CAB1641HDIEU

Instruction Manual

1U IP KVM Module for 1UCABCONS

1U 16-Port Digital IP KVM Module for 1UCABCONS

SERVER REMOTE CONTROL

StarTech.com

Making hard-to-find easy!®

FCC Compliance Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Use of Trademarks, Registered Trademarks, and other Protected Names and Symbols

This manual may make reference to trademarks, registered trademarks, and other protected names and/or symbols of third-party companies not related in any way to StarTech.com. Where they occur these references are for illustrative purposes only and do not represent an endorsement of a product or service by StarTech.com, or an endorsement of the product(s) to which this manual applies by the third-party company in question. Regardless of any direct acknowledgement elsewhere in the body of this document, StarTech.com hereby acknowledges that all trademarks, registered trademarks, service marks, and other protected names and/or symbols contained in this manual and related documents are the property of their respective holders.

Table of Contents

Introduction

Packaging Contents

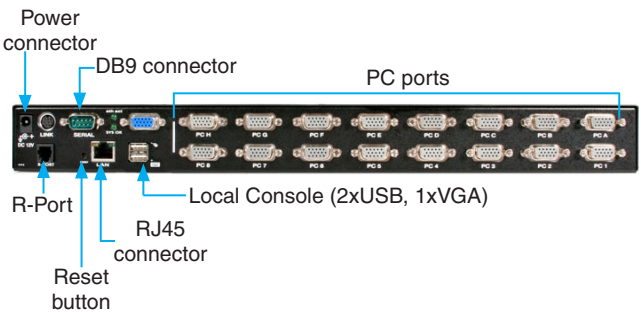
- 1 x 1U IP KVM Module for 1UCABCONS

System Requirements

- 1UCABCONS series Rackmount LCD Console

Front View

Rear View



Installation

Hardware Installation

This section will guide you through the hardware installation of your KVM Module. Please read through this section carefully and complete each step in the order listed.

1. Make sure all computers and devices are powered off.
2. Remove/disconnect any existing KVM Module from the rear of the 1UCABCONS series Rackmount Console.
3. Connect the KVM Module to your 1UCABCONS series Rackmount Console as directed in it's user guide.
4. Attach each of your managed computers to your StarView KVM console's PC ports using StarTech.com KVM cables. Use the cables to connect one of the PC ports on the back of the KVM module to the computer's keyboard/mouse, and video ports.

NOTE: These instructions are for a single KVM switch only. For information on cascading multiple KVMs, see Cascade Configuration below.

5. Connect the RJ45 Ethernet cable from the network switch/router to the LAN port on the KVM Module.
6. Turn on the 1UCABCONS and proceed with configuring the KVM Module.

NOTE: After the initial power up, you can hot-plug additional computers or slave KVM switches without having to power down your KVM.

NOTE: For any "CAB" series KVM Module, the connectors (keyboard and mouse) for the Local Console port on the rear of the KVM module are not active while the module is connected to the LCD Console by the C-36 Centronics connector. When the C-36 connector is no longer connected to the LCD Console, the keyboard/mouse ports become active and the KVM module can act as a rear-mount stand-alone KVM switch. The Local VGA port can be connected to an external VGA monitor at any time.

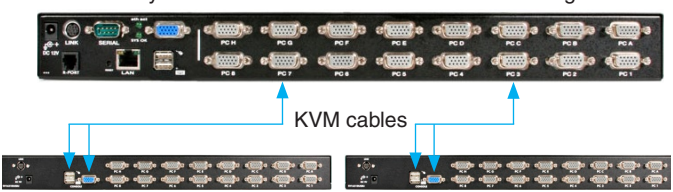
Cascade Configuration

You can connect a second level of KVM switches to one or more of your Master KVM switch's PC ports. The KVM switches connected to the Master switch are know as Slaves. Once connected, the KVM switches will automatically configure themselves as either Master or Slaves. You can only connect an equal or "smaller" KVM to the Master KVM. For example, a 16-port Master KVM switch can have both 16-port and 8-port slaves. An 8-port Master KVM switch can only have 8-port KVM slaves or lower.

The 8-port KVM can support 64 PCs, with 8 8-port Slave KVMs, each connected to 8 PCs. The 16-port KVMs can support 136 computers, with 8 16-port Slave KVMs, each connected to 16 computers. The Slave KVMs must be connected to the 1~8 ports, not the A~H ports.

To cascade your KVMs, use a StarTech.com KVM cable to connect one of your Master switch's PC ports to the Slave switch's Console ports.

A slave KVM module may be mounted to the rear vertical poles inside a rack cabinet by the rear brackets with the connectors facing out.



Driver Installation

The KVM Module uses generic keyboard/mouse/monitor drivers that are built into the operating system, so no additional drivers are required.

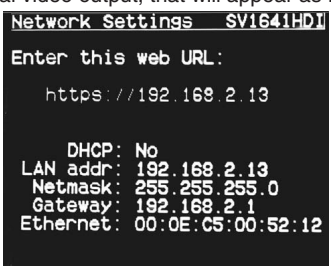
Configuring the Server Remote Control

The Server Remote Control module offers four distinct methods for configuring the unit for your network. Which method will work best will depend on your level of experience and your specific network configuration.

NOTE: Connecting and powering on the remote computers prior to following the steps outlined below can result in system instability. Please refrain from powering on the remote computers, until the local peripherals have been connected.

Network Configuration Using the On-Screen Display

Upon boot-up, including following a reset, the IP KVM will display a window on the local video output, that will appear as follows:



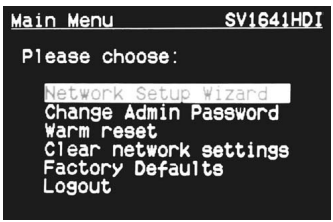
The initial screen will display the IP address assigned by your existing DHCP server (if present on your network). If no DHCP server is detected, a factory assigned IP address will be displayed in its place (10.0.0.15 by default). Please make note of the assigned IP address, as you will need to enter it into your web browser to access the Web Interface.

If static IP addresses are assigned, you will likely need to change the Net Mask, IP Address and other details, prior to connecting via your Web browser. In order to proceed, you will require an administrative username and password. By default, the username and password are *admin*. You will be given the opportunity to change the password

(recommended) to be performed once the configuration is complete.

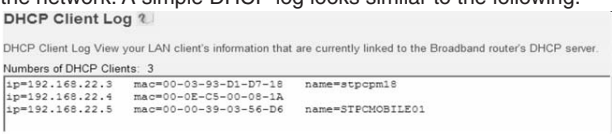
At the main OSD menu, you will be given several basic setup options. To configure the IP KVM to your required network settings, use the Network Setup Wizard. To select from the menus provided, use the arrow keys on your keyboard.

At any time, you can return to the previous menu by pressing the <Page Up> key.



Web Configuration Using DHCP

This method requires that your network implement DHCP (Dynamic Host Configuration Protocol), usually on a server or network access device such as a router that dynamically allows devices to join the network without pre-configuration. It also assumes that you will have easy access to your network's DHCP log, since you will need to know the IP address of the unit to complete the configuration over your Web browser. (If you are unsure of how to access your network's DHCP log, contact your System Administrator for details.) If the unit is powered on and connected to the network via the LAN port on the rear panel, it will automatically attempt to lease an IP address using DHCP. Before you can begin the configuration process, you will need to access the DHCP log from your file server or other device that acts as the DHCP server on the network. A simple DHCP log looks similar to the following:



The information displayed for your own network may vary significantly from the data displayed in the image, but should supply (at minimum) three essential details: IP address, MAC address, and device (or machine) name for the computers and other devices connected to your network. The values for the IP KVM tested above are as follows:

IP Address: 192.168.22.4

MAC Address: 00-0E-C5-00-08-1A

Device Name: (none)

The easiest way to identify your IP KVM on the network is by its MAC address, a unique hardware identifier that is specific to your unit. The MAC address of the unit can be found on a white sticker on the bottom of the unit. Retain this number for future reference. Once you locate the MAC address of your unit in the DHCP log, you can match it to its leased IP address and proceed with the Web configuration.

NOTE: Once you have located the IP address of the IP KVM and wish to proceed with the Web configuration, do not power off the unit or your DHCP server, since the Server Remote Control might lease a different IP address. Should this happen, reexamine the DHCP log to verify the IP address again.

Web Configuration Using Static IP

Since some networks rely on static IP addresses (every device has a pre-configured IP address that does not change), the DHCP access method described above is not applicable in those situations.

To access the Web configuration for this product, you will need to configure the workstation you are using to the same subnet (255.255.255.0) and also assign it a valid IP address (i.e. 192.168.1.100). For details on how to change the IP address of your computer (if necessary), consult your documentation or System Administrator for assistance.

NOTE: It is advisable to verify whether another device on your network is using the same IP address as the IP KVM before connecting it to the network, to avoid a conflict. Should an IP address conflict occur with another device on the network, power off the conflicting device or

assign it another IP address before continuing the installation.

NOTE: Not all IP addresses are valid for a given subnet. If you are required to change your subnet (and therefore IP address) to configure the unit, be sure the IP address you choose is within the allowable range for the 255.255.255.0 subnet.

Once your computer is configured to the same subnet as the IP KVM, you can use the IP address 192.168.1.123 to access the Web configuration system.

Terminal Configuration Using a Serial Cable

Configuring the IP KVM using a serial cable is the best choice if you need to preconfigure the unit before attaching it to a network (i.e. when sending to a branch office, customer site, etc). In general, the Web configuration is preferable because of its intuitive interface and the fact that you do not have to be within close physical proximity to perform the configuration. However, if you wish to use the serial cable method to configure the IP KVM, you can use any typical communication software package (UNIX: tip, cu, kermit, minicom; Windows: HyperTerminal, kermit).

You can use the serial port on the IP KVM to access the terminal configuration tool; to do so, you will require a null modem serial cable. Connect a female end of a serial cable to the serial port used for serial access on the host computer. Connect the opposite end to the IP KVM. Configure the terminal software with “8N1” settings:

Connection speed: 115200 bps

No. of bits: 8

Parity: None

Stop bits: 1

Flow Control: None

Using the Web Interface

The Web interface offers the most intuitive way to configure the Server Remote Control, as it provides a Java-based VNC client that can be used to control the host computer from a remote location, as well as support for any industry-standard HTML Web browser.

You can access the Web interface by opening your Web browser and entering the IP address of the Server Remote Control you wish to access/configure. The IP address will be either the **address assigned by your DHCP server** as identified in the previous section, or **192.168.1.123** (if your network uses static IP addressing).

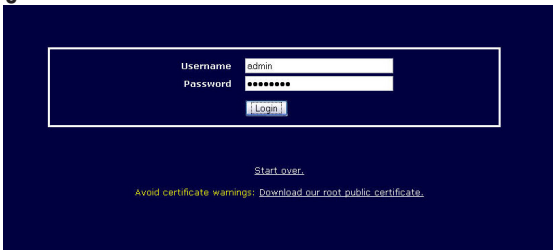
Using the web interface requires a browser, with cookies and JavaScript enabled. To start the Java VNC client, login to the Web configuration interface and click on the thumbnail of the desktop on the Home menu, or click on the *Connect* button, located in the Main Menu.

You may need to upgrade Java support in your browser; however, most modern browsers come with a version of Java that is compatible with this application. The Java VNC client makes a connection back to the Server Remote Control unit over port 5900 (by default) or 15900 (if encrypted). The encrypted connection is a standard SSL (Secure Socket Layer) encrypted link that encrypts all data from the session, including the actual video pictures.

Because Java is considered a “safe” programming language, the Java VNC client has some limitations. Certain special keystrokes cannot be sent, such as “Scroll Lock” on the keyboard.

This client software requires the use of Java 2 (JRE 1.4) to enable features like wheel mouse support. Sun Microsystems’s Java site, www.java.com, is an excellent resource to ensure your browser and operating system are updated accordingly.

The Login Screen



Before you can access the Web configuration interface, you must enter a username and password. The default username and password as shipped from the factory are username *admin*, with a password of *admin*.

NOTE: Before the login screen appears, your Web browser may display a warning about an invalid security certificate. This does *not* affect the security of your data in any way. Whenever you are prompted about a certificate security problem by your browser or the Java VNC client, always choose the option to continue.

Home

After the initial login screen, the Home screen will appear, offering a Screen Thumbnail view of the controlled computer, as well as basic file transfer functions, Monitoring Information, System Identification and VNC Client options.

Name: At the top of the screen, the name of the machine being controlled is displayed

Main Menu: At the left-most side of each page, the Main Menu is displayed, allowing users to choose functions offered by the Web Interface.

Help area: The right-most column offers an optional help summary for each page. If you don't wish to use this information, it can be closed by clicking the small [x] at the top right (within the Web Interface). If closed, click on the Help button near the top right of each page to re-display it.

NOTE: The aforementioned sections of the Web Interface will remain on the screen at all times. Selected categories will be displayed in the center of the screen.

The following elements of the Web Interface may not be available, based on assigned user privileges (i.e. non-admin users will not see any items under the Admin category).

User Preferences

The *User Preferences* screen offers several configuration options, pertaining to the functionality of the IP KVM on a per-user basis. Here, you will be able to customize settings to optimize overall performance, (e.g. Encryption options, VNC options, display and bandwidth options etc.), according to each user's individual preferences. Please save your selections by clicking the "*Save Changes"* button.

Snapshots

The Snapshots screen allows you to view and save a screenshot of the controlled computer in its current state. This screenshot will update periodically (automatically). Saved image files are stored in .PNG format.

Logout

Clicking on *Logout* logs you completely out of the web interface. You will have to login again to gain access to the web interface.

VNC

To launch or disconnect a Virtual Network connection with the controlled computer, click on “Connect” or “Disconnect” as appropriate.

Admin Functions

The Admin functions allow you to access all of the features you will need to perform an initial configuration of the IP KVM.

Network Config

DHCP (Dynamic Host Configuration Protocol)

Automatic network configuration using DHCP is: Enabled/Disabled. This feature applies only to the LAN port on the rear panel and is enabled by default. When enabled, the unit will automatically configure itself with an IP address when a DHCP server is present.

When disabled, the LAN port will use the values assigned to it in the IP Addresses and Routing section described below.

IP Addresses and Routing

This table allows you to assign IP information for the LAN and WAN ports separately. If you are using DHCP, the values for the LAN port will be filled in automatically and any changes made will not affect the

setup. If Ethernet Bridging is enabled, the WAN port will use the same settings as the LAN port, and any changes will not affect the setup for that port. Adjusting the setting for the WAN port allows you greater control over how the IP KVM is configured for access from outside the local network, particularly if a firewall or proxy is in use.

Domain Name Server (optional)

This section allows you to specify DNS servers and the default DNS domain suffix in use on the network. If DHCP is enabled, some of these values may be supplied automatically.

Clicking the “Commit” button applies any changes made on this page, but leaves the old settings active until the next time the unit restarts. Clicking “Make changes effective now” applies the changes and restarts the IP KVM so the new settings take effect immediately.

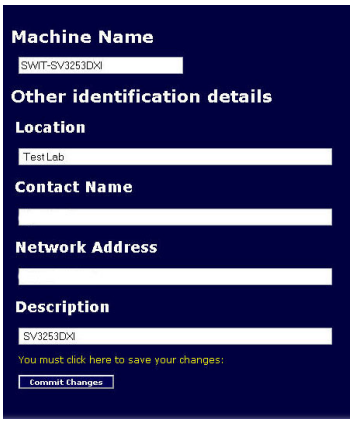
Ethernet Address (MAC Address)

This is the Ethernet hardware address of the IP KVM LAN port. This number is assigned as a factory default, and cannot be changed. You may need this number to configure your DHCP server.

User Accounts

This menu will allow you to add accounts other than admin to the system. These accounts will not have the authority to change settings, but can access the Web interface and log into the VNC console. Selecting Delete permanently removes the user from the system. If you enter values for a user that does not already exist under Edit User Details, the system will create that user for you when you click Record changes. If the user already exists, you will change the password for that user.

System Ident



Machine Name: This is the name that is used to uniquely identify this machine. You might want to create a DNS entry that matches this name. The name is provided as the Client Name for the DHCP server. It is also shown at the top of each page in the web browser interface and is the “desktop name” for VNC clients.

Other identification details: These values are for information purposes. They are visible from the VNC client and via SNMP (if enabled).

Location: This string is sent as the system.sysLocation value over SNMP. It should describe the location of this system.

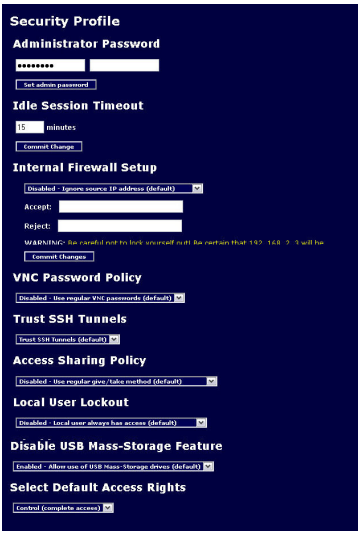
Contact Name: This string is sent as the system.sysContact value over SNMP. It should describe who to contact regarding this machine. Typically it includes an email address.

Network Address: This value is not used in our configuration, but is meant to store a user-defined value that identifies the controlled machine on the network. The official DNS name of the controlled machine is an obvious value to put here, but you may use it for any purpose.

Description: A user-defined description for the controlled machine.

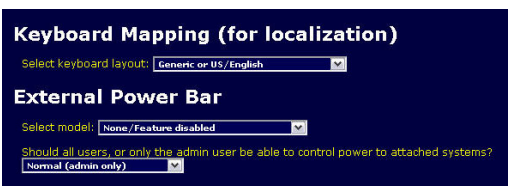
Security

This menu allows you to configure a number of settings, including changing the admin password (recommended). Read and consider the comments and instructions on this menu before making any changes, as changing these features could make the unit inaccessible through Web configuration (i.e. due to firewall filtering). Note that any password changes you make will have to be entered in duplicate to prevent the chance for error.



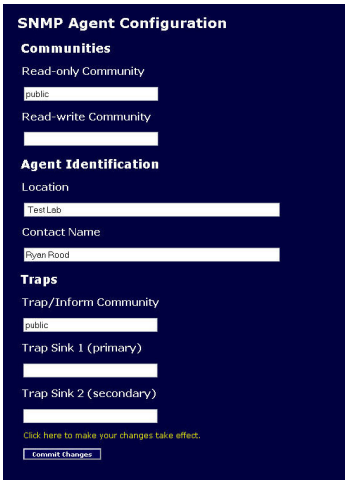
Compatibility

The Compatibility menu offers features that may offer enhanced functionality with certain KVM and power products, such as StarTech.com's Remote Power Switch (PCM8155HNA). These can be left at their default values if you are not connecting the unit to a KVM or power management device.



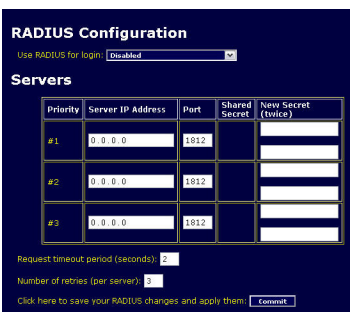
SNMP

The SNMP menu allows you to configure the IP KVM so it can be recognized and managed using industry standard Simple Network Management Protocol software.



RADIUS

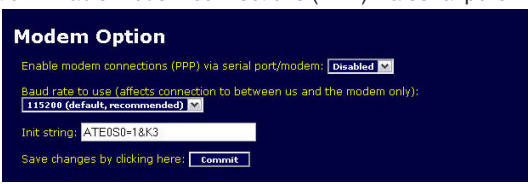
The RADIUS server requires the IP address, the UDP port number (1812 - default or 1645) and the shared secret. The shared secret is used to encrypt communications and corresponds to a shared password for the RADIUS server and the client machine. Two additional servers may be defined for backup purposes. Each server will be tried in order, using the indicated number of retries and timeout period, which are configurable on the same page.



Remember to enable RADIUS after configuring it. While RADIUS authentication is enabled, the locally defined accounts on the Server Remote Control unit will not be used, except for the SSH login. However, if a user name of the form “name.local” is given at the RADIUS prompt, the system will use “name”; check the password locally, and skip RADIUS authentication. Delete all local accounts to avoid this behavior. When connecting via VNC, a login screen is generated that asks for a RADIUS username and password.

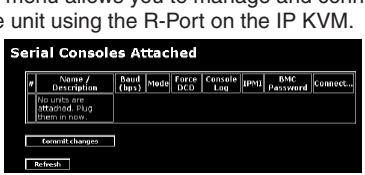
Modem

Enable this to allow the modem to answer the phone and start a PPP connection. Enable modem connections (PPP) via serial port/modem.



Serial Ports

The Serial Ports menu allows you to manage and connect to devices connected to the unit using the R-Port on the IP KVM.



Time / Date

Date and time are stored without consideration for time zone. If you are controlling multiple sites in different time zones, we recommend you use UTC (Universal Coordinated Time, also sometimes called GMT or Zulu) for all machines.

If the computer you are using to view this page knows the correct time, just press the button to set the time and date to the same time as your browser.

Firmware

The firmware on the Server Remote Control is field upgradeable. To upgrade to another version, login as admin.

Auto Self Upgrade: The IP KVM module includes an innovative feature allowing it to upgrade itself over the Internet. Simply click on the button labeled Upgrade to Latest and the unit will go out to the Internet and download the latest version of the system firmware and then install it.

If it cannot access the Internet directly (perhaps due to a web proxy or other firewalls), then a page will be shown that causes your browser to download the required file. Save this file to disk and then manually upload it as described in the next section.

Manual Upload: Enter the name of the firmware file that you downloaded from StarTech.com into the field provided (or use the Browse... button). Press Start Upload and wait until a successful upload message is shown.

NOTE: Remember the following during the firmware upgrade:

- Do NOT turn off power to unit before this operation completes successfully.
- The unit will sometimes reboot as part of the upgrade procedure,

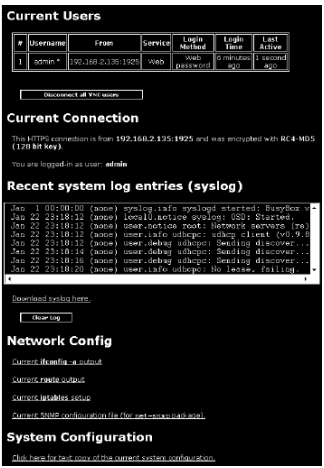
depending on which system component is upgraded. You will have to reconnect and re-login in those cases.

- Wait at least two minutes after pressing Start. Do not assume the upload did not work, the upload could simply be slow.
- Each distributed file upgrades a different component of the system. Be sure to apply all files provided as part of an upgrade. The system knows what to do with each file you give it, and they are checked for validity before being applied.

Auto Self Upgrade: Clicking the Upgrade to latest button will automatically download and install necessary revisions. To download upgrades for manual installation, please click on Get latest version.

Status

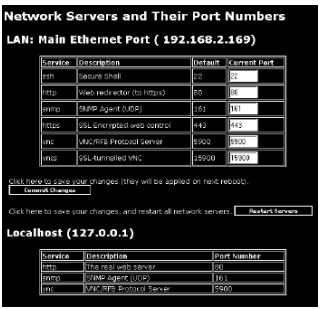
The Status screen displays a system security log, various system settings, and the ability to generate a copy of the system configuration in plain text format.



Port Numbers

Port Numbers provides a table allowing you to change TCP port values for services available on the IP KVM. By default, they are factory-set to common Internet values. You may wish to enhance security by disabling services that you will not use with the unit. To disable a service, change its port number to 0. When you have made any

necessary changes, click Commit Changes to use the settings the next time the IP KVM restarts. To force the unit to restart immediately, click Restart Servers.



Help Menu

Provides an FAQ (Frequently Asked Questions) listing to assist you with the features and operation of the IP KVM.

Site map Menu

This menu provides a hyperlinked directory of each setting available on the Web configurator.

Copyright Menu

Provides the Terms of Use and other information related to the firmware and software on the IP KVM.

Accessing the VNC Interface

There are three ways to communicate with the Server Remote Control unit in order to control the host computer:

- **Web interface:** The integrated Web server includes a Java-based VNC client. This allows easy browser-based remote control.
- **Native VNC client:** There are several third-party software programs that use the standard VNC protocol, available in open source and commercial VNC clients.
- **SSH access:** By default, there is a standard SSH server running on port 22 (the standard SSH port). Once connected via SSH, the VNC traffic is tunneled through the SSH connection and encrypts the VNC session. Each method will be discussed briefly in the following section. The type of encryption method or client used is not critical.

Web Interface

Using the IP KVM's web interface requires a browser, with cookies and JavaScript enabled. To start the Java VNC client, login to the Web configuration interface and click on the thumbnail of the desktop on the Home menu, or click on the Connect button, located in the Main Menu.

You may need to upgrade Java support in your browser; however, most modern browsers come with a version of Java that is compatible with this application. The Java VNC client makes a connection back to the Server Remote Control unit over port 5900 (by default) or 15900, if encrypted. The encrypted connection is a standard SSL (Secure Socket Layer) encrypted link that encrypts all data from the session, including the actual video pictures.

Because Java is considered a "safe" programming language, the Java VNC client has some limitations. Certain special keystrokes cannot be sent, such as "Scroll Lock" on the keyboard.

This client software requires the use of Java 2 (JRE 1.4) to enable features like wheel mouse support. Sun Microsystems's Java site, www.java.com, is an excellent resource to ensure your browser and operating system are updated accordingly.

Native VNC Client

This system implements the VNC protocol, so any off-the-shelf VNC client can be used. There are over 17 different VNC clients available and they should all work with this system. This system automatically detects and makes use of certain extensions to the basic RFB protocol that is provided by the better VNC clients.

The best client currently is TightVNC (www.tightvnc.com). Binaries are available for Windows, Linux, MacOS and many versions of Unix. Source code for all clients is available there too. This version of VNC is being actively developed. The authoritative version of VNC is available from RealVNC (www.realvnc.com). This source base is the original version of VNC, maintained by the original developers of the standard. For a commercial, supported version of VNC, you should consider TridiaVNC (www.tridiavnc.com). Their version of VNC is a superset of TightVNC and contains a number of enhancements for use in a larger corporate environment.

NOTE: Some native VNC clients may require a flag or setting indicating they should use BGR233 encoding by default. If this flag is not set, you may see a garbled picture and the client will fail. The Unix versions of VNC require the flag -bgr233. For examples on using this flag, review the commands in the following section.

SSH Tunnel (with Native VNC client)

If you are using openssh, here is the appropriate Unix command to use, based on the default settings on a machine at 10.0.0.34:

ssh -f -l admin -L 15900:127.0.0.1:5900 10.0.0.34 sleep 60

vncviewer -bgr233 127.0.0.1::15900

NOTE:

- A copy of these commands, with appropriate values filled in for your current system setting, is provided in the on-line help page. This allows you to “cut-and-paste” the required commands accordingly.

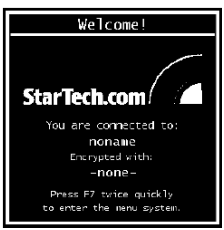
- You have 60 seconds to type the second command before the SSH connection will be terminated.
- The port number “15900” is arbitrary in the above example and can be any number (1025...65535). It is the port number used on your client machine to connect your local SSH instance with the VNC client. If you want to tunnel two or more systems, you will need to use a unique number for each instance on the same SSH client machine.
- Some Unix versions of the VNC client have integrated SSH tunneling support. Some clients require your local user id to be the same as the userid on the system.

Use a command like this: vncviewer -bgr233 -tunnel 10.0.0.34:2

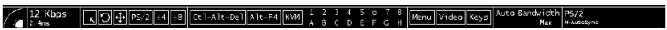
Using the VNC Menu

One of the unique features of this product is the VNC menu system. Whenever you see a window with a dark blue background and grey edges, this window has been inserted into the VNC data stream so that it is effectively laid over the existing video. These menus allow you to control the many features of the IP KVM without using the web interface or a custom client.

When you initially connect to the system, a Welcome Window will appear, indicating which system you are controlling, what encryption algorithm was used and what key strength is currently in effect. Click anywhere inside the window to clear it, or wait ten seconds.



Bribar Feature



Along the bottom of the VNC screen is a dark blue bar with various buttons known as the bribar. Its purpose is to show a number of critical status values and to provide shortcuts to commonly used features. Here is a snapshot of what it may look like. There will be slight differences based on optional features and system configuration. Starting from the left side of the Bribar, each feature and its function is outlined below.

PS/2: This area will show either PS/2 (as in this example) or USB to indicate if keyboard and mouse are being emulated via USB connection or PS/2 signals. If Autosync appears beneath this indicator, the mouse pointers on the local mouse and the VNC session will be synchronized automatically.

Bandwidth: Indicates current average bandwidth coming out of the Server Remote Control unit. The second number measures round trip time (RTT) of the connection when it was first established.

Resync: Re-aligns the remote and local mouse points so they are on top of each other.

Redraw: Redraws the entire screen contents; occurs immediately.

PS/2: Resets the PS/2 keyboard and mouse emulation. Useful to recover failed mouse and/or keyboard connections in PS/2 mode.

÷4, ÷8: Switches to thumbnail mode, at indicated size (i.e. 1/4,1/8)

Ctrl-Alt-Del: Sends this key sequence to the host.Works immediately.

Alt-F4: Sends the key sequence to host (closes windows).

KVM: Sends the KVM “hotkey” sequence. This function is only enabled when you have configured the unit to expect a particular brand of KVM downstream. It sends the key sequence to launch the KVM’s on-screen display (OSD) menu. This button is only present when a KVM model is selected in the Web interface.

Menu: Shows the main menu.

Video: Shows the video-tuning menu where the picture quality can be

adjusted.

Keys: Shows the VirtKeys menu, which allows you to simulate pressing special keys such as the Windows key or complex multi-key sequences.

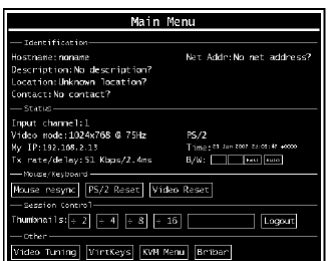
[1][A][S]: These flags show the state of the keyboard lights, NumLock, ShiftLock and ScrollLock respectively.

X: Click this button to close the Bribar and hide it. This can be very useful on a client machine that has a screen size the same as the remote machine. No vertical screen space is wasted with the Bribar. Use double-F7 to start the main menu, then click on the Bribar to restore the feature.

Other items: If the server's screen is larger than 1024x768, additional buttons will be shown to the right of the above listed items. These are all keyboard shortcuts and are duplicated in the Keys menu.

Main Menu

To access the main menu, quickly press F7 twice.You must press the key twice within one second. If you press it once or too slowly, then the F7 key(s) are sent to the host, just like any other key. This is the only way to get into the menu system, if the Bribar is disabled. Here is the main menu for a typical system:



The main menu window may be moved by clicking and dragging on the title bar. It can be closed by pressing Escape, or by clicking on the red X in the top right corner.

Here is a guide outlining various fields from the Main Menu. Most of the functions operate immediately. Other functions require a response to a confirmation prompt first before performing the requested function.

- **Identification:** Fixed text label that is defined by the user in the Web interface. This does not affect the operation of the system and is intended to assist with administration.

- **Status:** Current status of the attached system and the status of the unit.
- **B/W Min/Avg/Max/Auto:** Bandwidth control, whereincurrent operation will be indicated with white highlighting. If you choose Min/Avg/Max then you will override the default, Auto. As the automatic mode measures actual network performance, you may see the current mode switch from Min up to Avg or Max. The different modes indicate more time spent on compression versus more bandwidth. There is no visual difference between the modes, but there can be a noticeable difference in speed and smoothness.
- **Mouse Resync:** Resynchronizes the mouse pointer so that the local and remote mouse pointers are on top of each other.
- **PS/2 Reset:** Resets the PS/2 emulation going to the host and to the attached PS/2 devices. This can be used if the mouse stops responding or the PS/2 keyboard isn't working.
- **Take Control:** When multiple users are connected to the same system, use this button to take control away from another user. Only one user may control the keyboard and mouse at any time. All users see the same picture.
- **Thumbnails:** Switch to smaller thumbnail size screen images (click anywhere on thumbnail to restore it). Each button corresponds to a different sized image, from half size to one-sixteenth.
- **Logout:** End the VNC login session and disconnect.
- **Video Tuning:** Sub-menu with video adjustments, to be used when automatic picture adjustment does not provide a good quality picture.
- **VirtKeys:** Virtual keyboard provides a menu with special keys that are often hard to generate but needed by the remote system. The most common key sequence is the [Ctrl] – [Alt] – [Del].
- **KVM Menu:** Generates the key sequence used to access the on-screen menu for an enterprise-class KVM switch. When these conventional KVM switches are combined with the IP KVM, this key makes accessing their built-in menu easier, especially from the Java client. This button will only be shown when an external KVM has

been enabled via the web interface.

- **Bribar:** Closes or reopens the Bribar window along the bottom of the screen.

VirtKeys Menu

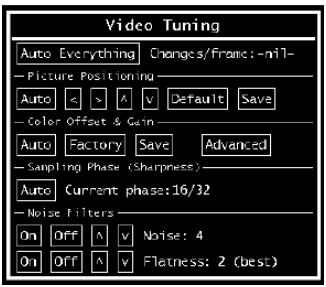
Clicking any button in the top half of the window simulates pressing and releasing the indicated key. In the bottom area of the screen, clicking will simulate the indicated Meta key being pressed.You may then click in the top part to send another key and release the Meta key at the same time. Alternatively, you may move the mouse outside this window, press the regular key, and then choose -RESET- to release all depressed keys.

The VirtKeys menu can be left open while using the host system.You can then click the required button at the suitable time, and still interact with the host in a normal fashion.

Examples:

- **[Ctrl]-[Alt]-[F4]:** Use L-Ctrl then L-Alt in the Toggles area. Then click F4.
- To bring up the Start menu under Windows: Click the L-Windows button at the top left of the above window.

Video Tuning menu



Use the Auto Everything button to automatically fine-tune all three adjustments. If the test pattern for Color Offset calibration is not present on the screen, then the Color Offset adjustment is skipped.

Changes/frame: indicates the number of 16x16 blocks of video that are being sent, on average, for every frame of video. With a static image being displayed by the server, this number will be zero (shown as -nil-). Moving the mouse, for example, will cause the number to jump to about 2 or 3.You may use this number to judge the picture quality as you adjust the controls on this menu.

Picture Positioning: affects the image position on your screen. If you see a black line on either side of your screen, or at the top or bottom, you can use the arrow buttons to shift the image in that direction. Pressing Auto does the same thing for you automatically. Use Save to save the changes you have made manually. Since this adjustment depends on the video mode, separate values are stored for each video mode.

Color Offset is a fine tuning adjustment that requires the use of a test pattern. There is a copy of the test pattern available on the Help! menu of the integrated web server. You must arrange for that image to be shown on the host computer. Do not allow scaling, cropping or any other changes to that image. Press the Auto button and the system will calibrate color for the best possible picture in approximately one minute. If the system cannot find the test pattern on the screen, it will

say so. Check that the pattern isn't scaled or covered up. It's important to do this operation in 24-bit or 32-bit color video mode (i.e. truecolor). Although the algorithm may work in 16-bit or 8-bit color video modes, the results will not be optimum and usually it won't be able to recognize the test pattern.

Pressing the **Advanced** button will open the **Advanced Video Tuning** menu. While the vast majority of users will not need to adjust these settings, it offers added control of the video settings of your VNC sessions.

Sampling Phase does not normally need to be used since the IP KVM tunes the sampling phase whenever the video mode changes. This button does not require a test pattern, but will perform optimally when used with our standard test pattern. For your reference, the sampling phase number is shown to the right of the Filtering button.

Noise Filter controls the advanced video filtering of our system. Unlike other filtering algorithms, our noise filter will only remove noise. It does not degrade the signal quality or readability of small text. You may turn it on and off using the indicated button, or set it to other values using the arrows. Higher numbers cause more filtering and may cause artifacts when moving windows. The most common visual artifact is a vertical line dropping when moving windows horizontally. You may use the Redraw button to correct these, or use a lower filter number. At minimum, these values must be greater than two.

Operating Your KVM Switch

To toggle between computers, you can use the hot-key commands, OSD (On-Screen Display) menu or by using the pushbuttons built into the 1UCABCONS series LCD Rack Console.

Push Buttons

A solid red indicator reflects the port selected. The indicator flashes red when in Auto or Manual Scan mode. You can press any of the corresponding pushbuttons to select the active computer. On the 16 port models, Port 1 and Port A share the same pushbutton, as do Port 2 and Port B, etc. To select Ports 1 through 8, press the pushbutton once. To select Ports A through H, press and hold the pushbutton for two seconds. Alternatively, if Port 1 is currently selected and you want to select Port A, you can press the pushbutton once to switch to Port A.

The K/M Reset function reconfigures your system without powering down your computers or your KVM switch. To reset the switch, press and hold the front-panel 1 and 2 buttons simultaneously.

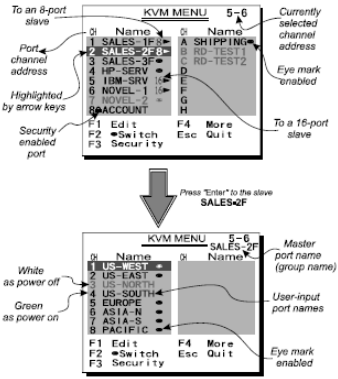
The Auto-Scan function automatically scrolls through your connected computers. Press and hold the front panel 7 and 8 buttons simultaneously to enter Auto Scan mode.

OSD Operations

A computer may be selected by issuing hot-key commands or by activating the OSD window. The **Auto-Scan** function automatically scrolls through your connected computers.

By hitting the left **<CTRL>** key twice within two seconds, you may see the Hotkey Menu (if it is enabled as an OSD option). Or, by hitting the left **<CTRL>** key three times within two seconds, you will see a KVM MENU screen (below) showing a list of the computers with corresponding channel addresses, names and status.

The port number of the currently selected computer is displayed in red, at the right corner of the OSD menu.



The color of a device name is green if it has power and is ready for operation, or the color is white if it has no power. The OSD menu updates the color when it is activated.

Use the <↑> and <↓> arrow keys to highlight a computer and the **<ENTER>** key to select it. Or, you may press **<ESCAPE>** to exit the OSD and remove the OSD menu from the display; the status window returns to the display and indicates the currently selected computer or operating status.

A triangle mark to the right of a name indicates the port is cascaded to a Slave; the number at the left of the triangle mark shows the number of ports the Slave has (i.e. 8 for an 8-port switch). The **<ENTER>** key brings you one level down and another screen pops up listing the names of the computers on that Slave. The name of the Slave will be shown at the upper right corner of the OSD menu. It is useful to group computers and still be able to see the group name.

An eye mark (👁) to the right of a name indicates the computer is selected to be monitored in Scan mode. In OSD, this mark can be switched on or off by function key **<F2>.** Press the **<ESCAPE>** key to exit OSD and to return to the selected computer; the computer name is also shown on the screen.

Editing Computer Name Assignments

Function key <F1> - To edit the name entry of a computer or a Slave, first use the <↑> and <↓> arrow keys to highlight a port then press **<F1>** followed by name entry. Valid characters are 'A'~'Z', '0'~'9' and the dash (-) character. Lowercase letters are converted to uppercase ones. Press **<BACKSPACE>** to delete one letter at a time. Non-volatile memory stores all name entries until you change, even if the unit is powered down.

Selecting Computers for Autoscan

Function key <F2> - Use this key to switch the eye mark (👁) of a computer on or off. First, use the <↑> and <↓> arrow keys to highlight it, then press **<F2>** to switch its eye mark on or off. If Scan Type reads 'Ready PC + 👁', only the power-on and eye mark selected computers will be displayed sequentially in Scan mode.

Locking Devices (Slave or computer

Function key <F3> - To lock a device (a computer or a Slave) from unauthorized access, use Security. Security is effective for only one device (a computer or a Slave). To lock a device, use the <↑> and <↓> arrow keys to highlight it, then press **<F3>**. Now, enter up to 4 characters ('A'~'Z', '0'~'9', '-') followed by **<ENTER>** as new password. A Security enabled device is marked with a lock (🔒)following its port number. To permanently disable the security function from a locked device, highlight it, press **<F3>** then enter the password.

If you want to access the locked device temporarily, simply highlight it and press **<ENTER>**. The OSD will prompt for the password. After entering the correct password, you are allowed to use the device. This device is automatically re-locked once you switch to another one. During Scan mode, OSD skips the security-enabled device. Note: Only one device (a computer or a Slave) can be locked by this function at a time.

- **NOTE**: If you forget the password, the only way to permanently disable the security function is to remove all possible power sources from the Console. You will need to turn off all computers and unplug all power adapters, then restart everything.

Advanced Functions

Function key <F4> - More functions are available by hitting **<F4>**. A new screen pops up displaying more functions as described below. Most of them are marked with a triangle (<▲>) indicating there are options to choose from. Using the <↑> and <↓> arrow keys, select the functions and press **<ENTER>**. Available options will be shown in the middle of the screen. Again, using the <↑> and <↓> arrow keys to view options, then press **<ENTER>** to select it. You can press **<ESCAPE>** to exit at any time.

Auto Scan

In this mode, the Console automatically switches from one powered computer to the next, sequentially in a fixed interval. During Auto Scan mode, the OSD displays the name of the selected computer. When Auto Scan detects any keyboard or mouse activity, it suspends the scanning until activity stops; it then resumes with the next computer in sequence. To abort Auto Scan mode, press the left **<CTRL>** twice, or, press any front button. Scan Type and Scan Rate set the scan pattern. Scan Type (**<F4>**:More\Scan Type) determines if scanned computers must also be eye mark selected. Scan Rate (**<F4>**:More\Scan Rate) sets the display interval when a computer is selected before selecting the next one.

Manual Scan

Scan through power-on computers one by one by keyboard control. Scan Type (**<F4>**:More\Scan Type) determines if scanned computers must also be eye mark selected. Press the <↑> key to select the previous computer and the down arrow key to select the next computer. Press any other key to abort Manual Scan mode.

Audio Stick

An optional multimedia module can be linked to the back of each KVM Module for selecting microphone and stereo speaker signals. There are two options for Audio Stick: On and Off. When set to On, audio selection follows computer selection. When set to Off, audio selection stops following computer selection. It is useful if you want to listen to a particular computer's audio signal while operating other computers. The non-volatile memory stores the Audio Stick setting.

Scan Type

Ready PC + 👁: In Scan mode, scan through power-on and eye mark selected computers. Ready PC: In Scan mode, scan through power-on computers. The non-volatile memory stores the Scan Type setting.

Scan Rate

Sets the duration of a computer displayed in Auto Scan mode. The options are 3 seconds, 8 seconds, 15 seconds and 30 seconds. The non-volatile memory stores the Scan Rate setting.

Keyboard Speed

The Console offers keyboard typematic settings that override similar settings in the BIOS and in Windows. Available speed options are Low, Middle, Fast and Faster as 10, 15, 20 and 30 characters/sec respectively. The non-volatile memory stores the Keyboard Speed setting.

Hotkey Menu

When you hit the left **<CTRL>** key twice within two seconds, the Hotkey Menu appears displaying a list of hot-key commands if the option is On. The Hotkey Menu can be turned Off if you prefer not to see it when the left **<CTRL>** key is hit twice. The non-volatile memory stores the Hotkey Menu setting.

CH Display

Auto Off: After you select a computer, the port number and name of the computer will appear on the screen for 3 seconds then disappear automatically. Always On: The port number and name of a selected computer and/or OSD status are displayed on the screen all the time. The non-volatile memory stores the CH Display setting.

Position

The position of the selected computer name and/or OSD status displayed on screen during operation. The actual display position shifts due to different VGA resolution, the higher the resolution the higher the display position. The nonvolatile memory stores the Position setting. UL as Upper Left, UR as Upper Right, LL as Lower Left, LR as Lower Right. MI as Middle.

Hot-key commands

A Hot-key command is a short keyboard sequence used to select a computer, to activate computer scan, etc. The Console constantly interprets keystrokes for hot-keys. A hot-key sequence starts with two left **<CTRL>** keystrokes followed by one or two more keystrokes. A built-in alarm generates a high-pitch beep for correct hot-key command; otherwise, one low-pitch beep for error and the bad key sequence will not be forwarded to the selected computer.

The short form hot-key menu can be turned on as an OSD function (**<F4>**: more\Hotkey Menu) every time the left **<CTRL>** key is pressed twice.

CTRL: is the **<CTRL>** key located at the left side of the keyboard.

1~8/A~H: are the number keys '1' ~ '8' at the upper row of the keyboard and character keys 'A' ~ 'H' case insensitive. Do not use the keypad at the right of the keyboard.

To select a computer by hot-key command, you must know its port number, which is determined by the KVM Module connection. For a computer connected to a Master, its port is represented by the PC port label (1~8 or A~H). For a computer connected to a Slave, two characters represent its port. The first character is the port number of the Master unit (1~8) and the second one is the port number of the Slave (1~8 or A~H). Please note that only Master's 'PC 1' ~'PC 8' ports can be connected to a Slave.

Left Ctrl + left Ctrl + 7

Selects a computer connected to port 7 of the Master.

Left Ctrl + left Ctrl + 6 + C

Selects a computer connected to port C of a Slave connected to port 6 of the Master.

To start Auto Scan, automatically scan power-on computers one by one at a fixed interval:

Left Ctrl + left Ctrl + F1

When Auto Scan detects any keyboard or mouse activity, it suspends the scanning till activity stops; it then resumes with the next computer in sequence. The length of the Auto Scan interval (Scan Rate) is adjustable, see below. To abort the Auto Scan mode, press the left Ctrl key twice.

* **NOTE:** Scan Type determines whether an eye-marked computer is to be displayed during Auto Scan.

Manual Scan enables you to manually switch back and forth between power-on computers.

Left Ctrl + left Ctrl + F2

Press <↑> or <↓> to select the previous or the next computer in sequence. Press any other key to abort the Manual Scan.

* **NOTE:** Scan Type determines whether an eye-marked computer is to be displayed during Auto Scan.

To adjust Scan Rate which sets the duration before switching to the next computer in Auto Scan:

Left Ctrl + left Ctrl + F3

The Rack Console sends one to four beeps indicating scan interval of 3, 8, 15 and 30 seconds respectively. To adjust keyboard typematic rate (characters/sec), this setting over-rides that of BIOS and any operating system:

Left Ctrl + left Ctrl + F4

The Rack Console will generate 1 to 4 beeps corresponding to 10, 15, 20 and 30 characters/sec respectively.

Change Configuration while Running

A device (a computer or a KVM switch) at any 'PC x' port can be changed at any time after initial power-up. If you change any one of the PC 1 to PC 8 ports connection from a computer to a Slave or vice versa, or replace the devices of a port, the OSD will update this change the next time it is activated.

* **NOTE:** Any new device must be turned off before it is connected to the Master.

Troubleshooting

Forgotten master password.

You can reset the master password using the serial interface on the unit. Use the 'S' command, and type a new password. The old password is not required for this procedure.

Remote mouse and local mouse don't line up.

Use the Mouse resync command in the main menu or press the Resync button on the Bribar. If the mouse pointers still don't line up, verify that mouse acceleration has been disabled.

* **NOTE:** The Windows login screen does not accept the "mouse acceleration" configuration, and always has the mouse accelerated regardless of your configuration. Therefore, on this screen it is best to avoid using the mouse.

Disabling Mouse Acceleration on the Host Computer

Many operating systems offer a feature called mouse acceleration, allowing the user to adjust the responsiveness of the cursor on the screen in relation to physical movements of the mouse. While this is usually a beneficial interface enhancement, it will interfere with the operation of the IP KVM and should be disabled on the host computer (connected to the IP KVM) before a remote session is attempted.

To disable mouse acceleration for the host computer operating system:

Windows 98

1. From the Control Panel, click on *Mouse*.
2. From Mouse Properties, click on the *Motion* tab.
3. Make sure the *Pointer speed bar* is centered and Acceleration is set to *None*.

Windows 2000

1. From the Control Panel, click on *Mouse*.
2. From Mouse properties, click on the *Motion* tab.
3. Make sure that the *Pointer speed bar* is centered and Acceleration is set to *None*.

Windows XP and Windows Server 2003

Go to Pointer Options in Control Panel and turn off *Enhance Pointer Precision*. Ensure that the pointer speed bar is centered.

Linux, UNIX and X-Windows

Add this command to your xinitrc, xsession or other startup script:

```
xset m 0/0 0
```

Also, under *Pointer Control*, verify that acceleration and threshold are zero, with the command:

```
xset q
```

After resync, the mouse pointers are still not aligned.

Use the video adjust menu to position your video image exactly where it should be. Normally a slight video positioning error is perceived as a mouse sync issue. A video positioning error is visible as a black line along the top or bottom (and right or left) edges of the remote screen. Remember to save your position changes!

Cannot login via SSH.

Remember to use either admin or a username created in the system as the user name you give your SSH client. If you see a warning about identity of host cannot be verified, and a question about saving the host's fingerprint, this is normal for the first time you connect to any machine running SSH. You should answer yes so that your SSH client saves the public key of this host and doesn't re-issue this warning.

Certificate warning shown when connecting via HTTPS

It is normal for a warning dialog to be shown when connecting via HTTPS. The SSL certificate the IP KVM uses is created when the unit is first produced. It does not contain the correct hostname (subject name) because you can change the hostname as required. Also, it is not signed by a recognized certificate authority (CA) but is signed by our own signing authority.

Mouse performance is erratic when using the GNOME or KDE desktop in a Linux X-Window environment.

The mouse controls in GNOME and KDE environments offer both an acceleration and sensitivity setting. The following directions correct this issue, and apply to Red Hat Fedora Core 2, but should be similar for other distributions that use GNOME or KDE:

1. Click the Launch menu icon.
2. Choose Preferences > Mouse.
3. Click the Motion tab.
4. Set the Acceleration bar to the setting immediately left of center.
5. Set the Sensitivity bar to the leftmost settings (lowest possible)

Specifications

	CAB1641HDIEU
Number of Ports	16
Connectors	16 x DE-15 PC connectors 1 x VGA female output 1 x RJ45 Ethernet female 1 x DB9 serial male 1 x Power connector **Inactive:** 2 x USB female input (keyboard/mouse)
Maximum Resolution	1920x1440
On Screen Display	Yes
Port Switching Control	Hot-keys, OSD, Push Button
Auto Scan	Yes
Auto Scan Interval	3, 8, 15, 30
Power Adapter Included	No (included with 1UCABCONS)
Dimensions	436.0mm x 180.0mm x 45.0mm
Weight	1380g

Technical Support

StarTech.com's lifetime technical support is an integral part of our commitment to provide industry-leading solutions. If you ever need help with your product, visit www.startech.com/support and access our comprehensive selection of online tools, documentation, and downloads.

Warranty Information

This product is backed by a one year warranty.

In addition, StarTech.com warrants its products against defects in materials and workmanship for the periods noted, following the initial date of purchase. During this period, the products may be returned for repair, or replacement with equivalent products at our discretion. The warranty covers parts and labor costs only. StarTech.com does not warrant its products from defects or damages arising from misuse, abuse, alteration, or normal wear and tear.

Limitation of Liability

In no event shall the liability of StarTech.com Ltd. and StarTech.com USA LLP (or their officers, directors, employees or agents) for any damages (whether direct or indirect, special, punitive, incidental, consequential, or otherwise), loss of profits, loss of business, or any pecuniary loss, arising out of or related to the use of the product exceed the actual price paid for the product. Some states do not allow the exclusion or limitation of incidental or consequential damages. If such laws apply, the limitations or exclusions contained in this statement may not apply to you.

StarTech.com

Making hard-to-find easy!®

StarTech.com has been making “hard-to-find easy” since 1985, providing high quality solutions to a diverse IT and A/V customer base that spans many channels, including government, education and industrial facilities to name just a few. We offer an unmatched selection of computer parts, cables, A/V products, KVM and Server Management solutions, serving a worldwide market through our locations in the United States, Canada, the United Kingdom and Taiwan.

Visit **www.startech.com** today for complete information about all our products and to access exclusive interactive tools such as the Cable Finder, Parts Finder and the KVM Reference Guide.