Thank you for choosing the AdderLink ipeps+ KVM-over-IP module. Using the tried and trusted RealVNC® software, each AdderLink ipeps+ module provides highly secure remote connectivity across the Internet or corporate network. The AdderLink ipeps+ module naturally permits secure remote access to a single host, however, with the addition of a suitable KVM switch, a choice of many hosts becomes possible.

Highly secure
Enterprise grade security (using AES 128 or 256-bit encryption and RSA 2048-bit public key authentication) is employed as standard. This is further enhanced by VNC®, which allows the creation of ciphered user communications.

User management
The AdderLink ipeps+ can create up to 15 user profiles (plus the admin user) with defined access rights. LDAP integration with Active Directory is provided for enterprise level user authentication. Up to 8 remote users may access the unit simultaneously, subject to available network bandwidth and content.

High quality remote video
Despite its small size the AdderLink ipeps+ offers video streaming at resolutions up to 1920 x 1200 at 30fps (subject to available network bandwidth), with non-blocking access for one local user and up to eight remote users.

HDMI™ is the native video port on the AdderLink ipeps+ module, however, using suitable third party converters you can also connect DVI or dual-mode DisplayPort™ (DP++) signals:

EDID management
The AdderLink ipeps+ has intelligent EDID management allowing the user to specify the video modes generated by the controlled device.

Local console
KVM connections are available for local user access. This may be useful during emergency and system maintenance activities.
ADDERLINK IPEPS+ FEATURES
The AdderLink ipeps+ module is contained within slimline metal casing measuring just 169 x 112 x 31mm.

Status indicators
These provide visual confirmation of various system functions. See Indicators for further details.  
- **LNK** - On when a network link is made.  
- **LOC** - On when a local user is logged in, flashes with keyboard and/or mouse activity.  
- **REM** - On when a remote VNC user is logged in, flashes with keyboard and/or mouse activity.  
- **PWR** - On blue when power is present, flashing red when upgrading or in recovery mode.

Optional feed to the local console (required for initial configuration)
- **USB** ports
- **HDMI** video port

Data link
Connection to LAN or wider networks
- **USB** port
- **HDMI** video port

Link to the main computer or KVM switch

Resident

Audio output port

Reserved
SUPPLIED ITEMS

AdderLink ipeps+ module

Power adapter with locking connector and country-specific mains cord

HDMI cable 1.5m

USB cable 2m (type A to B)

Information wallet containing:
- Quick setup guide
- Eight self-adhesive rubber feet
- Safety document

AdderLink ipeps+ module

Power adapter with locking connector and country-specific mains cord

HDMI cable 1.5m

USB cable 2m (type A to B)

Information wallet containing:
- Quick setup guide
- Eight self-adhesive rubber feet
- Safety document
OPTIONAL EXTRAS

USB cable 2m (type A to B) Part number: VSC24

HDMI/DVI-D passive converter cable 2m Part number: VSCD11

HDMI cable 1.5m Part number: VSCD15

Lockable HDMI cable 1.5m Part number: VSCD12

VESA™ mount kit (plus screws) Part number: RMK5V

Walldesk mounting kit (plus screws) Part number: RMK10

Replacement power adapter with locking connector Part number: PSU-IEC-12VDC-1.5A

Country-specific power cords
- CAB-IEC-EURO (Central Europe)
- CAB-IEC-UK (United Kingdom)
- CAB-IEC-USA (United States)
- CAB-IEC-JAPAN (Japan)

Dual rack mount bracket plus four retaining clamps and bolts Part number: RMK8
Installation

LOCATIONS
Please consider the following important points when planning the position of the AdderLink ipeps+ module:

- Situate the AdderLink ipeps+ module close to the system to which it will be connected and near to a source of mains power.
- Connections do not need to be carried out in the order given within this guide, however, to follow best practice, connect the power in as a final step.

MOUNTING
Before you begin making connections to the AdderLink ipeps+ module, it is advisable to first mount it in place, either:

- On a horizontal surface using the supplied self adhesive feet, or
- On a vertical surface using the optional wall/desk mounting kit, or
- Within an optional rack mount bracket.

CONNECTIONS
All connections are grouped into five main areas:

- Power connection
- Audio output port
- Reserved
- Console connections (USB port also available on the front panel)
- Computer connections
- Link connection

The pages that follow discuss the various connections.
Computer connections
The main connections to the host computer involves the HDMI™ video and USB ports. Video resolutions up to 1920 x 1200 @ 30 frames per second are supported, however, HDMI audio is not supported.

Where connection to multiple host computers is required, connect these ports to a suitable KVM switch, such as the AdderLink Infinity, DDX, XDIP and AV-4-Pro.

To make computer connections
1. Insert the supplied HDMI cable between the HDMI video socket (in the COMPUTER section) and the video output port on the computer (or KVM switch).
   - HDMI offers the great advantage that it is a straightforward task to convert its signals to and from other common video formats (DisplayPort™, DVI and VGA) - See page 8.
2. Insert the supplied USB type A to type B cable between the USB socket (in the COMPUTER section) and a vacant USB port on the computer.

Using the optional Adder HDMI cable with locking connectors
The optional VSCD12 HDMI cable features locking mechanisms on its connectors to prevent accidental disconnections. Please follow the procedures below when inserting and removing them:

**Insertion**
1. With the locking collar pulled back (to show green), insert the connector.
2. Push the locking collar forward (to show red).

**Removal**
1. Pull the locking collar back (to show green).
2. Gently pull the connector to disengage it from the socket.

**IMPORTANT:** Do not attempt to insert or remove the connector while the red band is shown.
Video format conversion

One of the many advantages offered by the HDMI (High Definition Multimedia Interface) standard is the ease with which it can be converted into- and out of- numerous other video formats, including single link DVI-D and DisplayPort (see next page).

Note: HDMI conversion cables and adapters (apart from the VSCD11 cable) are not available from Adder, but are widely sold elsewhere.

Adder HDMI/DVI-D passive converter cable (part number: VSCD11)
Video format conversion (continued)

DisplayPort/HDMI adapters - active or passive?
The choice of whether to use an active or passive adapter depends primarily upon the signal source.

If your computer outputs Dual-mode DisplayPort (also known as DP++), then you can use a (cheaper) passive adapter to derive a Single-link HDMI feed.

Conversely, when converting from HDMI to DisplayPort (to use with a DisplayPort monitor), the adapter will always be active. Note: Adapters are not bi-directional, specific models are required to go from DisplayPort to HDMI and vice versa.
Console connections

The console connections (video monitor and/or USB peripherals) allow initial configuration and local control/monitoring of the AdderLink ipeps+ module. Once the initial configuration has been completed, the retention of the console connections is optional. Video resolutions up to 1920 x 1200 @ 30 frames per second are supported, however, HDMI audio is not supported.

To make console connections

1. Insert the supplied HDMI cable between the HDMI video socket (in the CONSOLE section) and the video port on your monitor. HDMI offers the great advantage that it is a straightforward task to convert its signals to and from other common video formats (DisplayPort and DVI) - See page 8.

2. Connect the USB leads from your mouse and keyboard to the two sockets on the rear panel. The single socket on the front panel is also available (all three USB ports operate in the same manner).
**Link connection**

Use the link connection to join the AdderLink ipeps+ module to a suitable a network switch. It is also possible to connect a computer directly to the network port for configuration purposes.

**To make a link connection**

1. Insert a standard network cable into the socket on the far right of the rear panel.
2. Connect the other end of the cable either directly to a suitable network switch.

**Audio connection**

The AdderLink ipeps+ module can play out CD-quality stereo audio. Headphones are supported up to 32 Ohms impedance.

*Note:* Audio transfer from the host PC is not supported. The audio output port is used to play out a short tone to the local user that indicates when a remote connection is active.

**To make audio connection**

1. Connect your audio output (e.g. speakers or headphones, etc.) to the audio output (left hand) 3.5mm socket labeled 🎧 on the rear panel.

*Note:* The audio input port is reserved for future use.
Power connection

The module is powered using its supplied power adapter, which uses a locking-type plug to help prevent accidental disconnections; please follow the instructions shown on the right when disconnecting the power adapter.

To connect the power adapter

1. Attach the output plug of the supplied power adapter to the power input socket on the left side of the rear panel. As you insert the plug, pull back slightly on the outer body to assist the locking mechanism until the plug is fully inserted.
2. Insert the IEC connector of the supplied country-specific power cord to the socket of the power adapter.
3. Connect the power cord to a nearby mains supply socket.

To disconnect the power adapter

1. Isolate the power adapter from the mains supply.
2. Grasp the outer body of the power adapter plug where it connects with the module.
3. Gently pull the body of the outer plug away from the module. As the body of the plug slides back, it will release from the socket and you can fully withdraw the whole plug.

IMPORTANT: Do not use an unearthed power socket or extension cable.

Note: The power supply generates heat when in operation and will become warm to the touch. Do not enclose it or place it in locations where air cannot circulate to cool the equipment. Do not operate the equipment in ambient temperatures exceeding 40 degrees Centigrade. Do not place the products in contact with equipment whose surface temperature exceeds 40 degrees Centigrade.
Configuration

INITIAL CONFIGURATION

The initial configuration is carried out first using the locally connected console keyboard, mouse and video monitor, in order to set the basic network features. This is followed later using a remotely connected computer running the VNC® Viewer application to fine tune and complete the configuration process.

To perform the initial configuration

1. Connect the AdderLink ipeps+ module as discussed on pages 6 to 12. To carry out a complete configuration, the module must:
   - Have a local console connection, and
   - Be connected either to a valid network or have a computer connected directly to the network port, to allow a remote VNC connection to take place.

2. As the AdderLink ipeps+ module is powered on for the first time it will display the first of two configuration wizard pages:

   See page 27 for details.

Note: If the module has previously been configured the wizard may not be shown. Move the mouse connected to the AdderLink ipeps+ module to display the login dialog or, if already logged in, enter CTRL + ALT + C to display the main menu. You can then either use the Network and General pages to enter the configuration details or use the Reset page to perform a factory reset, which will cause the configuration wizard to be displayed. The default username is admin, while the password is initially left blank.

3. Within the initial wizard page you can achieve tasks such as:
   - Change the admin password,
   - Apply a name to the AdderLink ipeps+ module,
   - Set the time and date,
   - Determine the encryption method used.

4. Click the Next button to move on to the second page:

   See page 28 for details.

5. Use the options within the Network page to configure the basic network settings according to how the AdderLink ipeps+ is linked and then click the Next button. The login dialog will be displayed. If required, enter the username and password and press the Enter key. The default username is admin, while the password is initially left blank. Note: On the first login, the user will be forced to set a new password.
6 The next configuration steps cannot be carried out from the local console. Using a computer connected remotely to the AdderLink ipeps+ module (either through a network or connected via a direct patch link to the AdderLink ipeps+ network port), run the VNC Viewer application.

The VNC Viewer application is available as a free download from www.realvnc.com. It allows you to view and control the AdderLink ipeps+ and its host computer(s).

7 Use the network details entered earlier to guide the VNC Viewer to the AdderLink ipeps+ module. Once a connection is made, you should be presented with the login dialog:

![VNC Server](image)

Enter the admin password. If login is successful you should be presented with the VNC Viewer window with a menu bar at the top. Click the Configure button on the right side of the menu bar.

The main configuration menu should be displayed:

![Main Configuration Menu](image)

8 You can now complete the initial configuration. Common tasks include:

- Setting up **User Accounts** - see page 32.
- Completing the **Unit Configuration** (this page offers some of the options available in the console menu’s General page, plus many others) - see page 34.
- Adjusting the **Time and Date Configuration** manually or nominating an NTP server to automate the time keeping duties - see page 38.
- Completing the **Network Configuration**, including the set up of IP Access Controls - see page 39.
- Setting up the **Host Configuration** if multiple hosts are connected via a KVM switch - see page 42.

**WARNING:** The configuration wizard must be completed to ensure the default IP address is set correctly. If the wizard is interrupted (ie power cycling or reset), navigate to the **Network page** of the configuration menu and simply select Save.

The various configuration pages are covered within Appendix 2:

- **User Accounts**
  - **Menu Bar (Gui Edit Configuration)**
- **Unit Configuration**
  - **EDID Configuration**
  - **Console Configuration**
  - **Advanced Unit Configuration**
- **Time and Date Configuration**
- **Network Configuration**
  - **IP Access Control**
- **Serial Port Configuration**
- **Host Configuration**
- **Logging and Status**
- **LDAP Configuration**
**FIRMWARE UPGRADE**

The firmware within the AdderLink ipeps+ module is fully upgradeable using update files issued by Adder.

**To perform a firmware upgrade**

1. Download the required upgrade file from Adder, which will be of the form: `IPEPSPLUS_V0.00.0050.bin`.
2. Use the VNC viewer to make a remote connection (as the admin user) to the AdderLink ipeps+ unit and click the Configure button in the top right corner. See page 17.
3. Click the Advanced Unit Configuration option. See page 37.
4. Click the Upgrade Firmware button on the lower left side of the page to display the following page:

```
Logged on users: admin

Serial Number: 181161234567
Bootloader Firmware: v0.00.0016 - 16:41 06/11/19
Recovery Firmware: v0.00.0016 - 16:41 06/11/19
Current Firmware: v0.00.0050 - 16:16 06-01-19
Alternative Firmware: v0.00.0045 - 16:06 03/01/19

Upgrade Firmware  Switch Firmware
```

5. Click the Upgrade Firmware button to display the following dialog:

```
Information
Upgrading firmware is now using a web browser. If you click OK, this window will disappear. Wait for 30 seconds to allow the unit to restart. Then visit http://192.168.10.196 to perform the upgrade. (It may be necessary to press F5 to refresh the page)
```

6. Note the IP address shown in the dialogue box and click OK.

7. The unit is now ready to accept the upgrade files. Open your browser and log into the AdderLink ipeps+ using the IP address that was confirmed in the dialog. Once connected, the unit will display the following screen:

```
AdderLink ipeps+ Upgrade
Please specify the AdderLink ipeps+ firmware file to upgrade with

Choose file: No file chosen

Perform upgrade  Return to normal operation
```

8. Click the Choose file button and locate the .bin upgrade file that you downloaded earlier.

9. Click the Perform Upgrade button. The upgrade will take place and its progress will be shown on screen.
CONNECTING WITH THE HOST COMPUTER(S)

The AdderLink ipeps+ module allows up to eight concurrent users to remotely connect with a host computer. In addition, a locally connected console user can also make connections to the host. If an optional KVM switch is attached, a choice of multiple host computers becomes possible, although only one host may be selected at any one time.

Local connections

To locally connect with a host:

1. Move the mouse connected to the AdderLink ipeps+ module to display the login dialog (if already logged in, enter CTRL + ALT + C to display the dialog):

   ![AdderLink ipeps+ Login](image)

   **Note:** The default hotkeys (CTRL + ALT) can be changed within the General page if required.

2. Enter the username and password and press the Enter key. The default username is **admin**, while the **password** is initially left blank.

3. The Hosts page will be displayed:

   ![AdderLink ipeps+ Select Host](image)

4. Click on the required host computer name to connect with it.
   - Optionally change the Access method between the Shared (your connection will be viewable by other users) and Private (all other users are locked out) settings.
   - If necessary, use the Find option to locate a particular server name.

5. At any time, enter **CTRL + ALT + C** to re-display the AdderLink ipeps+ dialog.
Remote connections
The VNC Viewer application is available as a free download from www.realvnc.com. It gives you the ability to view and control the AdderLink ipeps+ and its host computer(s).

To remotely connect with a host
1 Install and run the VNC Viewer application. The connection dialog will be displayed:

![VNC Viewer connection dialog]

2 Enter the network address into the search bar and press Enter. The VNC Viewer will attempt make a connection to the AdderLink ipeps+ module.

Once a connection is made, you should be presented with the login dialog:

![VNC Viewer login dialog]

3 Enter your username and password and click OK.

4 If a successful connection is made a new window will be opened with a VNC menu bar along the top edge:

- **Viewer options**
  - Click the VNC icon to view the viewer window options.

- **Auto calibrate**
  - Determines the optimum mouse settings (when using Relative Mouse mode) 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.

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

- **Controls**
  - Displays a menu of options concerning keyboard, video, mouse and file transfer operations.

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

- **Power**
  - Click to access the power on/off options for the current host computer (if configured).

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

- **Dialogue area**
  - Indicates your username and the host system that you are currently viewing. This area also states the number of remote and local users.

- **Lock keys**
  - Click to disable the Num and/or Caps lock. Prevents keys becoming stuck, as VNC does not pass these through.

Note: The VNC Viewer Idle Timeout option is set to zero by default, ie, it will not automatically disconnect.
Auto calibrate
Auto calibrate will calibrate the mouse only if relative mouse mode is selected. This detects the mouse motion and will report back that the mouse has been calibrated correctly depending upon the operating system. See the notes on [Advanced mouse configuration](#) for more details. 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.

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

To re-synchronize 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 eight remote users can be simultaneously logged-in and all will view the same 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 prevents other users connecting at the same time.

To change the access mode
1. Click one of the arrow buttons adjacent to the Shared/Private indicator.

Power switching
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.

#### Single Mouse Mode

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

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

The single mouse mode does not require calibration.

#### Resync Mouse

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

#### Refresh Screen

This option refreshes the whole screen image to remove any artefacts 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.

---

See also

- Keyboard Control  see page 21
- Video Settings  see page 21
- File Transfer  see page 22
- Info  see page 20
**Advanced mouse configuration**

This dialog (accessible via the Mouse Control popup) allows the mouse acceleration to be configured according to the operating system in use and also permits manual fine tuning for situations where problems are encountered with the Calibrate function. For best results, choose the appropriate Change motion: entry to match the host in use.

The available Change Motion schemes are: Constant, Windows 7/8/10, Solaris, Solaris 9 and Mac OSX.

When the Absolute Mode option is ticked in the main Mouse Control menu, this dialog allows you to adjust the Absolute Offset scale:

---

**Info**

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

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

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

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
This dialog shows the current video mode and display activity.
**File Transfer**

The file transfer function requires a USB disc drive to be attached to one of the USB ports of the AdderLink ipeps+ module. The maximum size of a file that can be transferred is limited only by the size of this disc.

File transfer works in two modes:

- In the first mode, files can be transferred from the USB disc to a VNC viewer, and vice versa.
- In the second mode, the disc appears as a remote device connected to the host.

**Transferring files to the host**

1. Before starting ensure that the Enable File Transfer option is checked within the Advanced Unit Configuration dialog - see page 37.
2. To make files available to the host, they must be copied from the VNC Viewer to the USB disc and then from there to the host.
3. Bring up the file transfer menu (Controls->File Transfer) and ensure that the ‘USB Disc’ indicator (at the top of the dialog) points to ipeps+. This will enable the file transfer function in the viewer.
4. Files can now be copied to the disc by selecting ‘Transfer Files’ from the F8 menu or clicking on the equivalent icon in the VNC Viewer toolbar (accessed from the top of the screen):

   ![File Transfer](image)

   The File Transfer dialog refers to ‘VNC Server’; this means the AdderLink ipeps+ module.
5. Click on ‘Send files...’ and select the files to be sent. You can initiate multiple transfers to occur simultaneously.

   A progress dialog is displayed during the file transfer. Note that the OK button just exits the dialog, the file transfer will continue to completion.
6. Once the transfer is complete, click on the ‘USB Disc’ indicator to connect the disc to the host. This may take some time (during which the arrow will flash) as buffer data may still need to be written to the disc. The disc is now connected to the host and the files can be read in the usual way.

   **WARNING**: While transfers are in progress, avoid clicking on the ‘USB Disc’ indicator. A warning will be displayed and if you continue the transfer will be aborted; this includes any transfers initiated by other users.

**Transferring files from the host**

1. Before starting ensure that file transfer is enabled (see above).
2. To copy a file from the host, it must be copied in two stages; firstly to the attached USB disc and secondly from the disc to the VNC viewer.
3. Bring up the file transfer menu (Controls->File Transfer) and ensure that the ‘USB Disc’ indicator (at the top of the dialog) points to host. Copy the files to the USB disc in the usual way, and make sure that it can be safely removed.
4. Click on the ‘USB Disc’ indicator to connect the disc to the ‘ipeps+’. The files should appear in the window.
5. Select the files to be transferred and click ‘Send’. A ‘VNC Viewer – File Transfer’ dialog will indicate transfer progress.
6. If you select the Clear button, the log reverts to the default message, as per the dialog shown above. Please ignore the fetch files message, which relate to a software version of VNC Server, rather than one on an AdderLink ipeps+ module.
7. Files will either be stored in the pre-selected folder, or the user may choose to be prompted for the folder each time.
INDICATORS
The AdderLink ipeps+ module contains various indicators to provide you with status information.

Front panel status indicators
The status indicators on the front panel provide important feedback on current operation:

<table>
<thead>
<tr>
<th>Indicator</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LNK</td>
<td>On when a network link is made, similar to the green indicator on the link port.</td>
</tr>
<tr>
<td>LOC</td>
<td>On when a local user is logged in, flashes with keyboard and/or mouse activity.</td>
</tr>
<tr>
<td>REM</td>
<td>On when a remote VNC user is logged in, flashes with keyboard and/or mouse activity.</td>
</tr>
<tr>
<td>PWR</td>
<td>On blue when power is present, flashing red when upgrading or in recovery mode.</td>
</tr>
</tbody>
</table>

Green and amber status indicators
The indicators on the rear panel link port provide link status information:

<table>
<thead>
<tr>
<th>Indicator</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amber</td>
<td>This indicator will flash when data is being transferred.</td>
</tr>
<tr>
<td>Green</td>
<td>This indicator will be on whenever there is a valid link between this module and a network switch.</td>
</tr>
</tbody>
</table>
Further information

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

- Getting assistance - see right
- Appendix 1 - Local console menus
- Appendix 2 - Remote configuration menus (via VNC®)
- Appendix 3 - Networking issues
- Appendix 4 - Product compatibility
- Appendix 5 - Hotkey sequences
- Appendix 6 - Open source licenses

GETTING ASSISTANCE

If you are still experiencing problems after checking the information contained within this guide, then please refer to the Support section of our website:

www.adder.com
APPENDIX 1 - LOCAL CONSOLE MENUS

These menus are accessible using the locally connected console keyboard, mouse and video monitor. Using them you can begin basic configuration steps and/or switch between different host computers, when an optional KVM switch is used.

To display the local console menus

1. Move the mouse connected to the AdderLink ipeps+ module to display the login dialog (if already logged in, enter CTRL + ALT + C to display the dialog):

   ![Image](image.png)

   Note: The default hotkeys (CTRL + ALT) can be changed within the General page if required.

2. Enter the username and password and press the Enter key. The default username is admin, while the password is initially left blank.

3. The Hosts page of the configuration menu will be displayed:

   ![Image](image.png)

4. During the initial configuration, the Hosts page will be empty.

5. Click any of the page buttons to proceed. Details about each page are given on the following pages:
   - Hosts page
   - General page
   - Network page
   - Logging (Diagnostics) page
   - Reset page
Hosts page
This page allows you to quickly access the host computer(s) connected to the AdderLink ipeps+ module via an optional KVM switch:

To choose a host computer from the local console
1. Move the mouse to display the ipeps+ dialog.
2. Click on the required host computer name to connect with it.
   • Optionally change the Access method between the Shared (your connection will be viewable by other users) and Private (all other users are locked out) settings.
   • If necessary, use the Find option to locate a particular server name.

To add host computers to the list
Host computers are added to the list within the Host configuration page, which is accessed via the VNC Viewer application and a remote connection. See Host Configuration.

To get here
1. Move the mouse connected to the AdderLink ipeps+ module to display the login dialog (if already logged in, enter CTRL + ALT + C to display the dialog).
2. Enter the username* and password* and press the Enter key.
3. Click the ‘Hosts’ button located on the left hand side.

* The default username is admin, while the password is initially left blank.
General page
This page contains various important base settings:

![AdderLink ipeps+ Unit Config](image)

### Keybd Layout
Determines the language layout used for the console keyboard. Options include: UK, US,

### Admin Passwd
Allows you to set a new admin password. Passwords can be up to 16 characters in length. Passwords must be at least 8 characters, including at least 1 letter, 1 number and a special character.

### Unit Name
Allows you to set an identification name for this AdderLink ipeps module, which is declared to VNC viewers making contact.

### Hot Keys
Determines the hot keys that are used by the console keyboard to raise the configuration menu.

### Screensaver
Determines the idle period that should elapse before a screensaver is invoked on the console video monitor. *Note:* The user will need to log back in to continue.

### Time and Date
Determines the time and date used by the AdderLink ipeps+ module.

### Encryption
Four options are available:
- **Always On** – set encryption at 128 bit,
- **Prefer Off** – request encryption off at the server, but will accept on or off,
- **Prefer On** – request encryption on at the server, but will accept on or off,
- **Maximum** – set encryption at 256 bit.

The one to choose depends on the specific details of your installation. The use of encryption imposes a slight performance overhead of roughly 10% but is highly secure against third party intrusion.

---

To get here
1. Move the mouse connected to the AdderLink ipeps+ module to display the login dialog (if already logged in, enter CTRL + ALT + C to display the dialog).
2. Enter the username* and password* and press the Enter key.
3. Click the ‘General’ button located on the left hand side.

* The default username is admin, while the password is initially left blank.

---

Note: When you make any changes to items on this page, remember to click the Save button to fix them.
Network page
This page contains various key network settings. See also Appendix 3 - Networking issues for useful configuration advice.

MAC address
Media Access Control address – this is the unique and unchangeable code that was hard coded within the module 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
Determines whether a DHCP (Dynamic Host Configuration Protocol) server should be consulted on the connected network to automatically set an appropriate IP Address, Net Mask and Gateway.

IP Address
If the Use DHCP option is set to No, use this option to set an IP address for the AdderLink ipeps+ module which is appropriate for the network to which it is connected.

Net Mask
If the Use DHCP option is set to No, use this option to set a subnet-mask for the AdderLink ipeps+ module which is appropriate for the network to which it is connected.

Gateway
If the Use DHCP option is set to No, use this option to set a gateway address for a network router which gives access to another network, to be used whenever a required address lies outside the current network.

DNS Server
If the Use DHCP option is set to No, enter a valid IP address here for a Domain Name System server which is reachable through the connected network.

VNC Port
This is the logical link through which communications with a remote VNC viewer will be channelled. The default setting is 5900 which is a widely recognized port number for use by VNC® software. However, in certain circumstances it may be advantageous to alter this number.

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
Using the admin account via the remote VNC connection it is possible to specify ranges of addresses which will or won’t be granted access to the AdderLink ipeps+ module. However, it is possible to accidentally exclude all IP addresses, so this button (only on the local console connection) acts as a fail-safe to remove all access control entries.
Logging (Diagnostics) page
This page contains controls related to diagnostic activities.

Syslog Server
Enter the IP address of a valid syslog server where you wish to record log data generated by the AdderLink ipeps+ unit.

Dump log to USB
Insert a memory stick into one of the USB ports on the AdderLink ipeps+ unit and click the Trigger button to begin saving the current diagnostic log. The supported storage formats are ‘FAT’ and ‘EXT4’.

Remote Support
The AdderLink ipeps+ unit has a remote support feature that allows technical support to connect should the need arise. It works by establishing a secure SSL connection with a managed secure server hosted on the internet. Using a reverse tunnel, technical support can connect to the unit via the secure server. Each support representative has their own unique SSL keys for full traceability when making a remote connection.
Adder Technical Support will guide you through the enabling process and confirm whether the standard port number 22 needs to be changed.

Note: When you make any changes to items on this page, remember to click the Save button to fix them.

To get here
1. Move the mouse connected to the AdderLink ipeps+ module to display the login dialog (if already logged in, enter CTRL + ALT + C to display the dialog).
2. Enter the username* and password* and press the Enter key.
3. Click the ‘Logging’ button located on the left hand side.

* The default username is **admin**, while the password is initially left blank.
Reset page
This page allows you to reset all configuration options:

To get here
1. Move the mouse connected to the AdderLink ipeps+ module to display the login dialog (if already logged in, enter CTRL + ALT + C to display the dialog).
2. Enter the username* and password* and press the Enter key.
3. Click the ‘Reset’ button located on the left hand side.

* The default username is admin, while the password is initially left blank.

To reset the AdderLink ipeps+
Warning: Using this option will clear all configuration items and return the module to its default condition.

1. Near the foot of the page, click the RESET button.
   The module will be returned to all of its factory settings and will perform a cold reboot.

To reset the AdderLink ipeps+ using the front panel recover button
1. On the front panel, use a thin implement (such as a straightened out paper clip) to press the recessed button (located just below the ipeps+ logo) for around 12 seconds until the blue PWR indicator starts to flash. Once the button is released, the indicator will flash red to signify recovery mode is in progress.
   The Maintenance page will be displayed:
2. Click the Reset Configuration option.
   The module will be returned to all of its factory settings and will perform a cold reboot.

Note: When an AdderLink ipeps+ unit is put into recovery mode, if the Configure Network option is then used to change the IP address, this change will only apply whilst the unit remains in recovery mode. Once recovery mode is exited, the unit will revert to the previous IP address.
APPENDIX 2 - REMOTE CONFIGURATION MENUS (VIA VNC)

When connected remotely via VNC, with admin privileges, a Configure button is made available on the right side of the VNC menu bar. The resulting configuration menu provides access to all main settings of the AdderLink ipeps+ module:

The various configuration pages are covered within this appendix:

- User Accounts
  - Menu Bar (Gui edit configuration)
- Unit Configuration
  - EDID Configuration
  - Console Configuration
  - Advanced unit Configuration
- Time & Date Configuration
- Network Configuration
  - IP Access Control
- Serial Port Configuration
- Host Configuration
- Logging and Status
- LDAP Configuration

To view the main configuration menu

1. Using the VNC viewer application, log on as the ‘admin’ user.

2. Click the ‘Configure’ button in the top right corner. The main configuration menu will be displayed (shown above).
User Accounts
There is one admin user account, which has full access to the configuration menu. Up to 15 users can be created by the admin user, each with their own password and access privileges.

User Name
All user names must consist of lower case characters, numbers and certain non-alphanumeric characters (e.g. '_' ) only. No symbols or upper case characters are permissible. The user name can be between 1 and 32 characters in length but cannot contain foreign characters.

Password
Each password can be up to 16 characters in length. Passwords must be at least 8 characters, including at least 1 letter, 1 number and a special character.

Local
When ticked, the selected user can gain access via the local console connected directly to the AdderLink ipeps+ module.

Remote
When ticked, the selected user can gain access to the AdderLink ipeps+ module using VNC Viewer via an IP network link.

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).

Auto Logon
This feature affects the local console connection only and, when ticked, allows the specified user to access the host computer without entering their credentials. By default this option is disabled.

Menu Bar
Optionally click to customize the menu bar for each user. See next page.

To get here
1. Using VNC viewer, log on as the ‘admin’ user.
2. Click the ‘Configure’ button in the top right corner.
3. Click the ‘User Accounts’ option.
Menu Bar Edit (Gui Edit Configuration)
If required, you can customize the menu bar of the viewer window to ensure that it contains only the necessary options.
The menu bar can be edited locally by each user or edited singly by the admin or alternatively, the admin can globally alter the menu bar for all users.

To globally edit the menu bar via admin
1. Using VNC viewer, log on as the 'admin' user.
2. Click the ‘Configure’ button in the top right corner.
3. Click on User Configuration.
4. Click on the relevant Edit button.

To edit the menu bar locally
1. Login remotely via VNC viewer and display the viewer window.
2. Place the mouse pointer on the menu bar and click the right mouse button. A popup will be displayed:
3. Click on any option within the popup to add it to or remove it from the menu bar.
4. When all changes have been made, click anywhere else within the viewer window.
Changes made in this way will affect the individual user only.
Unit Configuration
This page provides access to a selection of both basic and advanced settings for the AdderLink ipeps+ module. Some of the settings displayed here are also accessible through the on-screen menu that is available to the local console.

New Connections Private
Allows you to determine whether new local or VNC connections should be set up as private (when ticked) or as shared (when unticked).

Menu Bar Toggle Hot Key
Determines the function key that can be used to display/hide the menu bar within the VNC screen.

Display Menu Bar for New Connections
If a menu bar hot key is set (see above), this tick box option becomes available and determines whether or not a menu bar is shown when each new connection occurs.

Encryption
Four options are available: Always On, Always Maximum, Prefer Off or Prefer On. The one to choose depends on the specific details of your installation. The use of encryption imposes a slight performance overhead of roughly 10% but is highly secure against third party intrusion. Maximum selects 256 bit encryption. See page 27 for explanations of the options.

Number of simultaneous VNC Users
Allows you to restrict the number of concurrent VNC sessions. The maximum number is 8 and the default is 4.

VNC Viewer Hot Key Sequence
When using the VNC Viewer, you can use key press combinations to select host computers and also to display the host selection menu. This option allows you to choose which keys should be used to form the hotkeys that will precede a switching command. The default setting is CTRL + ALT, so as an example when you press the CTRL ALT and 2 keys, the viewer will change to the host with “Hotkey Host Number” 2 - see Host configuration.

To get here
1 Using VNC viewer, log on as the ‘admin’ user.
2 Click the ‘Configure’ button in the top right corner.
3 Click the ‘Unit Configuration’ option.

Firmware Version
Indicates the version of the internal software within the AdderLink ipeps+ module flash memory.

Server Preferred Encoding
Determines the preferred graphics encoding method to be used across the VNC connection. Options are: JPEG (High performance), Use Viewer Preference, raw, RRE, hextile, TRLE, ZRLE. Note: If the Use Viewer Preference option is selected, the user may have to reset the unit (see Advanced Unit Configuration) when switching between different VNC Viewer Preferred Encoding property settings.

Host Keyboard Layout
Use the arrow buttons to match the keyboard layout expected by the host system. Note: The chosen keyboard layout may be different from the keyboard layout being used by one or more remote users.

Admin Password
Optionally edit the password that will be used to gain administrator access to the AdderLink ipeps+ module.

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

Firmware Version Configuration
Details the timings for the various video modes supported by the host computer and also allows you to edit timings where necessary. It is not normally necessary to make any changes within this section.

Console Configuration
Allows you to adjust settings which specifically affect users of the local console.

Advanced Unit Configuration
Allows access to timings and calibration options which do not usually require attention.
**EDID Configuration**

This page details the timings for the various video modes supported by the host computer. The Edit Preferred, Standard & DVT Timing page also allows you to edit timings where necessary. It is not normally necessary to make any changes within these pages.

When checked, the local monitor's EDID is passed through to the host PC; the other controls on this dialog are then ignored. The other controls are used if either the checkbox is clear or no local monitor is connected.

Note: The HDMI checkbox is normally checked, however it should be cleared if the local monitor does not have a native HDMI connector.
**Console Configuration**

This page allows you to adjust settings which specifically affect users of the local console.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Hot Key Sequence</td>
<td>Ctrl+Alt</td>
</tr>
<tr>
<td>Screensaver Timeout</td>
<td>10 mins</td>
</tr>
<tr>
<td>Notify Remote (VNC) Users of Other Logons</td>
<td></td>
</tr>
<tr>
<td>Notify Local User of Other Logons</td>
<td></td>
</tr>
<tr>
<td>Notification Text</td>
<td>ipeps+</td>
</tr>
<tr>
<td>Notification Foreground Colour</td>
<td>BlueZ</td>
</tr>
<tr>
<td>Notification Background Colour</td>
<td>Grey1</td>
</tr>
<tr>
<td>Inter User Switching Time</td>
<td>2 secs</td>
</tr>
<tr>
<td>Local Activity Monitor Time</td>
<td>off</td>
</tr>
</tbody>
</table>

**Local Hot Key Sequence**

Determines the hot keys used by the local console users to gain access to the AdderLink ipeps+ dialog.

**Screensaver Timeout**

Determines the idle time period before a screensaver is displayed on an active console connection.

**Notify Remote (VNC) Users of Other Logons**

When checked, remote (VNC) users will be shown a list of all logged-in users whenever there’s a change.

**Notify Local User of Other Logons**

When checked, the local user will be shown a list of all logged-in users whenever there’s a change.

**Notification Text**

Allows you to edit the text string (up to 30 characters) that will be shown in all notification popups.

**Notification Foreground Colour**

Determines the foreground colour used for notification popups.

**Notification Background Colour**

Determines the background colour used for notification popups.

**Inter User Switching Time**

This setting helps to solve contention issues between allowing the local and remote users to take control of the mouse and keyboard connections. This determines the idle time (period of inactivity in seconds) after which control can be established by the other party. Options are: 2 secs (default), 5, 10, 30, 40, 50 or 60 secs.

**Local Activity Monitor Time**

When enabled, the inactivity timeout information will be logged at the web location, http://<addr>/ActivityMonitor. Timeout thresholds are Off (default), 1, 2, 5, 10, 20 and 30 secs.
Advanced Unit Configuration
Click this button to display advanced options that do not normally require alteration.

<table>
<thead>
<tr>
<th>Advanced Unit Configuration</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Force VNC Protocol 3.3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Idle Timeout (minutes)</td>
<td>60</td>
<td></td>
</tr>
<tr>
<td>Session Sleep Timeout (minutes)</td>
<td>20</td>
<td></td>
</tr>
<tr>
<td>Protocol Timeout (seconds)</td>
<td>20</td>
<td></td>
</tr>
<tr>
<td>Background Refresh Rate</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mouse Latency Allowance (milliseconds)</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Mouse Rate (milliseconds)</td>
<td>20</td>
<td></td>
</tr>
<tr>
<td>Single Mouse Mode Mouse Switch</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Use Quick Mouse Calibration</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Use Absolute Mouse by default</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Behaviour for admin connections when limit reached</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enable File Transfer</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Force USB Fullspeed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Audio Volume</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Mouse Latency Allowance
This option (used only for Relative Mouse mode) is used during calibration to account for latency delays that may be caused as signals pass through a device.

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

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

Mouse Rate
Defines the rate at which mouse movement data are transmitted to the system. The default option is 20ms, which equates to 50 mouse events per second. This is used to slow down the rate in exceptional circumstances but normally requires no adjustment.

Single Mouse Mode Mouse Switch
Select the mouse button combination to exit from single mouse mode (when active).

Use Quick Mouse Calibration
Invokes optimized calibration techniques that handle the majority of mouse types (used only for Relative Mouse mode).

Use Absolute Mouse by default
When selected, absolute mouse positioning data will be used rather than relative values.

Behaviour for admin connections when limit reached
Determines what should occur when the limit on VNC users is reached. Options are: Replace oldest connection, Replace newest connection, and Don't replace.

Enable File Transfer
When checked, allows file transfers to occur. See page 22.

Force USB Fullspeed
When checked, forces the ipeps+ USB device to work in full-speed mode. The default is high speed.

Audio Volume
Controls the volume of the short tone that is played to the local user to indicate when a remote connection is active.

Upgrade Firmware
Allows you to upgrade the firmware of the AdderLink ipeps+ module. See page 15.

Reboot Unit
Performs a complete cold boot of the AdderLink ipeps+ module.
Time & Date Configuration
This page allows you to configure all aspects relating to time and date within the unit.

Use NTP
When this option is selected, the AdderLink ipeps+ module will synchronize its internal clocks using information from the (Network Time Protocol) server listed in the NTP Server IP address field.

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

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

Timezone specifier
Optionally enter a recognized timezone specifier related to the current position of the AdderLink ipeps+ module. When an NTP server is used, the specifier will be used to provide the correct real time.

The timezone specifier takes the following form:

\[ \text{std} \ \text{offset} \ \text{dst} \ \text{[offset]} \ \text{start} / \text{time} \ \text{end} / \text{time} \]

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

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

The remainder of the specification describes when Daylight Saving Time is in effect. The \text{start} field is when Daylight Saving Time goes into effect and the \text{end} field is when the change is made back to standard time. The most common format used for the daylight saving time is: \text{Mm.wd}

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

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

Typical examples are:

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

For further details
- For details of the Network Time Protocol (main RFC number: 1305; the SNTP subset used as the basis for the AdderLink ipeps+ module: 4330) [http://www.ietf.org/rfc.html](http://www.ietf.org/rfc.html)

To get here
1. Using VNC viewer, log on as the `admin` user.
2. Click the ‘Configure’ button in the top right corner.
3. Click the ‘Time & Date Configuration’ option.
Network Configuration
This page allows you to configure the various aspects of the IP port. See also Appendix 3 - Networking issues for useful configuration advice.

MAC address
Media Access Control address – this is the unique and unchangeable code that was hard coded within the module 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
Determines whether a DHCP (Dynamic Host Configuration Protocol) server should be consulted on the connected network to automatically set an appropriate IP Address, IP Network Mask and IP Gateway.

IP Address
If the Use DHCP option is set to No, use this option to set an IP address for the AdderLink ipeps+ module which is appropriate for the network to which it is connected.

IP Network Mask
If the Use DHCP option is set to No, use this option to set a subnet-mask for the AdderLink ipeps+ module which is appropriate for the network to which it is connected.

IP Gateway
If the Use DHCP option is set to No, use this option to set a gateway address for a network router which gives access to another network, to be used whenever a required address lies outside the current network.

DNS Server
If the Use DHCP option is set to No, enter a valid IP address here for a Domain Name System server which is reachable through the connected network.

VNC Port
This is the logical link through which communications with a remote VNC viewer will be channeled. The default setting is 5900 which is a widely recognized 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 channeled. 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 AdderLink ipeps+ module. 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.

To get here
1. Using VNC viewer, log on as the ‘admin’ user.
2. Click the ‘Configure’ button in the top right corner.
3. Click the ‘Network Configuration’ option.

IP Network Mask
If the Use DHCP option is set to No, use this option to set a subnet-mask for the AdderLink ipeps+ module which is appropriate for the network to which it is connected.

IP Gateway
If the Use DHCP option is set to No, use this option to set a gateway address for a network router which gives access to another network, to be used whenever a required address lies outside the current network.

DNS Server
If the Use DHCP option is set to No, enter a valid IP address here for a Domain Name System server which is reachable through the connected network.

VNC Port
This is the logical link through which communications with a remote VNC viewer will be channeled. The default setting is 5900 which is a widely recognized 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 channeled. 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 AdderLink ipeps+ module. 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, you will need to either perform a reset to factory default settings or use the local console (and Clear IP Access Control) in order to regain access.

To define a new IP access control entry
1. Click the Add button to display a popup dialog:

   **Host IP Address Filter**
   - **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.
   - **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.

To get here
1. Using VNC viewer, log on as the ‘admin’ user.
2. Click the ‘Configure’ button in the top right corner.
3. Click the ‘Network Configuration’ option.
4. In the Set IP Access section, click Add or Edit, as necessary.
Serial Port Configuration

In order to support serial connections for power control purposes, a USB to Serial port adapter is required (third party adapters with Prolific PL2302 or FTDI chipsets are supported). Once installed, this page allows you to configure the baud rate of the serial port (via the USB connection) that can be used to control power switch devices. A full range of standard baud rates are available.

Baud Rate
Determines the communication speed of the serial port (via a third party converter attached to one of the AdderLink ipeps+ USB ports). The other communication settings are fixed as: No parity, 8 bit word, 1 stop bit.

To get here
1 Using VNC viewer, log on as the ‘admin’ user.
2 Click the ‘Configure’ button in the top right corner.
3 Click the ‘Serial port Configuration’ option.
**Host Configuration**

This page provides the opportunity to configure various details for each of the host systems that may be connected to the AdderLink ipeps+ module. Each entry 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 create a new host entry**

1. Click one of the host entries to reveal a Host configuration dialog.
2. Enter the required information in each field.
3. Click the OK button.

**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.

**KVM Switch Macro**

Declare the hot key sequence that will cause the KVM switch to link with the required host system. *Note: If this is left blank, the host will not be included in the Hosts menu.*

**Hotkey Host Number**

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

**Power On**

Enter the code required to make an attached power control unit (via a third party converter attached to one of the AdderLink ipeps+ USB ports) apply power to the host.

**Power Off**

Enter the code required to make an attached power control unit (via a third party converter attached to one of the AdderLink ipeps+ USB ports) remove power from the selected host.

**Reboot**

Enter the code required to make an attached power control unit remove power and then re-apply it a few seconds later.

---

**Sort**

Allows you to reorder the list of hosts either alphabetically or by entry number.

**Erase Host Configuration**

Removes all hosts from the list.

---

**To get here**

1. Using VNC viewer, log on as the ‘admin’ user.
2. Click the ‘Configure’ button in the top right corner.
3. Click the ‘Host Configuration’ option.
Logging and Status

This screen provides various details about the user activity on the AdderLink ipeps+ module.

To get here

1. Using VNC viewer log on as the ‘admin’ user.
2. Click the ‘Configure’ button in the top right corner.
3. Click the ‘Logging and Status’ option.

To copy and paste the log

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

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

Syslog Server IP Address

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

For further details

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

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

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

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

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

Base DN
This field allows you to enter the top level of the LDAP directory tree at which to start an LDAP search. An example Base DN value might be: “dc=catxip1000,dc=com”

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

Anonymous Bind
If left unchecked then bind requests are sent with username (Base DN) and password (more suitable for Active Directory applications).
If checked, bind requests are anonymous (more suitable for Linux LDAP implementations).

Note: Anonymous bindings are not recommended.

Filter
Search filters enable you to define search criteria and provide more efficient and effective searches. AdderLink ipeps+ supports the LDAP search filters defined in RFC2254. These search filters are represented by Unicode strings.

For example:

“(&(objectCategory=person)(objectClass=user)(!(cn=pete)))”

All user objects except “pete”

“(&(objectCategory=person)(objectClass=contact)(|(sn=Jones)(sn=Brown)))”

All contacts with a surname equal to “Jones” or “Brown”

To get here
1 Using VNC viewer log on as the ‘admin’ user.
2 Click the ‘Configure’ button in the top right corner.
3 Click the ‘LDAP Configuration’ option.
APPENDIX 3 - NETWORKING ISSUES

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

Positioning AdderLink ipeps+ in the network

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

Placing AdderLink ipeps+ behind a router or firewall

A possible point of contention between the AdderLink ipeps+ 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 minimize the number of open ports. The AdderLink ipeps+ 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. Adder Technology 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 AdderLink ipeps+ 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 AdderLink ipeps+ correctly using only its network address. The firewall/router must be informed to transfer traffic, requesting these port numbers, through to the AdderLink ipeps+.

When a web server is also on the local network

Port 80 is the standard port used by web (HTTP) servers. If the AdderLink ipeps+ 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 AdderLink ipeps+ 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 AdderLink ipeps+.

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 AdderLink ipeps+.  

IMPORTANT: When the AdderLink ipeps+ is accessible from the Internet, you must ensure that sufficient security measures are employed.
Addressing
When the AdderLink ipeps+ 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 AdderLink ipeps+.

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 AdderLink ipeps+ via a network connection. To discover the allocated IP address:

1. Within Network configuration, set the ‘Use DHCP’ option to ‘Yes’ and select ‘Save’. Once the page is saved, the AdderLink ipeps+ 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 AdderLink ipeps+ 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 AdderLink ipeps+ 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 AdderLink ipeps+ alongside the firewall

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

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

Ensuring sufficient security

The security capabilities offered by the AdderLink ipeps+ 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.
• Ensure that you have selected secure passwords with at least 8 characters and a mixture of upper and lower case and numeric characters.
• 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).
• Use non-standard port numbers.
• Restrict the range of IP addresses that are allowed to access the AdderLink ipeps+ to only those that you will need to use. To restrict IP access.
• Do NOT Force VNC protocol 3.3.
• Ensure that the computer accessing the AdderLink ipeps+ is clean of viruses and spyware and has up-to-date firewall and anti-virus software loaded that is appropriately configured.
• Avoid accessing the AdderLink ipeps+ from public computers.

Security can be further improved by using the following suggestions:

• Place the AdderLink ipeps+ 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 Adder Technology Limited.

Ports

In this configuration there should be no constraints on the port numbers because the AdderLink ipeps+ 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 AdderLink ipeps+ 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
APPENDIX 4 - PRODUCT COMPATIBILITY

AdderLink ipeps+ is compatible with the following Adder products:

- AdderView DDX and AdderLink XDIP small Matrix systems.
- AdderLink Infinity 1000 and AdderLink Infinity 2000 receivers to allow a VNC connection into an Infinity Matrix.
- AdderView AV4PRO KVM switch to allow remote access to four USB/DVI computers.

Note: AdderLink ipeps+ is NOT compatible with the AdderView AV8PRO KVM switch.
AdderLink ipeps+ allows you to enter commands suitable for any KVM switch in order to choose from up to 128 host systems. These switching commands can take the form of hotkey sequences that emulate standard keypress combinations or, for KVM switches that support the Adder Port Direct format, merely basic port numbers.

**Hotkey sequences**

Almost any combination of keypresses can be emulated using the following notations:

- `+` means press down the key that follows;
- `–` means release the key that follows;
- `+–` means press and then release the key that follows;
- `*` means add a delay. The standard delay period is 250ms, however, if a number immediately follows the asterisk, this will define an alternate delay period (in milliseconds).

**Notes**

- The entries are not case sensitive.
- All characters can be entered using their ASCII codes, from 32 to 126 (i.e. A,B,C,… 1,2,3 etc.) with the exception of the special characters above.
- 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 number of KVM switches from alternative manufacturers use hot key sequences that begin with a press/release of either the Scroll Lock or Ctrl keys. These often require a delay between the initial key press and the channel number to allow the switch to respond. A 500ms delay is usually sufficient.

**Examples**

To send the command `Ctrl + Alt 4` you should use the following: `+Ctrl+Alt+4`.

To send the command `Ctrl + Alt 12` you should use the following: `+Ctrl+ALT+-1+2` (the `+-1` entry causes the 1 key to be pressed and released before the 2 key is pressed).

To send the command `Scroll Lock 1 + Enter` (with a 500ms delay) you should use the following: `+–Scr*500+1+Ent`.

**Main control keys** (see ‘Using abbreviations’)

| Backspace | Tab | Return | Enter | Ctrl | Alt | Win | Shift | LShift | RShift | LCtrl | RCtrl | LAlt | RAlt | LWIn | RWIn | Menu | Escape | Space | CapsLock | NumLock | PrintScreen | Scrolllock |
|-----------|-----|--------|-------|------|-----|-----|-------|--------|--------|-------|------|------|------|-------|-------|-------|---------|--------|-----------|----------|-------------|

**Math operand keys** (see ‘Using abbreviations’)  
Add (Plus) | Subtract (Minus) | Multiply

**Central control keys** (see ‘Using abbreviations’)  
Insert | Delete | Home | End | PageUp | PageDown | Up | Down | Left | Right | Print | Pause

**Keypad keys** (see ‘Using abbreviations’)  
KP_Insert | KP_Delete | KP_Home | KP_End | KP_PageUp | KP_PageDown | KP_Up | KP_Down | KP_Left | KP_Right | KP_Enter | KP_Add | KP_Subtract | KP_Divide | KP_Multiply | KP_0 to KP_9

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

**Creating macro sequences**

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

- `+SCRROLL-SCRROLL`
- `+SCRROLL`
- `+SCRROLL-`

Example:

`+SCRROLL+-SCRROLL+-SCRROLL+1+ENTER`

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

**Using abbreviations**

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

**Note:** Hotkey sequences and abbreviations are not case sensitive.

For information about where to enter these codes, please see the section Host configuration.
APPENDIX 6 - OPEN SOURCE LICENSES

This product includes binaries that are derived from the open source community. The modules listed below are licenced under the GNU General Public License v2 and must be provided, in source form, on request:

- u-boot
- linux-arm-freescale
- busybox
- util-linux
- udev
- e2fsprogs
- freetype
- libfftw
- linux-pam
- pam-ldap
- libalsa
- kmod

The software included in this product contains copyrighted software that is licensed under the GPL. You may obtain the complete Corresponding Source code from Adder for a period of three years after the last shipment of this product, which will be no earlier than 2028, by contacting support@adder.com or writing to:

Adder Technology Ltd, Saxon Way, Bar Hill, Cambridge, CB23 8SL, United Kingdom

Please write “Source for product XXXXXXXX ” in the subject line (where XXXXXXX is the model and version number). This offer is valid to anyone in receipt of this information.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License; Copyright (c) 1998-2011 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”
4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment: “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”

THIS SOFTWARE IS PROVIDED BY THE OpenSSL Project “AS IS” AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL Project OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com) All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscapes SSL. This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, MD5, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by
the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young’s, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement: “This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).” The word ‘cryptographic’ can be left out if the routines from the library being used are not cryptographic related :-).
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: “This product includes software written by Tim Hudson (tjh@cryptsoft.com)”

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ‘AS IS’ AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence].

-----------

Module: dropbear

Dropbear contains a number of components from different sources, hence there are a few licenses and authors involved. All licenses are fairly non-restrictive. The majority of code is written by Matt Johnston, under the license below. Portions of the client-mode work are (c) 2004 Miheea Stoennescu, under the same license:

Copyright (c) 2002-2015 Matt Johnston Portions copyright (c) 2004 Miheea Stoennescu All rights reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the “Software”), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions: The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

----------------------

LibTomCrypt and LibTomMath are written by Tom St Denis, and are Public Domain.

----------------------

sshtpy.c is taken from OpenSSH 3.5p1, Copyright (c) 1995 Tatu Ylonen <ylo@cs.hut.fi>, Espoo, Finland All rights reserved “As far as I am concerned, the code I have written for this software can be used freely for any purpose. Any derived versions of this software must be clearly marked as such, and if the derived work is incompatible with the protocol description in the RFC file, it must be called by a name other than “ssh” or “Secure Shell”

----------------------

loginrec.c
loginrec.h
atomicio.h
atomicio.c
and strlcat() (included in util.c) are from OpenSSH 3.6.1p2, and are licensed under the 2 point BSD license.

loginrec is written primarily by Andre Lucas, atomicio.c by Theo de Raadt.

strlcat() is (c) Todd C. Miller

----------------------

Import code in keyimport.c is modified from PuTTY’s import.c, licensed as follows:

PuTTY is copyright 1997-2003 Simon Tatham.
Portions copyright Robert de Bath, Joris van Rantwijk, Delian Delchev, Andreas Schultz, Jeroen Massar, Wez Furlong, Nicolas Barry, Justin Bradford, and CORE SDI S.A.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the “Software”), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions: The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY,
Whether in an action of contract, tort or otherwise, arising from, out of or in connection with the software or the use or other dealings in the software.

 Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

 Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

 1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

 3. All advertising materials featuring or use of this software must display the following acknowledgement: This product includes software developed by the University of California, Berkeley and its contributors.

 4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

 THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

curve25519-donna: Curve25519 elliptic curve, public key function http://code.google.com/p/curve25519-donna/ Adam Langley <agl@imperialviolet.org> Derived from public domain C code by Daniel J. Bernstein <djb@cr.yp.to> More information about curve25519 can be found here http://cr.yp.to/ecdh.html

djb's sample implementation of curve25519 is written in a special assembly language called qhasm and uses the floating point registers.

This is, almost, a clean room reimplementation of the curve25519 paper. It uses many of the tricks described therein. Only the crecip function is taken from the sample implementation.

- Module: libjpeg-turbo

This software is based in part on the work of the Independent JPEG Group.

- Module: freebsd-libc

COPYRIGHT 8.2 (Berkeley) 3/21/94

All of the documentation and software included in the 4.4BSD and 4.4BSD-Lite Releases is copyrighted by The Regents of the University of California. Copyright 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994T he Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials featuring or use of this software must display the following acknowledgement: This product includes software developed by the University of California, Berkeley and its contributors.

4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

This software is provided by The Regents and Contributors "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The Institute of Electrical and Electronics Engineers and the American National Standards Committee X3, on Information Processing Systems have given us permission to reprint portions of their documentation.

In the following statement, the phrase "this text" refers to portions of the system documentation. Portions of this text are reprinted and reproduced in electronic form in the second BSD Networking Software Release, from IEEE Std 1003.1-1988, IEEE Standard Portable Operating System Interface for Computer Environments (POSIX), copyright 1988 by the Institute of Electrical and Electronics Engineers, Inc. In the event of any discrepancy between these versions and the original IEEE Standard, the original IEEE Standard is the referee document.

In the following statement, the phrase "This material" refers to portions of the system documentation.

This material is reproduced with permission from American National Standards Committee X3, on Information Processing Systems. Computer and Business Equipment Manufacturers Association (CBEMA), 311 First St., NW, Suite 500, Washington, DC 20001-2178. The developmental work of Programming Language C was completed by the X3J11 Technical Committee.

The views and conclusions contained in the software and documentation are those of the authors and should not be interpreted as representing official policies, either expressed or implied, of the Regents of the University of California.

- Module: openssl

The OpenLDAP Public License Version 2.8, 17 August 2003

Redistribution and use of this software and associated documentation ("Software"), with or without modification, are permitted provided that the following conditions are met:

1. Redistributions in source form must retain copyright statements and notices,
2. Redistributions in binary form must reproduce applicable copyright statements and notices, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution, and

3. Redistributions must contain a verbatim copy of this document.

The OpenLDAP Foundation may revise this license from time to time. Each revision is distinguished by a version number. You may use this Software under terms of this license revision or under the terms of any subsequent revision of the license.

THIS SOFTWARE IS PROVIDED BY THE OPENLDAP FOUNDATION AND ITS CONTRIBUTORS “AS IS” AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OPENLDAP FOUNDATION, ITS CONTRIBUTORS, OR THE AUTHOR(S) OR OWNER(S) OF THE SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The names of the authors and copyright holders must not be used in advertising or otherwise to promote the sale, use or other dealing in this Software without specific, written prior permission. Title to copyright in this Software shall at all times remain with copyright holders. OpenLDAP is a registered trademark of the OpenLDAP Foundation. Copyright 1999-2003 The OpenLDAP Foundation, Redwood City, California, USA. All Rights Reserved. Permission to copy and distribute verbatim copies of this document is granted.
Index

A
Access control
configuration 40
Access mode
shared & private 18
Adapters
video 8
Addressing 46
DNS 46
network issues 46
Audio connections 11
Auto calibrate 18

C
Cable specifications 49
Calibrate
mouse 18
screen 18
Configuration
advanced mouse 20
Connections
audio 11
computer 7
console 10
link 11
overview 6
power 12
Controls
viewer options 19

D
DHCP
discovering allocations 46
Diagnostics 29
DisplayPort 9
DNS addressing 46
Dump log 29
DVI conversion 8

F
File Transfer 22
Firewall 45
Firmware upgrade 15

H
HDMI 35
Host computer
configuration 42
Hotkey sequences 49
codes and macros 49
HTTP port
remote setting 28,39
when altered 45

I
Indicators 23
IP access control 40
IP address
remote setting 28,29,39
IP network mask 28,39

K
Keyboard codes
sending 21
Keyboard Control 21
Keyboard layout
remote setting 34

L
LDAP 44
Link connection 11
LNK
indicator 23
Local network
connection 45
Logging 29,43

M
MAC address 38,39
Mounting 6
Mouse
advanced configuration 20
calibration 18
control 19
resync 18,19

N
Network configuration 39
Networking issues 45

O
Optional extras 5

P
Power connection 12
Power switching
on & off select 18
user permissions 32
via viewer 18
Private
access mode 18
PWR
indicator 23

R
Rack mount bracket 6
Recover button 3,30
Recovery mode 30
Refresh screen 19
Remote configuration
host configuration 42
logging and status 43
network configuration 39
unit configuration 34
user accounts 32
Remote Support 29
Reset page 30
Resync mouse 19
Router 45

S
Screen
refresh 19
Security 47
ensuring 47
Server
configuration 42
Shared
access mode 18
Single mouse mode 19
Supplied items 4
Syslog 43
Syslog Server 29

T
Time & date configuration 38

U
Unit Configuration 34
Unit name
remote setting 34
User accounts 32
User configuration 32,33

V
Video format
conversion 8,9
Video resolutions
maximum 7
Video settings 20,21
Virtual media. See File Transfer
VNC port
remote setting 28,39
when altered 45