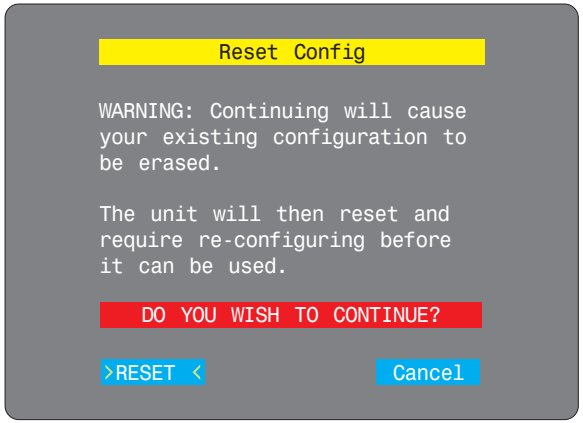
Init string
The codes entered here are used to prepare the connected modem or ISDN terminal adapter for use with the CPU IP. The default code is a Hayes-compatible string to configure auto answer mode and would be understood by the vast majority of modem/ISDN devices. The code is sent when the CPU IP is first switched on or whenever the Initialize button is clicked.

Initialize port
When selected, this option sends the characters entered in the 'Init string' field to the connected modem or ISDN terminal adapter.

Restore Defaults
When selected, this option resets the 'Baud rate' and 'Init string' values to their original default settings.

Reset configuration

This option allows you to completely reset the CPU IP.



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

To reset the CPU IP configuration

1 With the RESET option highlighted, press ↵.
2 The first screen of the initial configuration process will be displayed. See Initial configuration for details.

To get here

1 Use the local keyboard and log on as the 'admin' user.
2 Press Ctrl Alt C (hotkeys may be different).
3 Select 'Configuration'.
4 Select 'Reset configuration'.

Clear IP access control

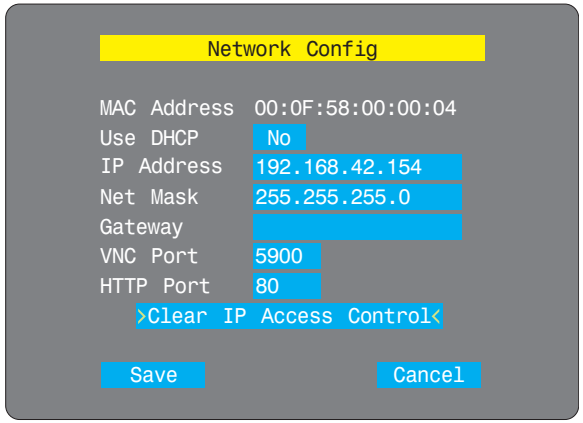
This option removes all entries from the IP access control feature within the CPU IP.

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 CPU IP. If set incorrectly, it is possible to exclude all network users and so this option provides an emergency recovery point.

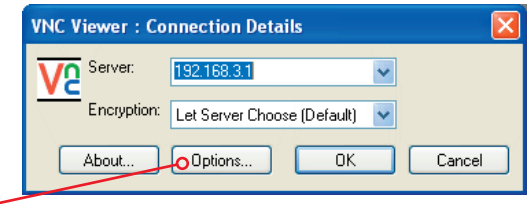
To clear IP access control

1. Use the local keyboard and log on as the 'admin' user.
2. Press Ctrl Alt C (hotkeys may be set differently).
3. Select 'Configuration'.
4. Select 'Network configuration'.
5. Highlight the 'Clear IP access control' option and press ↵.



Appendix 2 - VNC viewer connection options

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

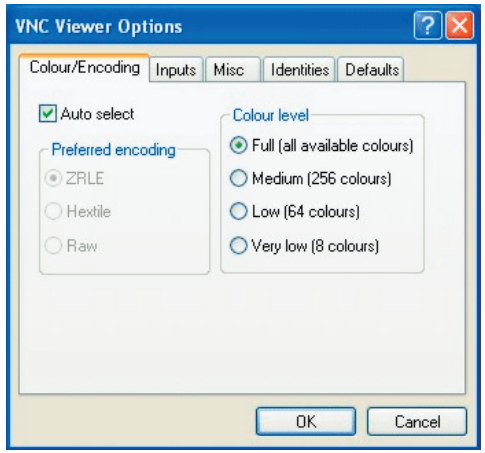


Click here to access the options

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 'Defaults' tab and click the 'Save as defaults' button.

There are five tabbed pages of options:

Colour/Encoding



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

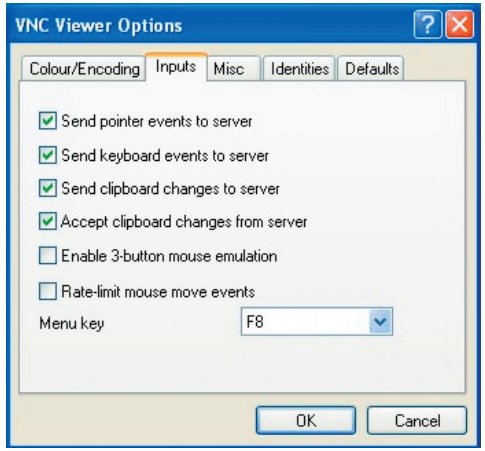
Preferred encoding
There are three manually selectable encoding methods which are accessible when the Auto select option is unticked.

- **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 CPU 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 CPU 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.

Inputs



Send pointer events to server
When un-ticked, the VNC viewer will not send mouse movement or click data to the CPU IP or host system.

Send keyboard events to server
When un-ticked, the VNC viewer will not send keyboard information to the CPU IP or host system.

Send clipboard changes to server
This feature is restricted to software server versions of VNC and has no effect on CPU IP installations.

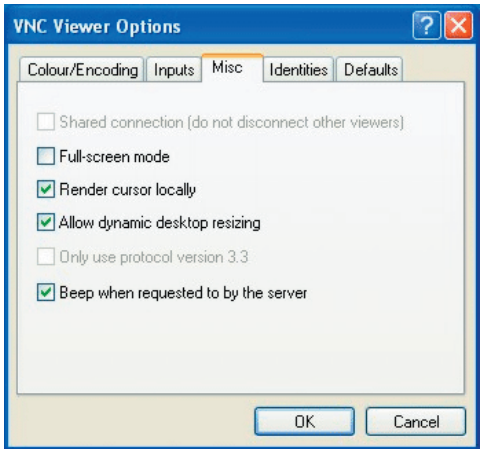
Accept clipboard changes from server
This feature is restricted to software server versions of VNC and has no effect on CPU IP installations, except for retreiving the activity log as desribed in the logging and status section.

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.

Rate-limit mouse move events
When ticked, this feature reduces the mouse movement information that is sent to the CPU 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.

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.

Misc



Shared connection (do not disconnect other viewers)
This option does not apply to CPU 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.

Render cursor locally
This option does not currently apply to CPU IP connections.

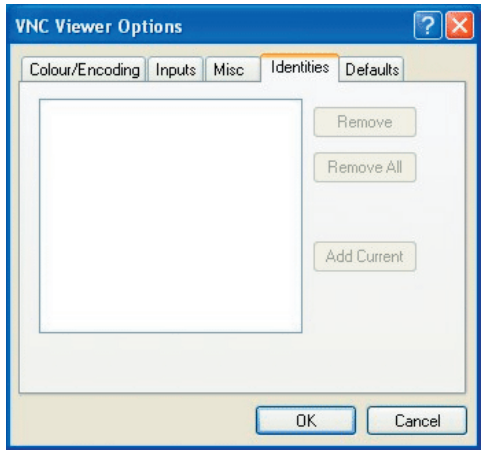
Allow dynamic desktop resizing
When ticked, the viewer window will be automatically resized whenever the host system's screen resolution is altered.

Only use protocol version 3.3
This option does not apply to CPU 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 CPU IP.

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 'Defaults' tab and click the 'Save as defaults' button.

Identities

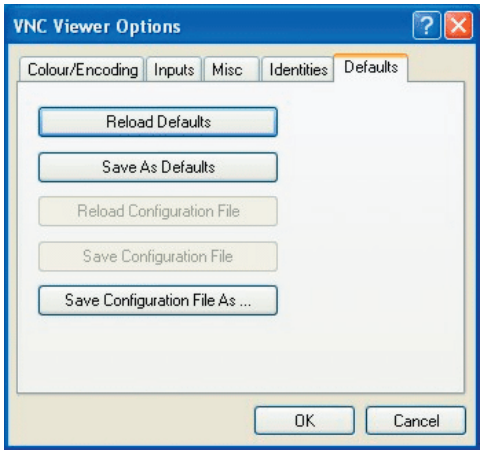


This feature helps your VNC viewer to confirm that a revisited CPU IP is genuine and not another device masquerading as a CPU IP. The list given will retain the identities of all visited CPU IP units (that have full security enabled).

When you first make a secure connection to the CPU IP, the security information for that CPU IP unit is cached within this Identity tab (i.e. the CPU IP's "identity" is known). The next time that you connect to the CPU 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 CPU 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.

Defaults



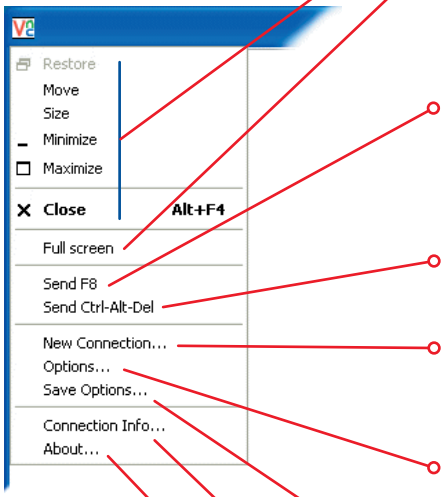
Reload defaults
When clicked, all connection options are returned to the default settings that are currently saved.

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

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

Appendix 3 - 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.

Send F8
Passes the F8 function key code to the CPU IP and host system. This is necessary because F8 is trapped by the VNC viewer for use as the trigger for this options menu.

Send Ctrl-Alt-Del
Passes a Ctrl-Alt-Del sequence to the host system.

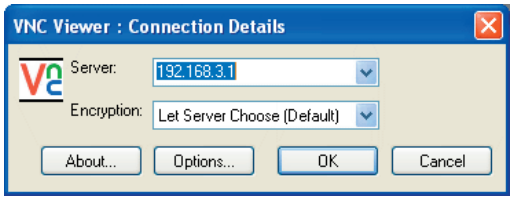
New connection...
Displays the connection dialog so that you can log on to a different CPU IP or VNC server location.

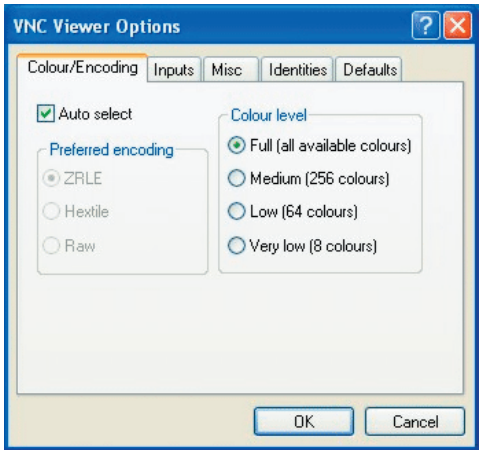
Options...
Displays the full range of connection options - see Appendix 2 for more details.

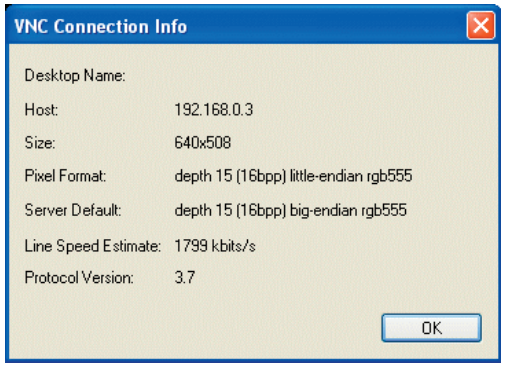
Save options...
Allows you to save the current VNC connection options for use during the next session.

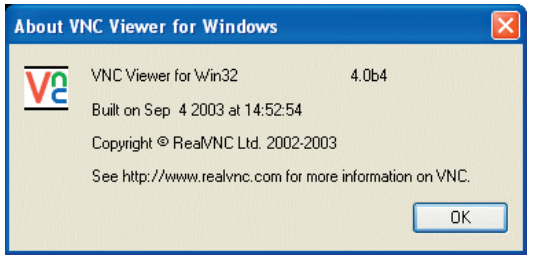
Connection info...
Displays various connection and display details.

About...
Displays information about your VNC viewer.



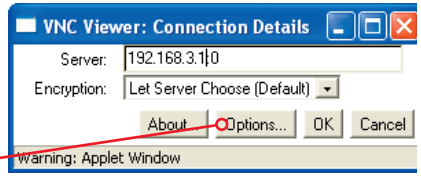






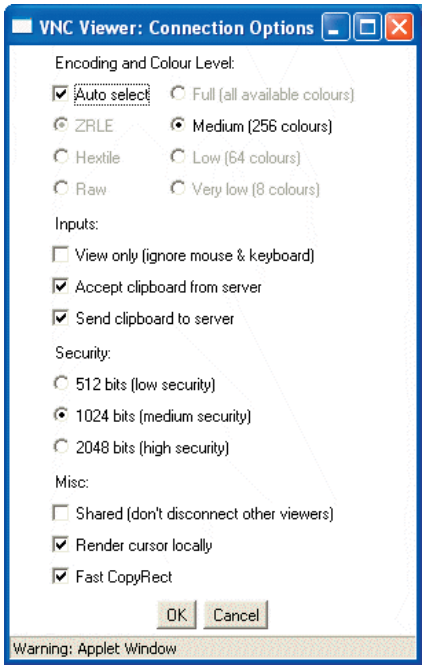
Appendix 4 - Browser viewer options

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



Click here to access the options

There is a single page of options:



Encoding and colour level

Auto select
When ticked, this option will examine the speed of your connection to the CPU 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 CPU 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 CPU IP or host system.

Accept clipboard from server
This feature is restricted to software server versions of VNC and has no effect on CPU IP installations.

Send clipboard to server
This feature is restricted to software server versions of VNC and has no effect on CPU IP installations.

Security

512 bits (low security)
Selects the lowest level of encoding for communications between the browser and the CPU IP.

1024 bits (medium security)
Selects the middle level of encoding for communications between the browser and the CPU IP.

2048 bits (high security)
Selects the highest level of encoding for communications between the browser and the CPU IP.

Misc

Shared (don't disconnect other viewers)
This feature is restricted to software server versions of VNC and has no effect on CPU IP installations.

Render cursor locally
This feature is restricted to software server versions of VNC and has no effect on CPU IP installations.

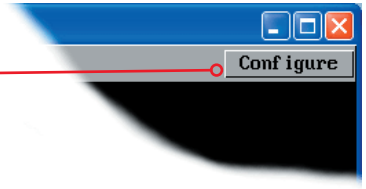
Fast CopyRect
This feature is restricted to software server versions of VNC and has no effect on CPU IP installations.

Appendix 5 - Remote configuration menus

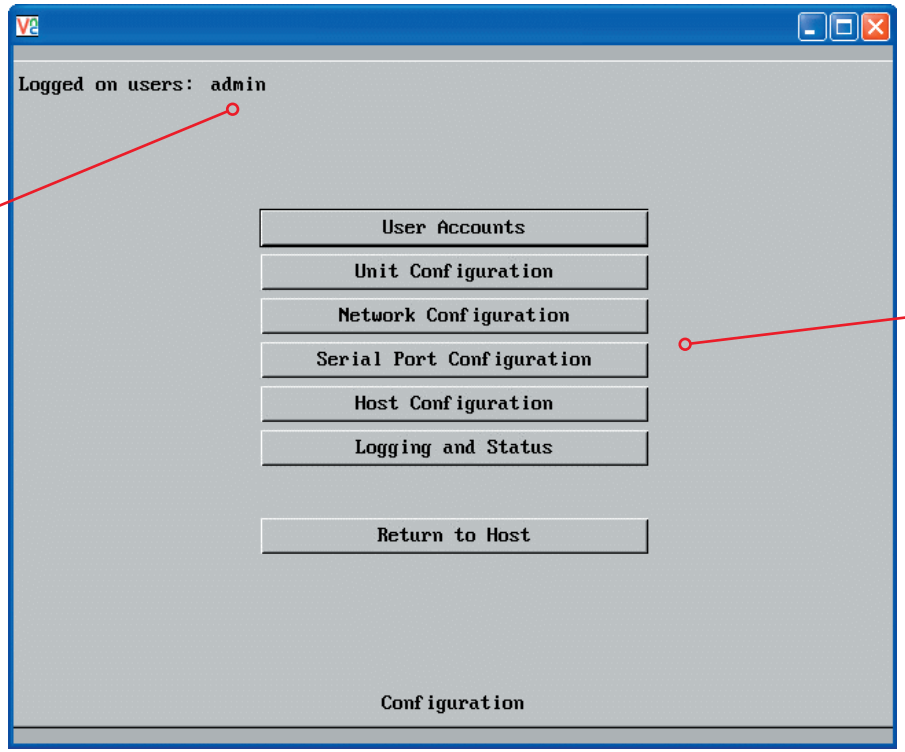
This section covers the configuration menus that are available to remote admin users using either the VNC viewer or the browser methods of access.

To access the remote configuration menus

- Click the Configure button in the top right corner of the window when logged on as the admin user.



Main configuration menu



Logged on users
Indicates the current users irrespective of whether they are connected locally, by modem/ISDN or via a network.

Click the required option

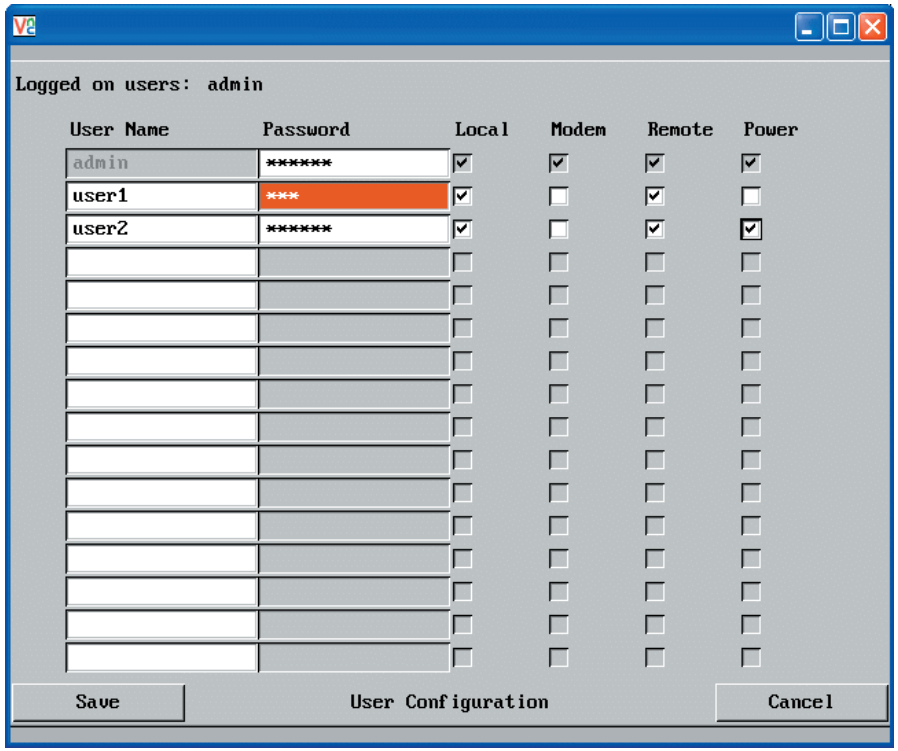
- User accounts
- Unit configuration
- Network configuration
- Serial port configuration
- Host configuration
- Logging and status

User accounts

This section 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.



To create a new 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, Modem, Remote and Power 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 CPU 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.

Local
When ticked, the selected user can gain access using the local KVM console directly connected to the CPU IP.

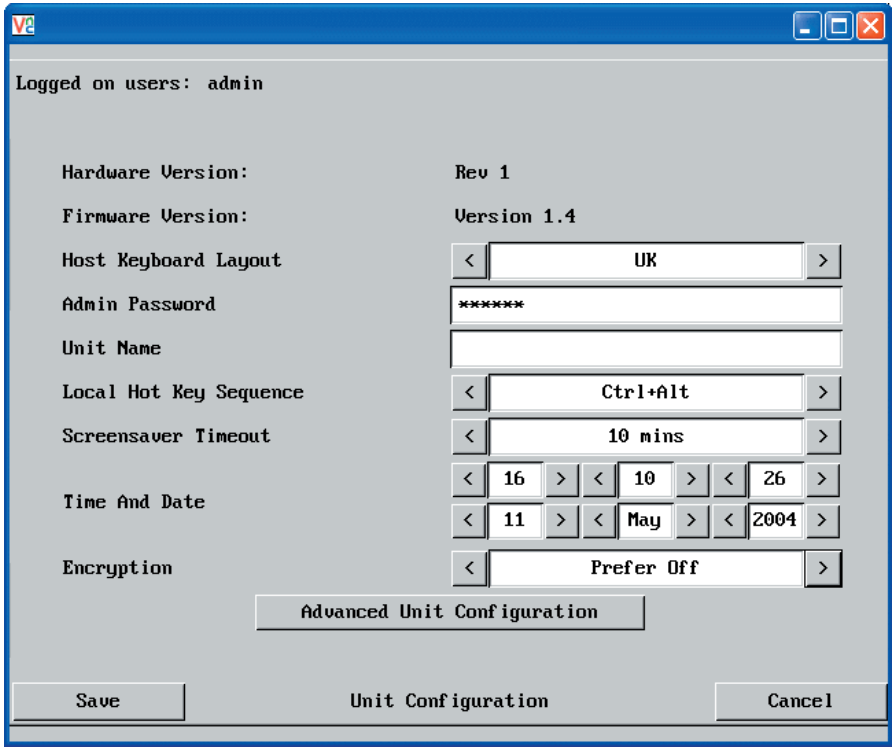
Modem
When ticked, the selected user can gain access via a modem or ISDN link (requires external modem/ISDN equipment to be connected to the CPU IP).

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 CPU IP is connected).

Power
When ticked, the selected user will be permitted to control the power input to host systems (requires optional power control switch unit(s) to be fitted).

Unit configuration

This page provides access to a selection of both basic and fundamental settings for the CPU IP. Many of the settings displayed here are also accessible through the on-screen menu on the locally attached keyboard, mouse and monitor.



Hardware Version

Indicates the version of the electronic circuitry within the CPU IP unit.

Firmware Version

Indicates the version of the hardwired software within the CPU IP's 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 CPU 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/browser windows.

Local hot key sequence

Use the arrow buttons to select an appropriate hot key sequence for the locally connected keyboard. This sequence is used in combination with other keypresses to access the on-screen menus and to change between hosts. The options are: Ctrl+Alt (default), Ctrl+Shift, Alt+Shift, Alt Gr, Left + Right Alt, Left Ctrl + Alt or Right Ctrl + Alt.

Screensaver timeout

Use the arrow keys to select an appropriate period of inactivity before a screensaver is displayed and the user is logged out. This setting applies to local users only and once the screensaver is displayed, for security purposes the user is required to log in again. The timeout period can be selected between 5 minutes and 1 day (24 hours), it cannot be disabled.

Time and date

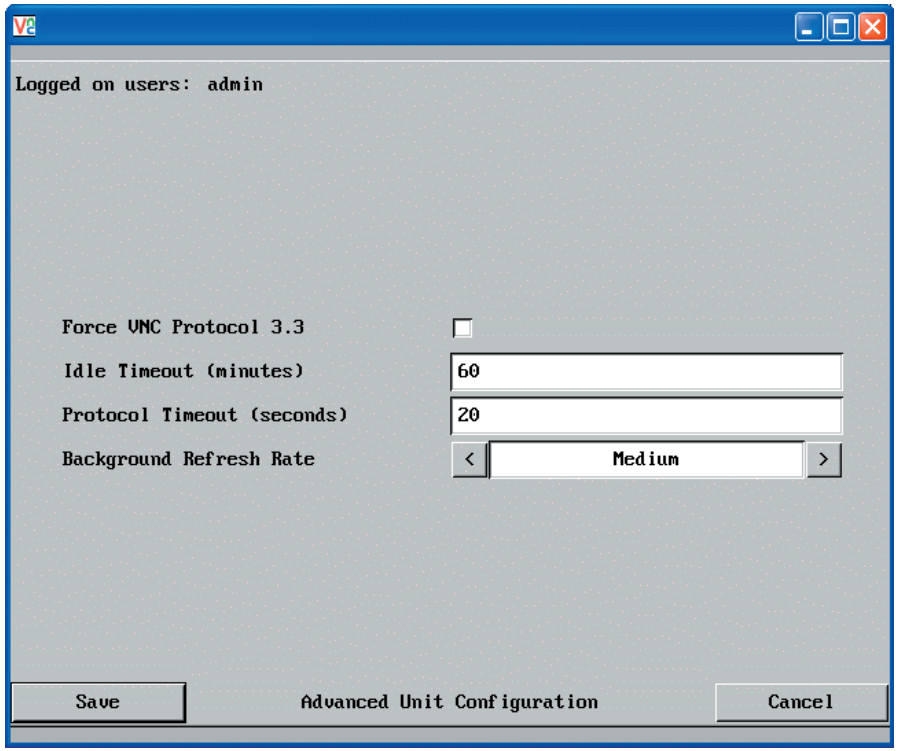
Use the arrow keys to select the correct time and date. The time entry uses the 24 hour clock notation. The internal real time clock will continue to run for roughly one week without power to the CPU IP, after that it will be lost and require resetting.

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

Click this button to display several 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 remote 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.

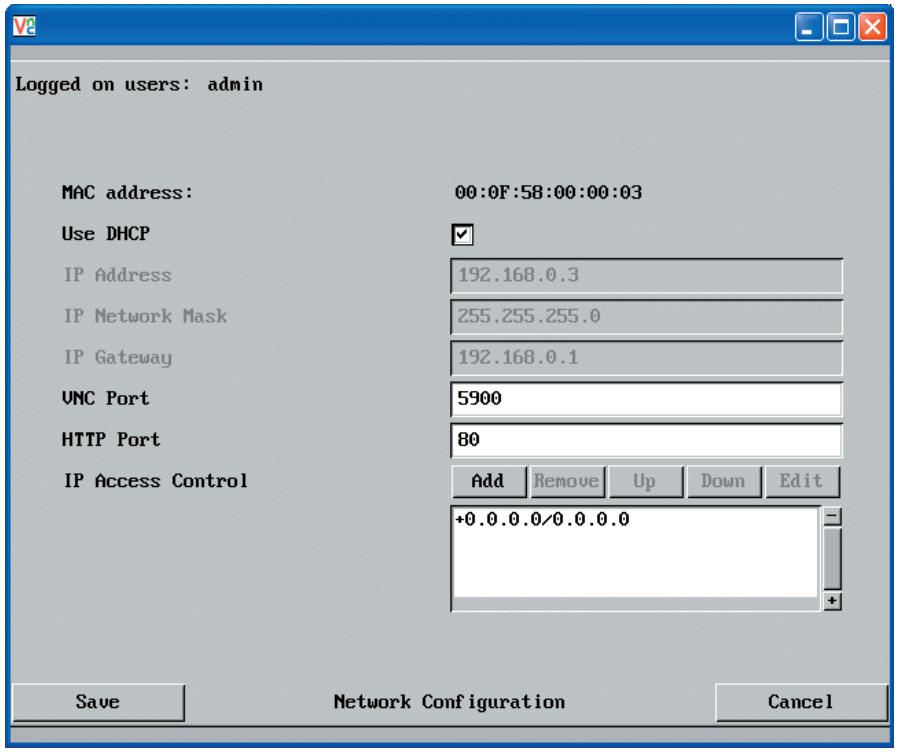
Background refresh rate

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 connections speed is detected, the background refresh is automatically disabled, regardless of the settings of this option.

Network configuration

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



MAC address

Media Access Control address – this is the unique and unchangeable code that was hard coded within your CPU 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 CPU IP will attempt to locate a DHCP server on the network. If such a server is located, it will supply three things to the CPU 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 CPU 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 CPU IP within a network. The IP address can be thought of as the telephone number of the CPU 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 CPU 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 CPU 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 Clear IP access control for details about how to regain access.

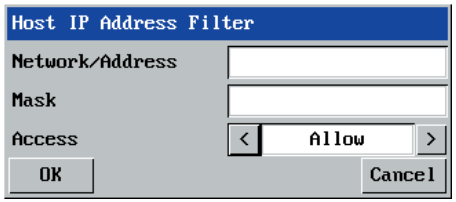
In the list, access control addresses prefixed by '+' are allow entries while those prefixed by '– ' are deny entries.

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.

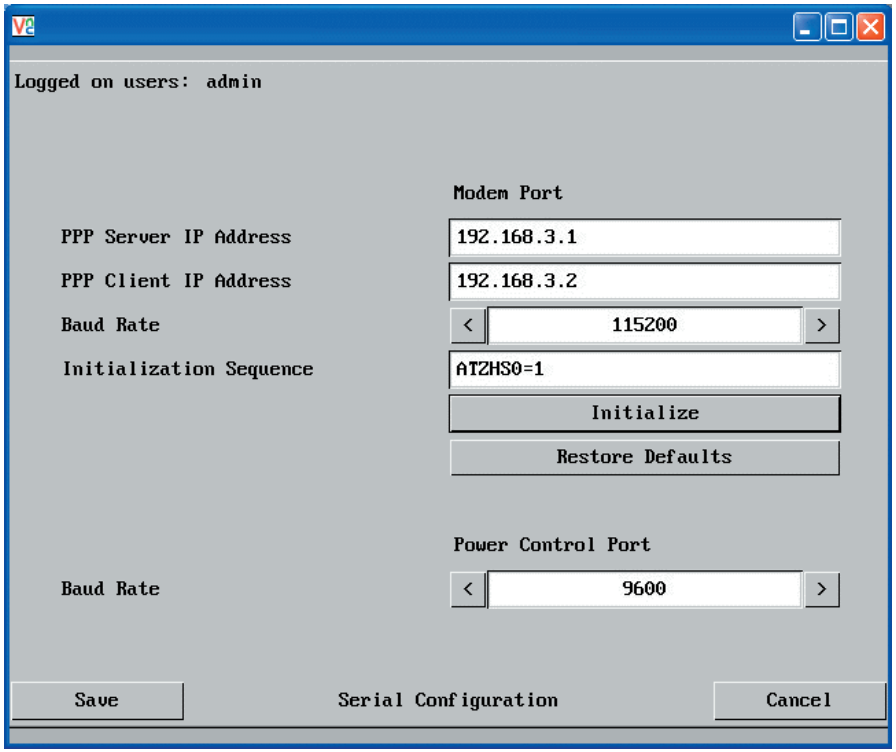
1. In the access control list, click on the entry to be moved.
2. Click the Up or Down buttons as appropriate.

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 two serial ports (modem and power control) that are situated at the rear of the CPU IP.



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.

Modem port

PPP server IP address / PPP client IP address
When a user dials into the CPU IP via a modem or ISDN adapter, the CPU IP sets up a temporary two-device network using PPP (Point to Point Protocol). For this purpose, both devices must have 'dummy' IP addresses so that they can communicate correctly. These two addresses can be almost anything expressed in the quad octet format (i.e. 192.168.3.1.). However, it is advisable not to make them the same as the real IP addresses used by either the remote system or the CPU IP.

Baud rate
This option configures the speed of the serial connection between the CPU IP and a connected modem or ISDN terminal adapter. The default setting is 115200. The other communication settings are fixed as: No parity, 8 bit word, 1 stop bit.

Initialization sequence
The codes entered here are used to prepare the connected modem or ISDN terminal adapter for use with the CPU IP. The default code is a Hayes-compatible string to configure auto answer mode and would be understood by the vast majority of modem/ISDN devices. The code is sent when the CPU IP is first switched on or whenever the Initialize button is clicked.

Initialize
When clicked, this option sends the characters entered in the Initialisation sequence field to the connected modem or ISDN terminal adapter.

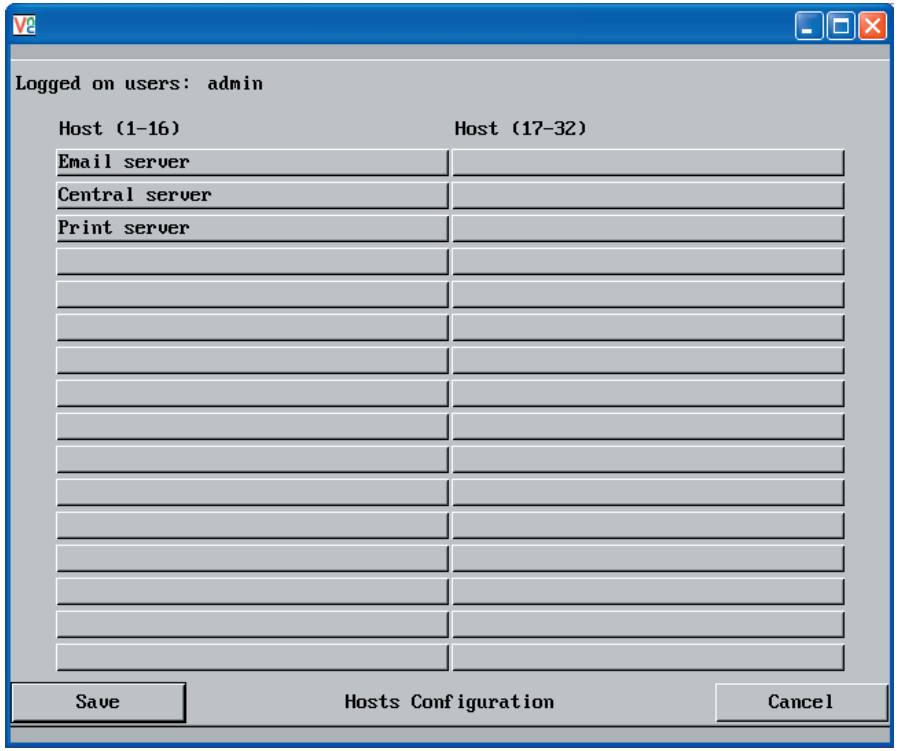
Restore Defaults
When clicked, this option resets the Baud rate and Initialisation sequence values to their original default settings.

Power control port

Baud rate
This option configures the speed of the serial connection between the CPU IP and a connected power control unit. The default setting is 9600 as used by the majority of power units. 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 CPU IP via one or more KVM switch units. There are 32 entries, each of which can be configured with a name, the permitted users, the hot key combinations required to switch to it and, if required, appropriate power control commands.

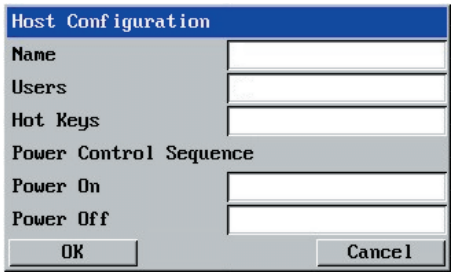


To get here

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 32 host entries to reveal a Host configuration dialog.



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,andy,steve).

Hot keys
Declare the hot key sequence that will cause the KVM switch to link with the required host system. The following notations are used: '+' means press down the following key; '-' means release the following key; * means add a 250 millisecond delay; the entries are not sensitive to case.
For instance, to send the command Ctrl + Alt 4 you should enter the following: +Ctrl+Alt+4.
To send the command Ctrl + Alt 12 you should enter the following: +Ctrl+ALT+1-1+2
(the '-1' entry causes the 1 key to be released before the 2 key is pressed).

Note: It is not necessary to specify all keys to be released at the end because they are all released automatically after the last code. A list of valid codes are given in Appendix 8.

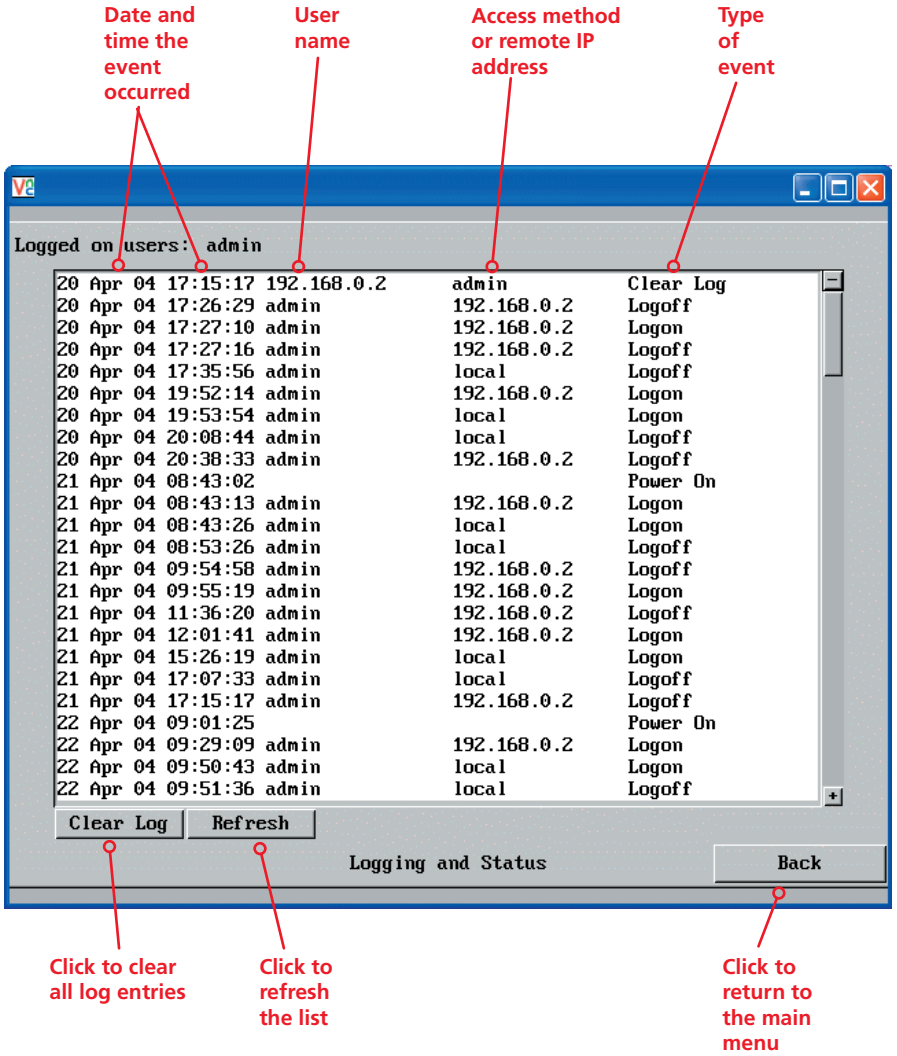
Power On
Enter the code required to make an attached power control unit apply power to the selected host. See Power switching configuration for details.

Power Off
Enter the code required to make an attached power control unit remove power from the selected host. See Power switching configuration for details.

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 CPU IP.



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'.

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.

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).

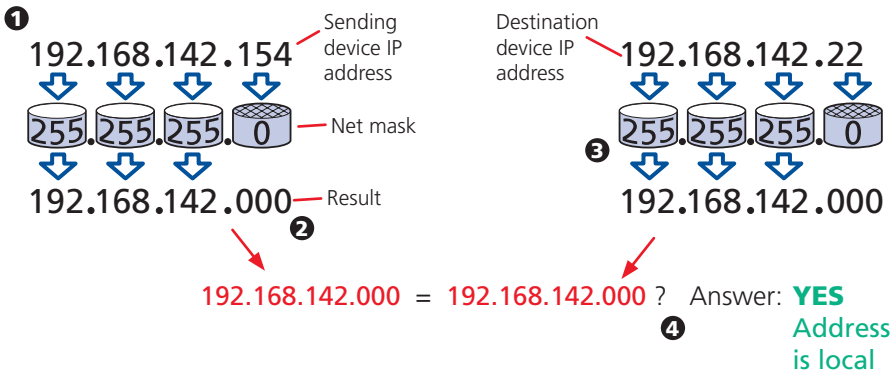
When two network devices communicate with each other, they always "dial the whole number" regardless of their respective locations in a network. However, they still need to know whether the other device is local to them or not, and this is where the net mask comes into play.

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?

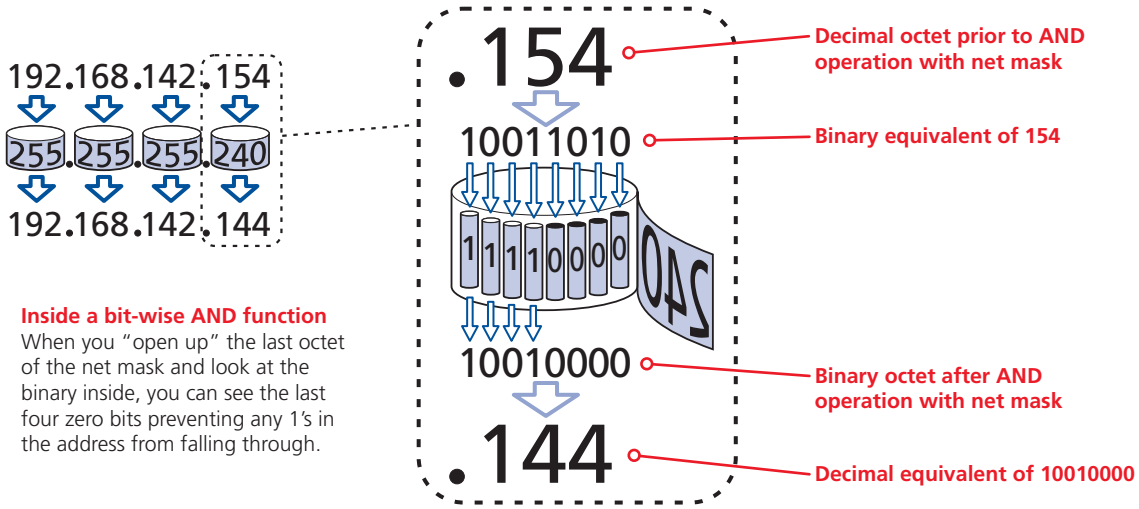
Net masks - the binary explanation

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:



Inside a bit-wise AND function
When you "open up" the last octet of the net mask and look at the binary inside, you can see the last four zero bits preventing any 1's in the address from falling through.

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:

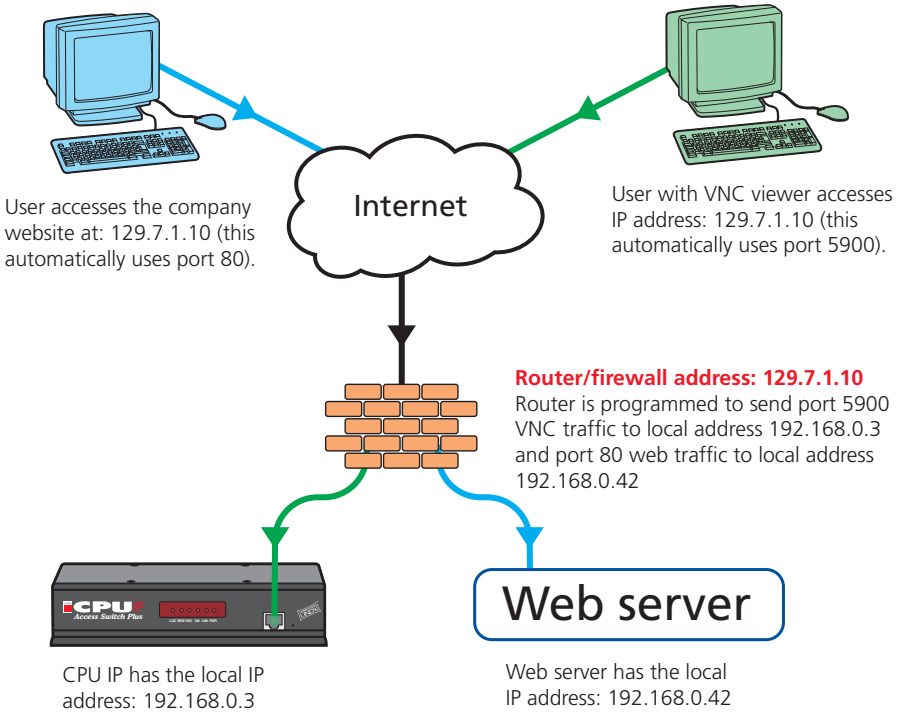
Network/address entry	Mask entry	
192.168.142.67	255.255.255.255	*defines 1 address (.67)*
192.168.142.68	255.255.255.252	*defines 4 addresses (.68 to .71)*
192.168.142.72	255.255.255.248	*defines 8 addresses (.72 to .79)*
192.168.142.80	255.255.255.248	*defines 8 addresses (.80 to .87)*
192.168.142.88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

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

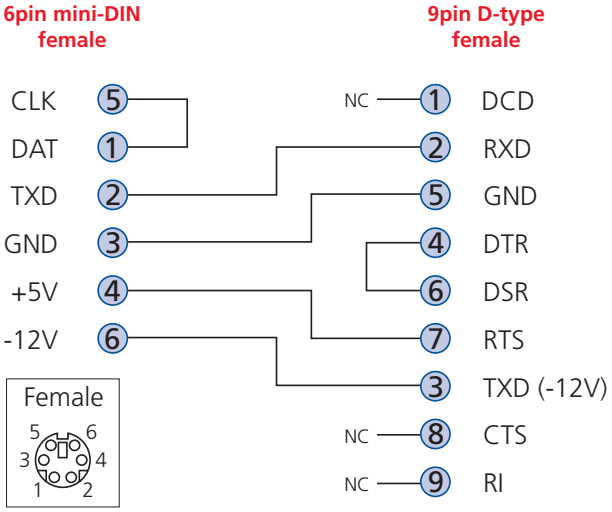
The settings of port numbers become important when the CPU IP is situated behind a network firewall. In order for a remote VNC viewer or web browser to make contact with your CPU IP, it is necessary for the firewall to allow communication through a particular numbered port to occur.

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 CPU IP ports to use the same number. The other alternative is to place the CPU IP unit outside the firewall and take full advantage of its secure operation features – see Networking issues for details.

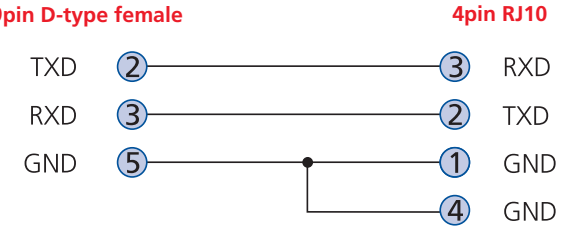
IMPORTANT: The correct configuration of routers and firewalls requires advanced networking skills and intimate knowledge of the particular network. LINDY cannot provide specific advice on how to configure your network devices and strongly recommend that such tasks are carried out by a qualified professional.

Appendix 7 – Cable and connector specifications

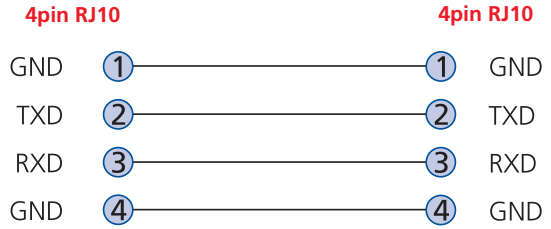
RS232 serial mouse to PS/2 converter cable



CPU IP to power switch cable



Power switch to power switch daisy chain cable



Appendix 8 – Hotkey sequence codes

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

Main control keys

Backspace | Tab | Return | Enter | Ctrl | Alt | Win | Shift | LShift | RShift
LCtrl | RCtrl | LAlt | AltGr | RAlt | LWin | RWin | Menu | Escape | Esc

Math operand keys

Add | Subtract | Multiply

Central control keys

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

Keypad keys

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

Codes with special meanings

+ means press down the following key
– means release the following key
* means wait 250ms

Other products in the CPU Switch range

The following related LINDY CPU Switch items are available:

- Matrix CPU Switch Dual Junior 2 user, 8 computer (part number: 32351)
- Matrix CPU Switch Dual Junior 2 user, 16 computer (part number: 32352)

- Matrix CPU Switch Dual Pro 2 user, 4 computer (part number: 32361)
- Matrix CPU Switch Dual Pro 2 user, 8 computer (part number: 32362)
- Matrix CPU Switch Quad Pro 4 user, 16 computer (part number: 32364)

- Extender Junior - remote unit (part number: 32391)
- Extender Plus - remote unit (part number: 32396)
- Extender Pro - remote unit (part number: 32392)
- C5 Extender Junior - remote unit (part number: 39391)

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.
- 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 CPU 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 CPU IP yourself.

Safety considerations when using power switches with CPU IP

- Follow the manufacturer's instructions when setting up and using power switching products.
- Always ensure that the total ampere rating of the devices plugged into the power switching product does not exceed the power switching product'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.

General Public License (Linux)

The CPU 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.realvnc.com/products/CPUIP/gpl.html.

Radio Frequency Energy

A Category 5 (or better) twisted pair cable must be used to connect the CPU IP 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 standard EN55022. 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.

Release 1.0c
October 2004

Documentation by: CORPORATE TEXT & DESIGN www.ctxd.com

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 control
  configuration 49
  mask calculation 55
Access mode
  shared & private 27
Account
  creation for users 45
Address
  explanation 53
Addressing
  DNS 18
  network issues 18
  power switch boxes 10
Admin password
  initial setup 12
  local setting 34
Advanced unit configuration 47
Artifacts
  on screen 25
Assistance
  from LINDY 32
Auto select 39,43

B

Baud rate
  local setting 36
  remote setting 50
Binary
  net masks 54
Brackets 5
  fitting 6
Browser
  connection 24

C

Cable specifications 53,57,58
Calibrate
  mouse 27
  screen 27
Calibrate all
  video settings 29
Clear IP access control
  local setting 35
Client IP
  local setting 36
Colour level 39
COM1
  baud rate 50
  connection 9
COM2
  baud rate 50
  connection 10
Configuration switches 4
Connections
  host computer 7
  ISDN 9
  keyboard 8
  KVM switch 7
  local 22
  modem 9
  monitor 8
  mouse 8
  network port 8
  power supply 9
  remote 23
Connector specifications 57
Controls
  viewer options 28
Control menus
  for local connection 33
  for remote connection 25,44
Control strings
  power switching 20

D

Daisy chain cable 57
Date
  local setting 34
  remote setting 46
DHCP
  discovering allocations 18
  during initial setup 12
  local setting 21,35
  remote setting 48
Dial up
  connection 30
DNS addressing 18

E

Encryption key 12

F

Firewall 17
Firmware
  current version 46
  upgrade 21
Flash upgrade 21
Force encryption 34
Full screen mode
  escape from (F8) 25

G

Gateway
  local setting 21,35
  remote setting 48

H

Hextile 39,43
Hosts
  changing between 25
Host computer
  connecting 7
  power switching setup 20
Host configuration 51
Host selection 26
Hotkeys
  to access menus 33
Hot keys
  changing 34
  remote setting 46
HTTP port
  initial setup 12
  local setting 35
  remote setting 48
  when altered 17

I

IEC power lead 9
Indicators 4
Initialise button 50
Initialize port
  local setting 36
Initial configuration 11
Init string
  local setting 36
IntelliMouse 14
IP access control 48,49
  calculating mask 55
IP address
  explanation 53
  local setting 21,35
  remote setting 48
IP gateway 48
IP network mask 48
IP network port 4
  connecting 8
ISDN
  connecting 9
  dial up link 30

K

Keyboard codes
  sending 28
Keyboard Layout
  remote setting 46
Keyboard layout
  local setting 34
KVM console 4
KVM switch
  connecting 7

L

Local connection 22
local control menus 33
Local network
  connection 17
Logging 52
Log on 24

M

MAC address 35,48
Mask
  explanation 53
  for IP access control 55
Menus
  local 33
  remote 44
Menu bar
  viewer window 25
Menu key
  changing 40
Modem
  connecting 9
  dial up link 30
Modem configuration 36
Modem port 4
Mounting 6

Mouse
restoration 13,14
Mouse calibration 27
Mouse control 28

N

Networking issues 17
Network configuration 35,48
Network port
connecting 8
Net mask 21,35
explanation 53

O

Octets
ip address 53

P

Password
admin - setting 34
initial setup 12
remote logon 24
setting for users 45
unknown 15
Port number
entering 30
Power control port 4
connecting 10
Power strings
for switching 20
Power supply
connecting 9
Power switching
configuration 20
on & off select 27
user permissions 45
PPP client IP address 50
PPP server IP address 50
Preferred encoding 39
Private
access mode 27

R

Rack mounting 6
Raw 39,43
Remote configuration 16
Remote connection 23
Reset
to factory defaults 15
Reset configuration 37
Restore Defaults
local setting 36
RJ10 connector 10
Router 17

S

Safety information 59
Screen
best resolution 25
navigation 25
Screensaver
local setting 34
remote setting 46
Serial port
modem connection 9
Serial port configuration 50
Server IP
local setting 36
Setup procedure
local setup 11
remote setup 16
Shared
access mode 27
Slow connections
optimising for 25
Supplied items 5

T

Time
local setting 34
remote setting 46
Troubleshooting 32

U

Unit configuration 34,46
Unit name
local setting 34
remote setting 46
Upgrade
firmware 21
Username
initial setup 13
remote logon 24
User accounts 45
Use DHCP
local setting 21,35

V

Video settings 29
Viewer window 25
VNC port
initial setup 12
local setting 35
remote setting 48
when altered 17
VNC viewer
configuration menus 44
connection 24
connection options 39
download 30
window options 42

W

Warranty 59
Web browser
connection 24
viewer options 43

Z

ZRLE 39,43