

Rackmount LCD Console with Integrated 16 Port IP KVM

CABCONS1716I



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	1
Features	1
Required Cables and Hardware	1
Assembly.....	4
Hardware Guide	9
Front Panel Functions.....	9
LCD Panel Power SwitchRear Panel Functions	10
Network Configuration.....	11
Web Configuration Using the On-Screen Display.....	11
Web Configuration Using DHCP	12
Web Configuration Using Static IP	14
Terminal Configuration Using a Serial Cable.....	14
Using the Web Interface	16
The Login Screen	16
Navigating the Web Interface.....	17
Main Menu selections.....	18
Using the Terminal Interface via Serial Port.....	25
The VNC Interface.....	25
Web Interface	25
Native VNC Client.....	26
Using the VNC Menu	28
Main Menu.....	30
VirtKeys Menu	32
Video Tuning menu	33

Accessing KVM Features	35
Cascade Configuration	35
OSD Operations	36
OSD Function Keys	37
Hot Key Commands.....	40
Changing Your Configuration	42
Optimizing video performance	42
Using the Advanced Video Tuning feature	43
Using the Modem Feature	45
Connecting a Modem	45
Modem configuration	46
Configuring the Remote Connection	47
Accessing the Web Interface	48
Modem Troubleshooting Guide.....	50
Serial Remote Control operation	50
Advanced Configuration Using the Integrated SSH Shell.....	53
Remote Login via SSH	54
About Security Certificate Warnings.....	55
Troubleshooting	56
Keyboard Replacement	58
Touchpad Replacement	58
Specifications	60
Technical Support	61
Warranty Information	61

Introduction

Thank you for purchasing a StarTech.com 17" Rackmount LCD Console with Integrated 16 Port IP KVM.

An ideal solution to help save valuable cabinet space, CABCONS1716I allows you to securely access connected servers from anywhere in the world over the Internet or over a LAN or WAN, and integrates a 17" active matrix LCD monitor, low-profile keyboard and touchpad that can be folded down into just 1U of cabinet space.

Features

- High resolution 17" Active Matrix Color TFT LCD monitor, displays up to 1280 x 1024 pixels
- Users can reboot the system, access the BIOS, and have full control over the connected keyboard and mouse - as if they are on site
- Modular design
- Web-based control allows client access using a standard browser - eliminating licensing costs and simplifying usage
- "Keep-alive" feature draws power from PC keyboard ports if power is lost. The Switch will continue to operate during power outage even if it loses power

Required Cables and Hardware

Depending on your needs, you may require one or more of the following cables:

All applications

- StarTech.com part number: M45PATCHxxxx
1 x Straight-through Ethernet patch cable (to connect the unit to your LAN)
- StarTech.com part number: SVECONxx
StarTech.com PS/2 3-in-1 KVM Cables (1 for each managed computer)

- StarTech.com part number: SCNM9FF
StarTech.com 10 ft. Cross Wired Serial/Null Modem Cable DB9 F/F
- StarTech.com part number: SVECONUSXX
StarTech.com Ultra-Thin USB 2-in-1 KVM Cable

Console Installation

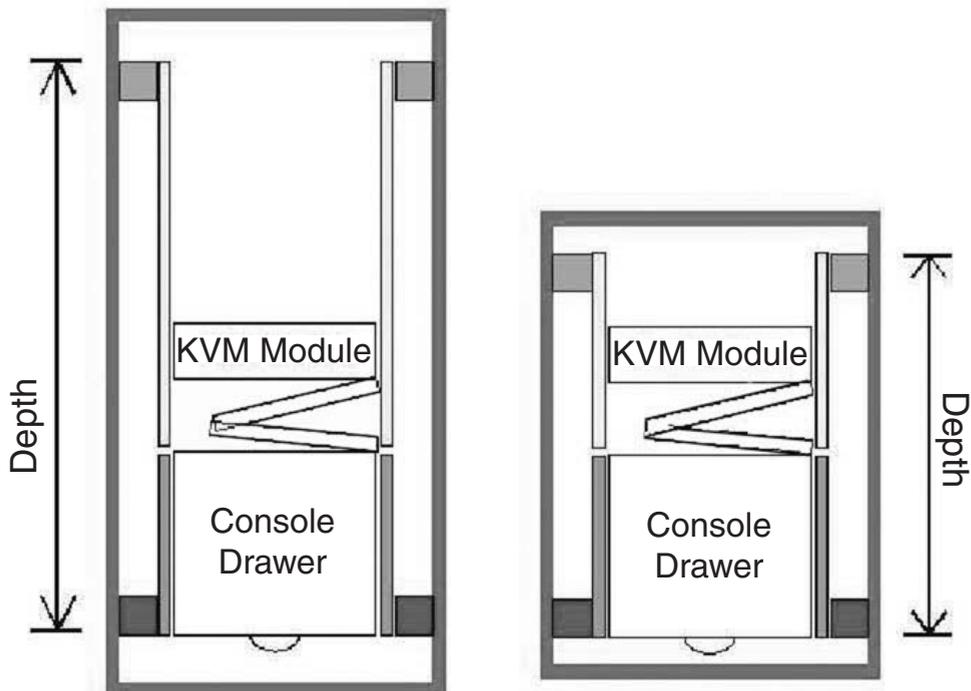
- 1U Cabinet Console - assembled “LCD panel + keyboard + touch pad” drawer
- Rear bracket & extension kit - This kit contains two pieces of rear brackets and two extensions. Make sure you have the correct kit to fit the depth of your cabinet.

Note: the following length is measured between front and rear poles, *inside* the rack cabinet not the outside depth of a rack

Front pole to rear pole distance (Depth)	cm	inch
Minimum	59	23.2
Maximum	96	37.8

Front pole to rear pole distance (Depth)	CABCONS30KIT		CABCONS42KIT	
	cm	inch	cm	inch
Minimum	57.5	22 5/8	77.5	30 1/2
Maximum	70.5	27 3/4	90.5	35 5/8

Overhead Diagram

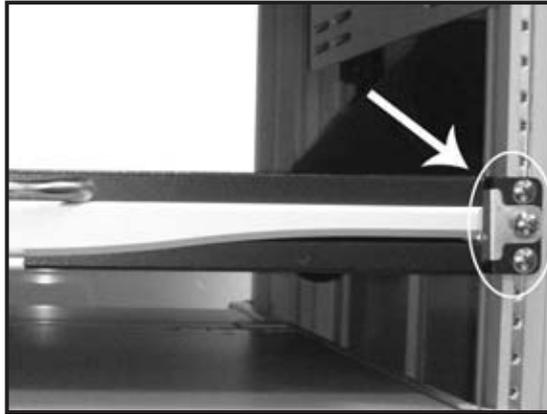


The KVM Module can be connected to a console, or be used as a stand-alone KVM Switch. There are three major categories: PS/2, USB and Sun Interfaces.

Please note: You can only connect to a computer using the PS/2 port.

Assembly

1. Remove the safety stopper from the console drawer. The safety stopper is designed to prevent the drawer from sliding out during transportation. Please note that once the Safety Stopper is removed, the drawer is free to slide out when the console is tilted. Be cautious, as this could cause injury.



2. Attach the extensions (from the Rear bracket & extension kit) to both sides of the KVM switch module. Please note the length of the extensions and mount them as shown. For a 2U module, the extensions are mounted to the lower half of the module.



Instruction Manual

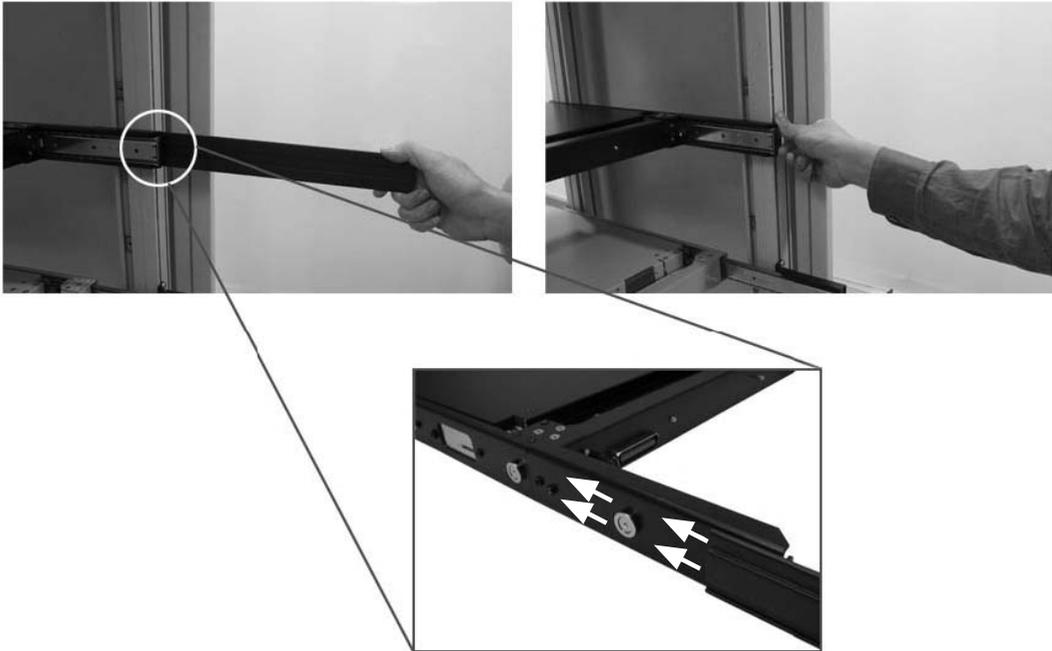
Please note the orientation of the wide side of the extension



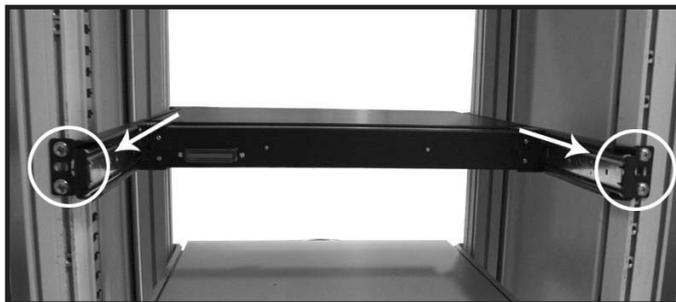
3. Fasten the console to the rack, using the provided screws.



- Slide the rear bracket into both sides of the unit, ensuring the three round screws are **INSIDE** the bracket track, while sliding inward (noting the arrows in the diagram below).



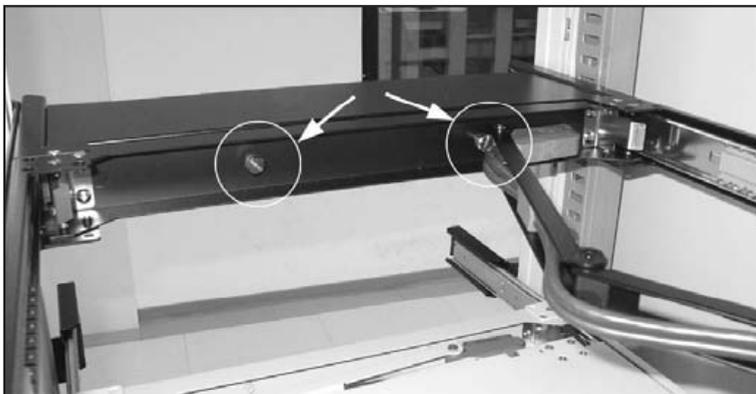
- Attach both brackets to the rack:



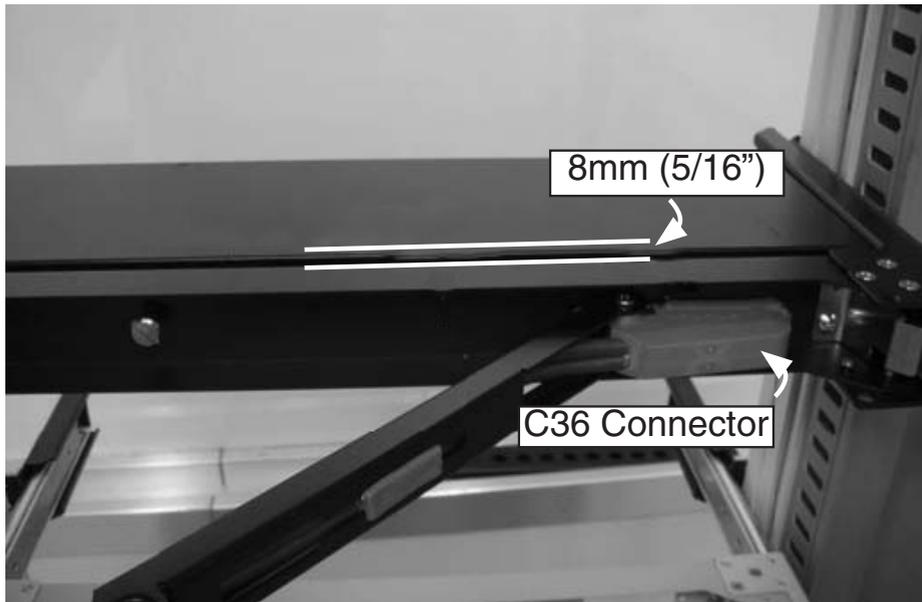
6. Push the KVM switch module evenly toward the drawer:



7. Slide the console drawer out and fasten both units using the screws provided:



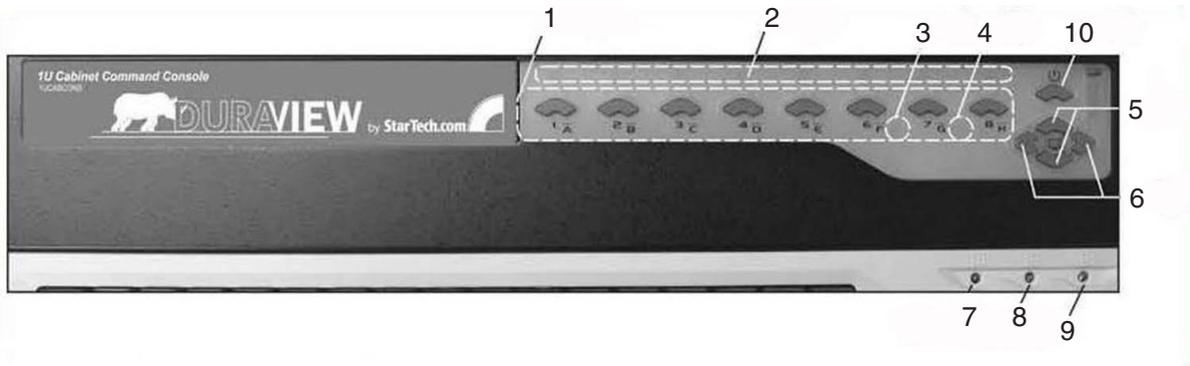
8. Make sure the C-36 connectors are firmly connected:



9. Connect the power supply to the power jack on the KVM module to complete the assembly.

Hardware Guide

Front Panel Functions



KVM Control and Status:

(This section is effective only when a KVM switch module is connected.)

- 1. Computer Selection Pad** - Press one of these pushbuttons to select a computer. For 16 port models, 1-8 represent the lower 8 ports, while A-H indicates the higher 8 ports. Port 1 and A share the same push button; if port 1 is already selected, tap its pushbutton to select port A. If port 1 is not selected, press and hold pushbutton 1 for two seconds to select port A.
- 2. Selected Computer Indicator** - One of the indicators turns red when a corresponding computer is selected by pushbuttons, hotkey or OSD menu.
- 3. Local Console in Operation** - When a computer is accessed through the console, this will illuminate green.
- 4. Remote Console in Operation** - This will illuminate green when a computer is accessed by another set of keyboard/mouse/monitor connected to the Remote console when the KVM Switch Function Module is a 2-console KVM.

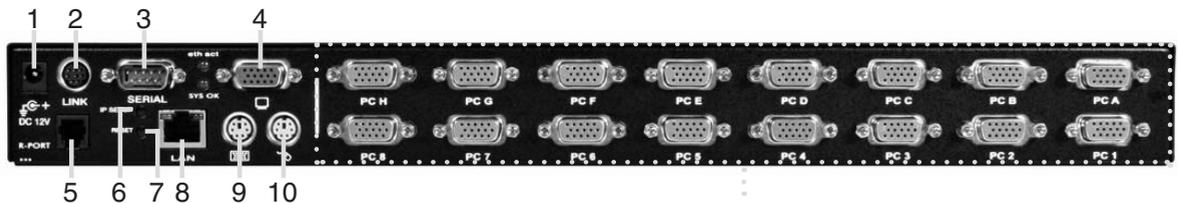
LCD Panel Control:

- 5. LCD Panel Menu** - These buttons invoke the OSD menu for the LCD panel and acts as menu selection/navigation
- 6. LCD Panel Adjustment** - Lets you adjust settings for the LCD panel.

Keyboard Status and LCD Panel Power Switch:

7. **Num Lock** - Keyboard Num Lock status
8. **Caps Lock** - Keyboard Caps Lock status
9. **Scroll Lock** - Keyboard Scroll Lock status
10. **LCD Panel Power Switch**

Rear Panel Functions



11

1. **DC In**
2. **Link**
3. **Serial Port**
4. **VGA Out**
5. **R-Port**
6. **IP Setup button** - Pressing this button (using a paperclip, etc.) will automatically load the On-Screen Display.
7. **Reset button**
 - a) Power reset - reboots power to the CABCONS1716I unit
 - b) Configuration reset - During configuration, resets values to default
8. **LAN**
9. **PS/2 Keyboard**
10. **PS/2 Mouse**
11. **Remote connections (x 16)**

Network Configuration

CABCONS1716I offers four distinct methods for configuring the unit for your network. Which method will work best depends on your level of experience and your specific network configuration.



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

Web Configuration Using the On-Screen Display

Upon boot-up, including following a reset, CABCONS1716I will display a window on the local video output (front VGA connector), that will appear as follows:

Assigned IP Address

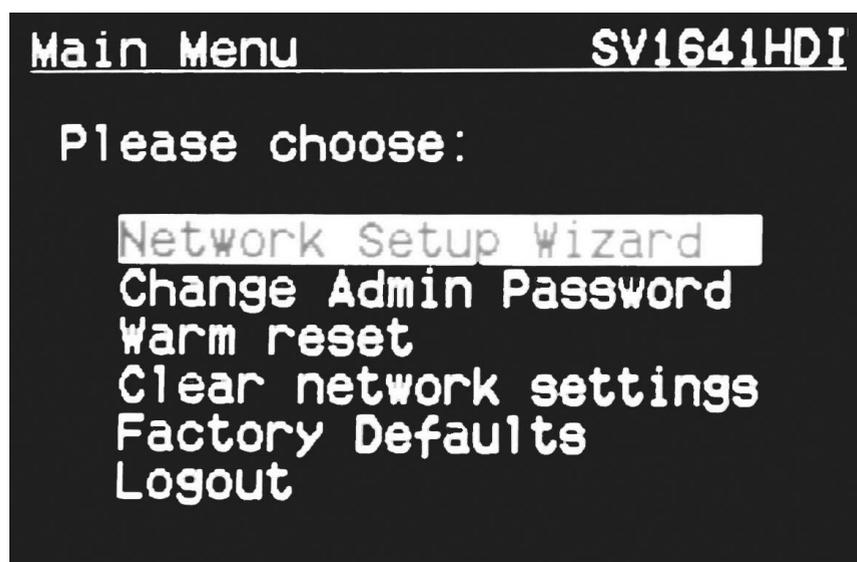
```
Network Settings SV1641HDI
Enter this web URL:
https://192.168.2.13
DHCP: No
LAN addr: 192.168.2.13
Netmask: 255.255.255.0
Gateway: 192.168.2.1
Ethernet: 00:0E:C5:00:52:12
```

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. If this is the case, connect a local PS/2 keyboard and press the **Enter** key. In order to proceed, you will require an administrative user-name 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.

Alternatively, you may press the **Setup** button on the front panel, and you will not be asked to enter the admin password if you just press Enter.

At the main OSD menu (pictured below), you will be given several basic setup options. To configure CABCONS1716I to your required network settings, use the Network Setup Wizard. To select from the menus provided, use the arrow keys on your keyboard.



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:

DHCP Client Log 		
DHCP Client Log View your LAN client's information that are currently linked to the Broadband router's DHCP server.		
Numbers of DHCP Clients: 3		
ip=192.168.22.3	mac=00-03-93-D1-D7-18	name=stpcpm18
ip=192.168.22.4	mac=00-0E-C5-00-08-1A	
ip=192.168.22.5	mac=00-00-39-03-56-D6	name=STPCMOBILE01

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 CABCONS1716I 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 CABCONS1716I 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 CABCONS1716I. 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 CABCONS1716I 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, re-examine the DHCP log to verify the IP address again.

Web Configuration Using Static IP

Unlike the DHCP access method described above, some networks rely on static IP addresses wherein every device has a pre-configured IP address that does not change.

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 CABCONS1716I 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 CABCONS1716I, you can use the IP address 192.168.1.123 to access the Web configuration system.

Terminal Configuration Using a Serial Cable

Configuring the CABCONS1716I 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 CABCONS1716I, you can use any typical communication software package (UNIX: tip, cu, kermit, minicom; Windows: HyperTerminal, kermit).

You can use the serial port on the CABCONS1716I 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 CAB-CONS1716I. Configure the terminal software with “8N1” settings:

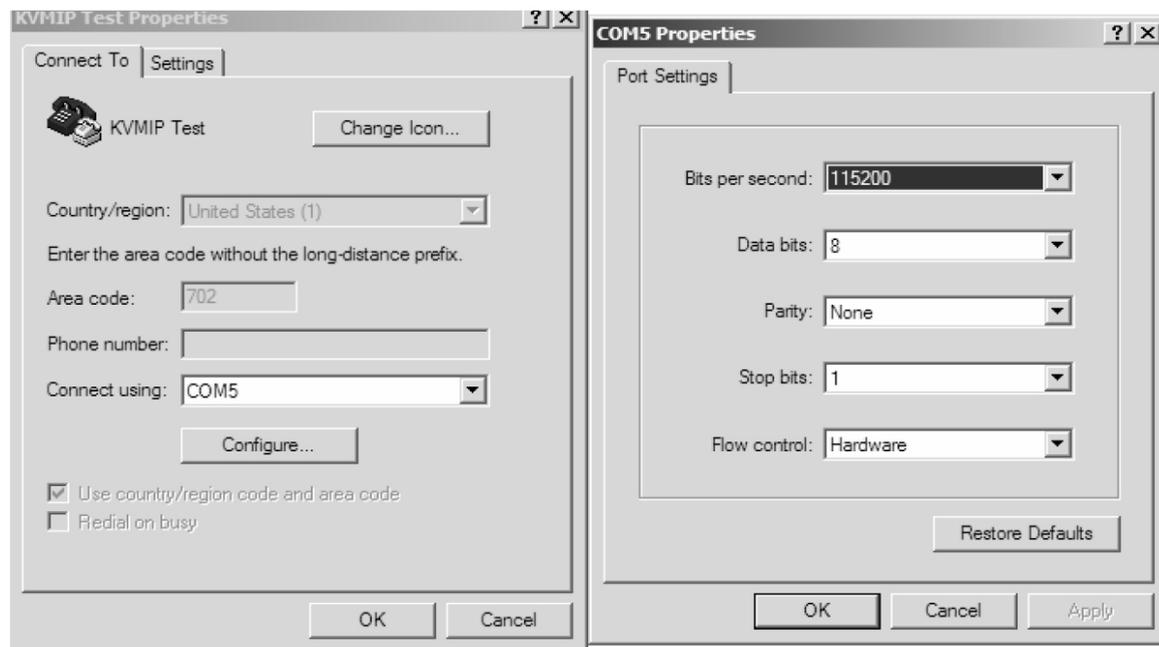
Connection speed: 115200 bps

No. of bits: 8

Parity: None

Stop bits: 1

Sample HyperTerminal configuration:



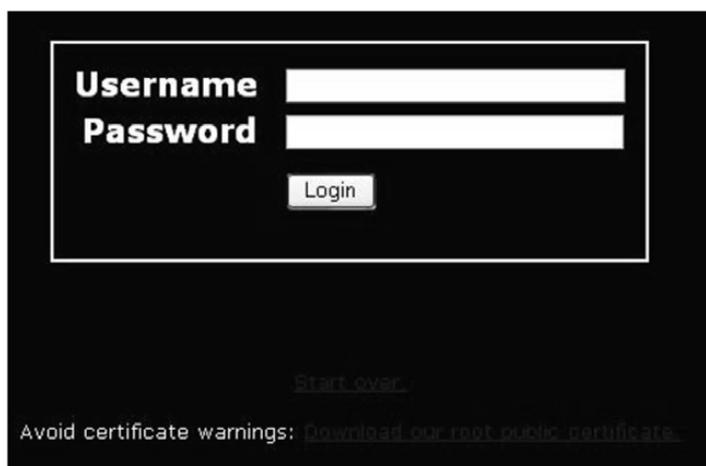
Using the Web Interface

The Web interface is the most intuitive way to configure the CAB-CONS1716I. As it offers 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 CABCONS1716I you wish to configure. The IP address will be either:

- a) The address assigned by your DHCP server as identified in the previous section, or
- b) 192.168.1.123 if your network uses static IP addressing.

The Login Screen



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

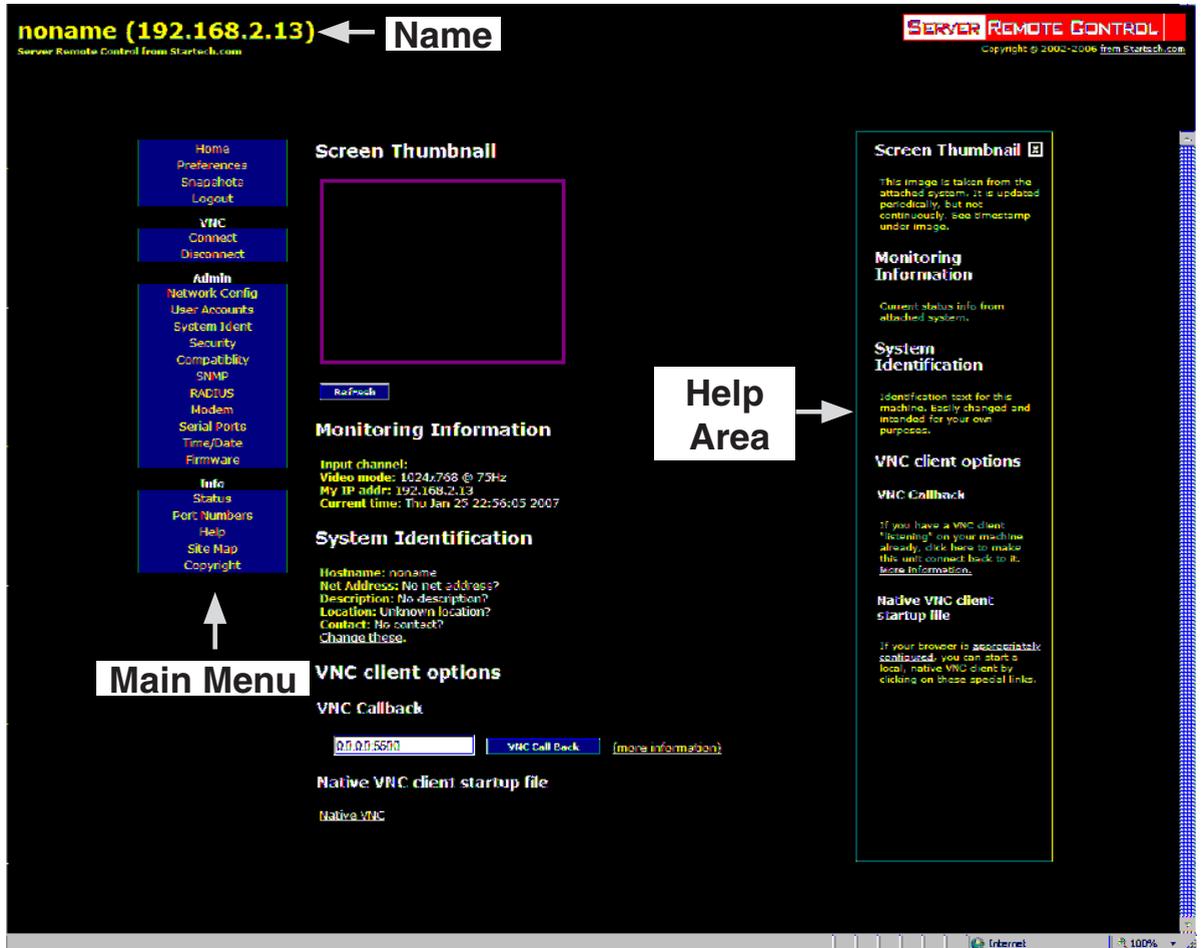
Whenever you are prompted about a certificate security problem by your



Please 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.

browser or the Java VNC client, always choose the option to continue.

Navigating the Web Interface



After the initial login, the screen is divided into several sections, three of which will remain on the screen at all times while viewing the Web Interface:

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.

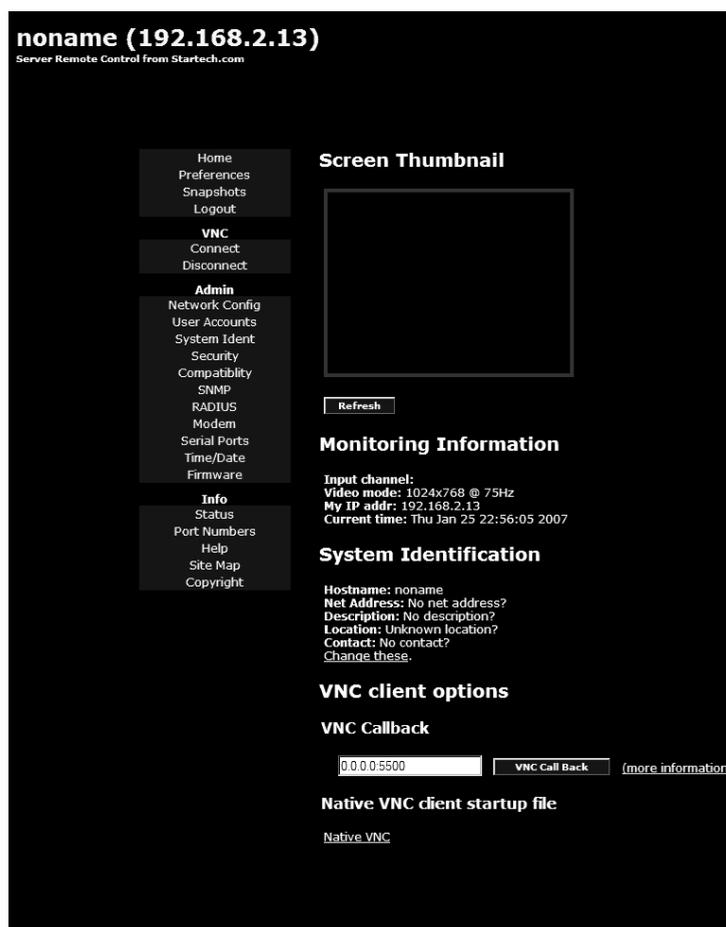
Help area: The right-most column offers an optional help summary for each page. If you don't wish to use this information, it can be closed by clicking the small [x] at the top right (within the Web Interface). If closed,

click on the Help button near the top right of each page to re-display it.

Please note: The aforementioned sections of the Web Interface will remain on-screen, with selected categories displayed center screen.

Main Menu selections

Please note: Some of the following items may not be present, based on assigned user privileges (i.e. non-admin users will not see any items under the Admin category).



Home: The **Home** screen offers a Screen Thumbnail view of the controlled computer, as well as basic file transfer functions, Monitoring Information, System Identification and VNC Client options:

Preferences: The **Preferences** screen offers several configuration options, pertaining to the functionality of CABCONS1716I. Here, you will be able to customize settings to optimize overall performance, (i.e. Encryp-

tion 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 will terminate your Web Interface section. To re-initiate the Web Interface, you will be required to re-enter your user-name and password.

VNC: To launch or disconnect a Virtual Network connection with the controlled computer, click on Connect or Disconnect as appropriate

Network Configuration

Please note: You are viewing this page over the network, so these values are probably very close to what you want. Make changes here with great caution.

[View/debug current network setup values here.](#)

Dynamic Host Configuration Protocol (DHCP)

Automatic network configuration using DHCP is:

IP Addresses and Routing

Port	IP Address	Subnet mask	Gateway (or 0.0.0.0 for none)	Broadcast (or leave blank)
LAN	192.168.2.169	255.255.255.0	0.0.0.0	192.168.1.255

Default gateway (or 0.0.0.0 for none):

Domain Name Server

DNS Servers (example: 10.0.0.123,10.2.3.34):

Default DNS domain suffix (example: startech.com):

Commit Network Changes

Click here to save your changes (they will be applied on next reboot).

Click here to reconfigure network settings immediately.

Ethernet Address (MAC Address)

LAN: 00:0e:c5:00:52:12

Network Config:

DHCP: 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 on the IP Addresses and Routing table 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.

Domain Name Server: 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 CABCONS1716I so the new settings take effect immediately.

Ethernet Address (MAC Address): This is the Ethernet hardware address of this unit's LAN/WAN port. It is set at the factory and cannot be changed. You may need this number to configure your DHCP server.

#	Username	Password	Delete user
	(None yet)		

Edit User Details

Select a user name from the above list, then edit here.

Username:

Password:

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 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).



Please 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 provide 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 CABCONS17161 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 in 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 CABCONS17161.

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

RADIUS Configuration

Use RADIUS for login:

Servers

Priority	Server IP Address	Port	Shared Secret	New Secret (twice)
#1	0.0.0.0	1812		
#2	0.0.0.0	1812		
#3	0.0.0.0	1812		

Request timeout period (seconds):

Number of retries (per server):

Click here to save your RADIUS changes and apply them:

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 CABCONS1716I unit is able to upgrade itself over the Internet. Simply click on the button labeled **Upgrade to Latest** and the unit will access the Internet to 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.

Purchase Options: Certain firmware features may be offered separately from the base unit, in order to reduce the initial cost for the Server Remote Control unit.



NOTE: If you wish to upgrade after the system is in operation, go to the Manage Firmware page and scroll down to the section entitled **Purchase Options**.

Look for a unique code, such as: 4-C80C-B960-1-0. If you provide this code to the technical support department, they can give you an unlock code that will open any feature you request. Types in the code provided, exactly, into the area provided and click **Submit**. The new features opened by the code will be enabled immediately, but you may need to reboot the unit to begin using certain features.

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 CABCONS1716I. By default, they are factory configured 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 CABCONS1716I 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 CABCONS1716I.

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 CABCONS1716I.

Using the Terminal Interface via Serial Port

The terminal interface can be accessed via the serial port for configuration of the basic settings of the CABCONS1716I. While not intended to be a substitute for the Web interface, it does allow you to configure similar functions. The menu list below describes the options that can be modified through the terminal interface.

Note that you must use the **W** option to confirm and apply any changes made before you exit the terminal session.

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 the VNC session is encrypted. Each method will be discussed briefly in the following section. The type of encryption method or client used is not critical.

Web Interface

Using CABCONS1716I's web interface requires a browser, with cookies and JavaScript enabled. To launch 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, <http://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 several different VNC clients available, all of which should work with this system, as the system automatically detects and makes use of certain extensions to the basic RFB protocol as provided by the VNC clients.

The best client currently is TightVNC (<http://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 (<http://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, the following Unix command is appropriate 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
```

Same command, but using the WAN port:

```
ssh -f -l admin -L 15900:127.0.0.1:5900 10.0.0.98 sleep 60  
vncviewer -bgr233 127.0.0.1::15900
```

Notes:

- 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 10.0.0.34:22`

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 CABCONS1716I 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 of the features and their respective functions are 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.

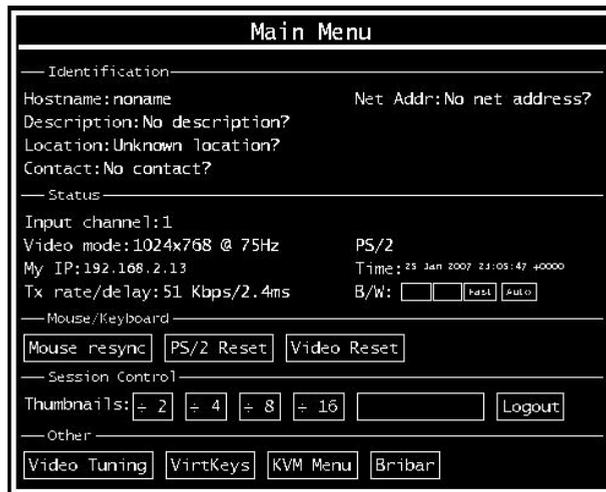
[1][A][S]: These flags show the state of the keyboard lights, NumLock, ShiftLock and ScrollLock respectively.

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.

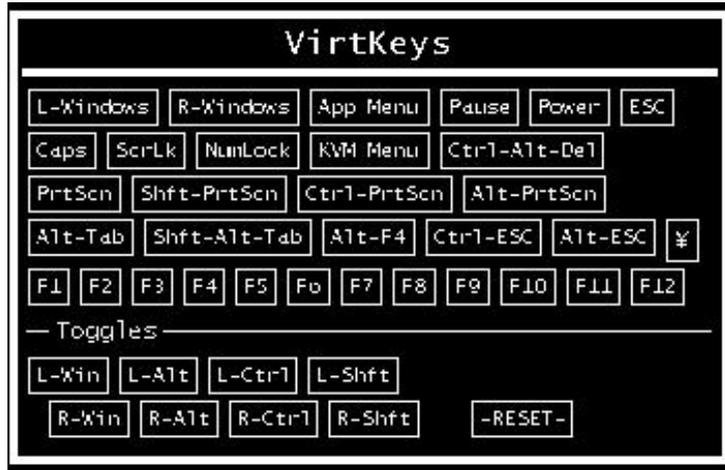
Here is a guide outlining various fields from the VNC Main Menu. Most of the functions operate immediately. Other functions require a response to a confirmation prompt first before performing the requested function.

- **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, wherein current 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 are 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 CABCONS1716I, 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



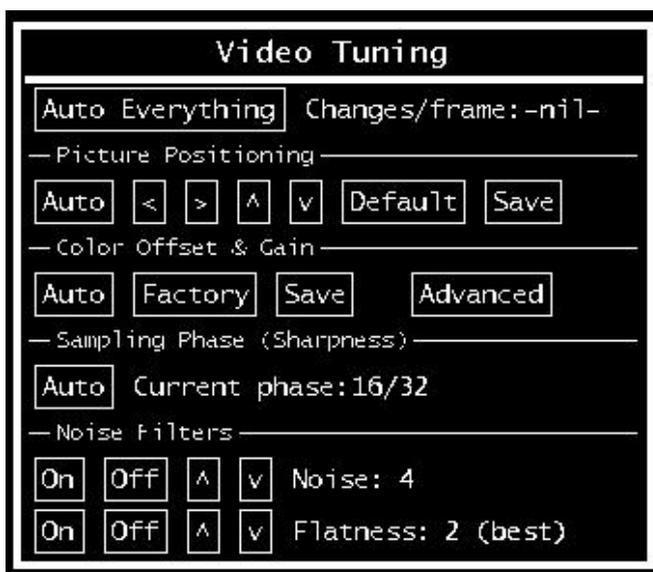
Clicking any button in the top half of the window simulates pressing and releasing the indicated key. In the bottom area of the screen, clicking will simulate the indicated Meta key being pressed. You may then click in the top part to send another key and release the Meta key at the same time. Alternatively, 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 when suitable, 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 VirtKeys Menu.

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 within approximately one minute.

If the system cannot find the test pattern on the screen, check that the pattern isn't scaled or covered up. (perform 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 CAB-CONS1716I 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.

Accessing KVM Features

Once you can access and configure the networking component of the Server Remote Control, you can use it to select and control the managed computers connected to it. This section describes how to add additional KVM switches to the master unit for greater flexibility, and how to use the on-screen display (OSD) system to manage your computers. Once you have established a VNC session, you can access the KVM features as though you were at a local console.

Cascade Configuration

You can connect a second level of KVMs to one or more of your Master Server Remote Control's PC x ports. The KVM switches connected to the Server Remote Control (the "Master switch") are known as Slaves. Once connected, the units will automatically configure themselves as either Masters or Slaves. You can only connect an equal or "smaller" KVM to the Master: a 16-port master Server Remote Control switch can have both 16-port and 8-port KVM slaves, an 8-port Master Server Remote Control switch can have 8-port and 4-port Slaves, and so on.

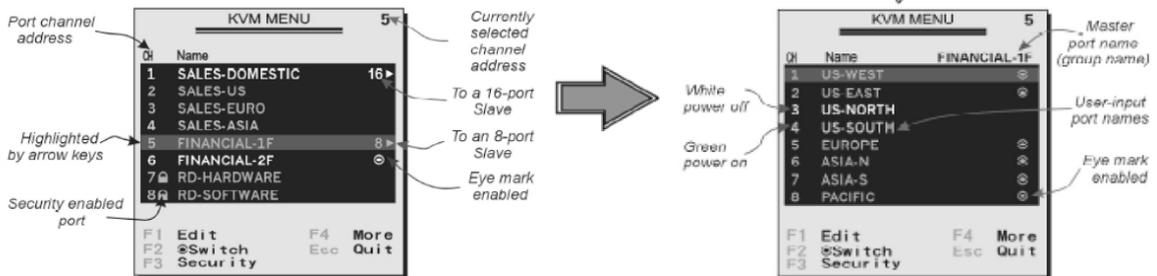
For example, the 16-port unit can support 136 computers, with 8 16-port Slave KVMs, each connected to 16 computers. The Slave KVMs must be connected to the PC 1~8 ports, not the PC A~H ports.

To cascade your KVMs, use a 3-in-1 PS/2 KVM cable to connect one of your Master switch's PC ports to the Slave switch's PC 1~8 ports. When turning on your cascaded switches, turn on the Slave switches prior to turning on the Master switch.

Please Note: When turning on your cascaded switches, turn on the Slave switches prior to turning on the Master switch.

OSD Operations

By hitting the left **<CTRL>** key twice within two seconds, you may see the 'Hotkey Menu' if it is enabled (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 (or channel address) of the currently selected computer is displayed in red in the top right of the screen.
- The device name is green if the device has power and is ready for selection or white if it has no power. The OSD menu automatically updates the color when it is activated
- Use the **<UP>** and **<DOWN>** arrow keys to highlight a computer and the **<ENTER>** key to select it.
- Press **<ESCAPE>** to exit the OSD menu and remove the OSD menu from the screen.
- A triangle mark on the right side of the screen indicates the port is cascaded to a Slave KVM; the number at the left of the triangle mark shows the number of ports the Slave has. With that port highlighted, press **<ENTER>** to bring up a screen listing the computers connected to that Slave. The name of the Slave KVM will be shown at the upper right corner of the OSD menu.
- An eye mark on the right side of the screen indicates that the computer has been selected to be monitored in Scan mode. You can switch this mark on and off using function key **<F2>**.
- Press **<ESCAPE>** to exit the OSD and to return to using the selected computer.
- The computer name is shown on the screen.

OSD Function Keys

You can use the function keys when the OSD menu is active.

The **Function key <F1>** edits the name of a managed computer or a Slave KVM. First, use the **<UP>** and **<DOWN>** arrow keys to highlight a channel then press **<F1>** followed by name entry.

Your name can be up to 14 characters long. Valid characters are **A to Z**, **0 to 9**, and the dash character. Lowercase letters are converted to uppercase. Press **<BACKSPACE>** to delete a letter one at a time. Nonvolatile memory stores all name entries until you change, even if the unit is powered down.

The **Function key <F2>** Marks a computer to be scanned by switching the eye mark on or off. First, use the **<UP>** and **<DOWN>** arrow keys to highlight the device, then press **<F2>** to switch its eye mark on or off. If Scan Type is **Ready PC + Eye** (see Function key **<F4>**), only the powered and eye-marked computers will be displayed in Scan mode.

The **Function key <F3>** Locks a device (a computer or a Slave) from unauthorized access. To lock a device, use the **<UP>** and **<DOWN>** arrow keys to highlight it, then press **<F3>**. Now, enter up to 4 characters (**A to Z**, **0 to 9**, **dash**) followed by **<ENTER>** as a new password. A Security enabled device is marked with a lock beside its channel 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>**. Enter the password and you can access the device. The device is automatically re-locked once you switch to another device. During Scan mode, OSD skips the security-enabled device.

The **Function key <F4>** will open a pop up window, displaying the functions described below. Most of them are marked with a triangle indicating there are options from which to choose. Using the **<UP>** and **<DOWN>** arrow keys, select the function and press **<ENTER>**.

Available options will be shown in the middle of the screen. To select an option, use the **<UP>** and **<DOWN>** arrow keys then press **<ENTER>** to select the options. You can press **<ESCAPE>** to exit at any time.

Auto Scan: In this mode, the KVM 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. 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: Scans through powered computers using keyboard control. Scan Type (<F4>: **More\Scan Type**) determines if scanned computers must also be eye mark selected. Press the up arrow key to select the previous computer and the down arrow key to select the next computer. Press any other key to abort the Manual Scan mode.

Audio Stick: A multimedia module can be LINKed to the back of each KVM 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. Off mode 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. (Note: This is an optional feature requiring that a separate device be connected to the master switch.)

Scan Type:

Ready PC + Eye: In Scan mode, scans through only powered computers that are eyemarked selected.

Ready PC: In Scan mode, scans through all powered 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 Scan Rate setting is stored in non-volatile memory.

Keyboard Speed: The KVM offers a keyboard typematic setting that overrides the typematic settings in the BIOS and Windows operating system. Available speed options are Low, Middle, Fast and Faster as 10, 15, 20 and 30 characters/sec respectively. The Keyboard Speed setting is retained in non-volatile memory.

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, by pressing the left **<CTRL>** key twice. The nonvolatile memory stores the Hotkey Menu setting.

CH Display:

Auto Off: After you select a computer, the channel address and name of the computer will appear on the screen for 3 seconds then disappear automatically.

Always On: The channel address and name of a selected computer and/or OSD status is/are displayed on the screen all the time. The non-volatile memory stores the CH Display setting.

Position: You can choose where the selected computer name and/or OSD status is displayed on your screen during operation. The actual display position shifts due to different VGA resolutions: the higher the resolution the higher the display position. The non-volatile memory stores the Position setting.

UL as Upper Left **UR** as Upper Right

LL as Lower Left **LR** as Lower Right

MI as Middle

ESC: To exit the OSD, press the **<ESCAPE>** key

Hot Key Commands

A hot key command is a short keyboard sequence to select a computer, activate a computer scan, etc. A hot-key sequence starts with two Left Control keystrokes followed by one or two more keystrokes.

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. **Left <Ctrl>** refers to the <CTRL> key located at the left side of the keyboard.

1~8/A~H refer to the number keys 1 to 8 at the upper row of the keyboard (Do not use the keypad at the right of the keyboard) and character keys A to H (case insensitive).

Selecting a Computer:

To select a computer by hot-key command, you need to know the device's channel address as determined by the KVM connection. For a computer connected to the Master switch, the address is represented by the PC port number (1~8 or A~H). For example, to access the PC plugged into port **7** of the Master KVM switch, type: **left <Ctrl> + left <Ctrl> + 7**.

For a computer connected to a Slave KVM, you need to know the channel address of the Slave unit (1~8) and then the channel address of the device (1~8 or A~H). (Please note that only the Master's PC 1 to PC 8 ports can be connected to a Slave.) For example, to access the computer plugged into port **C** of a Slave KVM Switch that is plugged into Port 6 of the Master switch, type: **left <Ctrl> + left <Ctrl> + 6 + C**

Auto Scan:

Auto Scan automatically scans through powered computers at a fixed interval. To activate, key in **left Ctrl + left Ctrl + F1**.

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. The length of the Auto Scan interval (Scan Rate) is adjustable (see Scan Rate on the following page). To abort the Auto Scan mode, press the left Ctrl key twice.

Manual Scan:

Manual Scan enables you to manually switch back and forth between powered computers: **left Ctrl + left Ctrl + F2**. Press the up or down arrow to select the previous or next computer in sequence. Press any other key to abort the Manual Scan.

NOTE: The Scan Type setting will determine whether computers must be eye-marked to be included in the scan.

Scan Rate:

Scan Rate sets the duration between switching to the next computer in Auto Scan mode: **left <Ctrl> + left <Ctrl> + F3**

The unit switches between scan intervals of **3, 8, 15** and **30** seconds.

Keyboard Typematic Rate:

You can adjust the keyboard typematic rate (given in characters/sec). This setting overrides the keyboard typematic rate of your BIOS and any operating system. To activate, key in **left <Ctrl> + left <Ctrl> + F4**, following which the unit will switch between rates of 10, 15, 20 and 30 characters/sec.

Audio Stick:

A multimedia module can be LINKed to the back of the master KVM 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. To activate, key in **left Ctrl + left Ctrl + F5**.

Please note that this is an optional feature requiring that a separate device be connected to the master switch.

Changing Your Configuration

After the initial power up, any device (either a KVM or a PC) can be added or removed from any PC x port on the KVM without having to power down the Master KVM Switch.

Make sure that devices are turned off before connecting them to the Master KVM switch. Please note that after changing your configuration, the OSD will automatically update to reflect the new configuration.

Optimizing video performance

Choose the best video mode

We recommend using a display resolution of 1024x768 @60Hz refresh rate, as facilitates fitting multiple windows on your remote desktop. Higher refresh rates put unnecessary stress on the quality provided by the video card, and do not provide any additional information or benefit.

Noisy video cards

A digital KVM works by converting the analog video signals emitted by your video card into digital data. If there is noise on that signal, then it must also be digitized and sent over the network. Quality video cards, in our experience, offer better performance simply because they don't add analog noise.

- Some external KVM switches generate video noise as well. Try to keep cables short, in order to reduce this effect.
- Enable the **Noise Filter** option (in the Video Tuning menu) to mitigate noise issues.

Network performance

The CABCONS1716I will always send as much data as it can, given what's happening on the screen and the actual network performance. When nothing is changing on the video screen, zero bytes are sent over the network. If the whole screen is changing, then the unit will send as much data as can be supported by your network connection.

- Network latency, which is the total time it takes for a packet to get to the CABCONS1716I and come back, has the biggest impact on perceived performance and usability.
- Network bandwidth has a lesser effect, particularly when just moving the mouse around. Only a few bytes need to be sent when the mouse is moving (and nothing else is changing on the screen), but the round-trip-time limits the hand-eye coordination of the user if it is too great. Both actual bandwidth and measured network latency are shown in the Main Menu.

Using the Advanced Video Tuning feature

The **Advanced Video Tuning menu** allows you to adjust the qualities of the video in your VNC sessions, and can be accessed by clicking the Advanced button on the Video Tuning VNC menu. While many users will probably allow the CABCONS1716I to automatically configure the video properties, you can use this menu to exercise a great deal of control over the settings if required.

The **Presets** section contains up to sixteen different settings, plus the factory setting. If a number is highlighted, then that preset has been programmed with valid settings and may be used. Please note that the Factory preset is always available and can be restored by simply clicking on the appropriate button.

To save settings to a preset, click on the **Save->Preset** button in the **Actions** pane. The preset buttons will highlight. Click the desired preset button to save the values. Note that any previous settings assigned to that button will be lost. If you do not wish to save the presets after clicking the **Save->Preset** button, click the **Save->Preset** button a second time and the save function will be canceled.

The section of the screen marked **Current Values** indicates the various video parameters that can be adjusted. For each parameter, there are a series of buttons: [, <<, -, **Auto**, +, >,].

- The '[' and ']' buttons set the parameter to its smallest or largest values, respectively.
- The '<<' and '>>' buttons decrease or increase the parameter by a large amount. In the case of phase, this is 4 units. For all others, this

is 10 units.

- The '-' and '+' buttons decrease or increase the parameter by one unit.
- The middle button sets the parameter to the middle value. The text of the middle button also indicates which parameter is being controlled. Note that in the case of phase, the middle button invokes the auto-phase algorithm.

The **Performance** section of the screen gives an indication of the quality of the video.

Changes/frame is the average number of tiles that change for each frame sampled by the hardware. Flatness is an indication of what percentage of the screen contains tiles that are comprised of only one color.

The **Regrab Screen** button in the **Actions** section causes the screen to be re-captured. When making small changes to the video parameters, sometimes these changes are not reflected in the displayed screen immediately, particularly if the noise filter is enabled. Press this button to see the immediate effect of the changes.

Use the **Show Diffs** button to learn which parts of the screen are being sent over the Internet. When you click this button, the screen is cleared to a medium grey color. All blocks that are sent from that point on will show up on the screen as they are sent. Click the button again to reset the screen to grey. To return to normal operation, click the **Regrab** button. It is very easy to visually identify the effect noise has on signal processing, using this feature.

The **Auto Offset & Gain** button in the **Actions** section invokes the automatic algorithm for setting the video parameters. The algorithm requires the factory calibration test pattern to be correctly displayed on the screen.

Using the Modem Feature

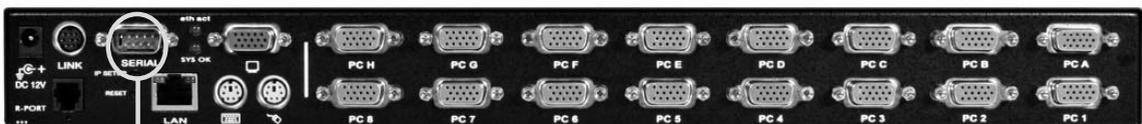
The Modem feature allows the CABCONS1716I to act as an Internet connection server for increased security and flexibility in connecting with the host computer.

Unlike the TCP/IP connection used with the standard Web configuration and VNC clients, the modem creates a one-to-one connection between the CABCONS1716I and the computer you are using, bypassing the public Internet completely.

NOTE: This feature requires both an external modem (most standard connection protocols are supported) and a dedicated phone line that can be connected to the modem for external access. While it is possible to use the modem feature through some PBX systems, this increases the complexity and reduces the performance of the connection. For clarity, the instructions presented here assume that the modem is connected to a typical POTS (Plain Old Telephone System) line that is not routed through a phone management system or shared with other devices.

If you wish to use this feature through a PBX system, it may require some experimentation and additional support from your telecom services provider, and is not supported by StarTech.com.

Connecting a Modem



Modem
Connection

The CABCONS1716I will work with virtually any Hayes-compatible modem capable of recognizing the standard AT command set. Some modem manufacturers offer “enterprise” grade modem products that include technology to improve the stability of connections; whether this type of product would be beneficial to your application depends on whether you consider the modem connection to be mission-critical, the quality of your telecom infrastructure, and your budget for implementing this solution. The model of modem attached is essentially transparent to the CAB-

CONS1716I.

It is important to note that modems that offer “56K” (or 56,000 bps) connections often achieve connection speeds that are far lower than their maximum capabilities.

Given the limitations of telecom infrastructure (many locations have yet to implement fully digital switching technology, and still rely on older analog technology for some segments), the maximum “upstream” transfer rate is limited to a maximum of 33,600 bps between two modems; the “downstream” rate is often within a similar range for a typical connection. Therefore, speeds below 56,000 bps do not indicate a problem with the modem or the CABCONS1716I, but simply reflect the line conditions at the time the connection is made.

The Serial port can be used for serial port configuration when the modem is connected. It requires the use of a null modem serial cable.

Place the modem near the CABCONS1716I and an available telephone jack. Connect the modem to the telephone jack, data cable, and power source according to the instructions in its documentation. The opposite end of the modem’s data cable should be a DB9 female serial connection. Connect that end of the cable to the Serial connection on the rear panel of the CABCONS1716I.

Modem configuration

Although most connections will work appropriately with the default settings on CABCONS1716I, manual changes can be made. To do so:

Login to the Web interface as Admin. Click Modem, listed on the left side of the main page. You will then be presented with the Modem Option menu (see above). Make the following changes to enable and configure the modem connection:

1. Enable modem connections (PPP) via serial port/modem: select **Enabled**.
2. Baud rate to use (affects connection between us and the modem only): select **115200**.
3. Init string: leave as **ATE0S0=1&K3**.

The baud rate dictates the connection speed between the CABCONS1716I's serial port and the modem, and does not affect the connection speed between the local and remote modems, as they will negotiate their own connection speed when a connection is made. It is highly recommended that this setting be left at the default for best performance.

The initialization ("init") string is the command (using the standardized Hayes AT command set) that the CABCONS1716I will send to the modem to activate it. The included string should work with the majority of modems and configures the following connection properties: **answer incoming calls on the first ring, enable hardware flow control, and lock the connection speed.**

Your modem's documentation will describe other potential init strings in greater detail, that you can use to alter the connection properties. For instance, you could commit the settings to the modem's non-volatile memory (NVRAM) or allow the modem to adjust the connection speed for greater stability (and so on).

To simplify the troubleshooting process, you may wish to test the connection with the default init string first, prior to making changes specific to your modem model or situation.

Click the **Commit** button to save your changes and activate the modem feature with the specified settings.

Configuring the Remote Connection

This section describes how to configure a typical Windows dial-up session to access the modem connection on the CABCONS1716I. The instructions here relate to a Windows XP configuration; other versions of Windows are similar.

1. Open **My Network Places** from the desktop or the **Start** menu.
2. Click **View network connections**.
3. Click **Create a new connection** under **Network Tasks**.
4. The New Connection Wizard window will open. Click **Next**.
5. Select **Connect to the Internet** and click **Next**.
6. Select **Set up my connection manually** and click **Next**.

7. Select **Connect using a dial-up modem**, then click **Next**.
 8. In the space provided under ISP Name, type an appropriate name of your choosing for the connection. Click **Next**.
 9. In the space provided under **Phone Number** enter the phone number for the line to which the CABCONS1716I's modem is connected. You may need to add the area code, country code, or other digits needed to access the outside line as appropriate. When finished, click **Next**.
 10. Make your choice from **Anyone's use** or **My use only** and click **Next**.
 11. Beside **User name**, enter the user name of any valid user created using the Web interface of the CABCONS1716I. Beside **Password** and **Confirm password**, enter the password that corresponds with the username entered.
 12. This screen also includes three checkboxes. **Uncheck all 3 checkboxes**.
 13. Click **Next**.
 14. You may select to add a shortcut to the desktop for this connection. **Click Finish**.
- PPP (Point-to-Point Protocol) must be used; no other authentication methods are supported.
 - TCP/IP must be installed/enabled on the computer making the connection, and must be used for the dial-up connection.
 - The connection must be configured to obtain a dynamic IP address.
 - The user name/password must match a user currently configured on the CABCONS1716I.
 - For best performance and to simplify the troubleshooting process, firewall software should not be used with the dial-up connection.

Accessing the Web Interface

Once a dial-up connection has been established, you can access the Web interface or start a VNC session using the following IP address:

<https://99.99.99.99>

You can now login to the Web interface (and/or VNC session) normally. Note that the remote machine (the one you dialed from) is automatically assigned the IP address 99.99.99.100 for the PPP session. This, and the IP address of the CABCONS1716I, cannot be modified. The following TCP/IP port numbers are assigned for a PPP connection, regardless of the settings configured in the Web interface for the LAN or WAN ports:

HTTPS: 443

VNC (clear-text): 5900

VNC (SSL secured): 15900

SSH: 22

Performance Notes

- All images over the PPP connection will be grayscale to conserve bandwidth. If other users are connected while a PPP session is active, their screens will be in grayscale as well. When PPP is inactive, color is automatically re-enabled.
- Some areas of the screen may not be updated as frequently as others, and animations or other auto-updating areas of the screen may appear out-of-focus or “blocky” as a result. Since the area around the mouse pointer is refreshed most frequently, hold the pointer over an area to improve its clarity.
- It may be beneficial to minimize any unnecessary icons, backgrounds, or other clutter on the host computer’s desktop to make the dial-up connection as efficient as possible.
- If you need to configure the device over a serial connection while the modem option is enabled, connect a serial cable and begin a terminal session following the instructions under **Terminal Configuration Using a Serial Cable** in this manual. Once connected, you will see the following message:

Expecting a modem, if human, type admin password (Or start PPP)

Type the password for user admin and press **Enter**. The password will not appear on the screen. The configuration menu will appear. Make the changes you wish or press **q** and **Enter** to exit and leave the modem connection active.

Modem Troubleshooting Guide

The following messages will appear in the system log on the Status screen in the Web interface and may help to diagnose problems with the modem configuration.

Starting PPP (for auth) on port...

Modem is connecting and the PPP login process is starting.

Modem hang up. Resetting

The connection has been closed or terminated unexpectedly.

Timeout during login process. Giving up

The PPP client connecting over the modem has waited too long to complete the authentication process or supplied an invalid user name and/or password.

Modem init chat script failed

The modem did not respond to the initialization string from the CAB-CONS1716I. You may need to change the init string or verify the cabling and modem status.

Modem init okay

The modem has responded appropriately to the init string.

Saw PPP startup from client

A PPP authentication has occurred and a session has started.

Phone line rings

An incoming call has been detected by the modem.

Modem answers: xxxxxxxxxx

The connection speed and protocol used for a connection, as reported by the modem. The exact contents of the message will vary depending on the modem make and model. Using Optional Serial Remote Control (R-Port) Modules

Serial Remote Control operation

The CABCONS1716I offers a unique way to expand the functionality of the base product. Using the integrated R-Port on the rear panel, you can manage up to 16 serial devices using a specialized daisy-chain technology. The CABCONS1716I includes integrated control functionality that

allows you to monitor and configure serial devices using the interactive Web interface. To minimize space and infrastructure requirements, the R-Port modules use a single cable to carry both power and the data signal. All configuration settings are stored separately in each attached device in non-volatile memory so that they will not be lost in the event of a power outage or disconnection.

Connecting Serial Remote Control Modules to the CABCONS1716I

The cable for each serial device is similar to a phone cable and uses an RJ-14 connector. For the first module, connect the cable (provided) to the R-Port on the rear panel of the CABCONS1716I. Connect the opposite end to the DATA OUT (or similar) port on the Serial Remote Control unit. Note that some devices may use an integrated cable, so you will not need to make a separate connection on the serial device. Once you have added the first serial device to the CABCONS1716I, you can connect additional modules to the DATA IN (or similar) port on the previous module in the chain.

Once the cabling is attached, the module becomes active after a 15 second initialization period. For specific information regarding cabling and status indicators for a specific serial console, refer to the instructions that came with the product.

Configuring/Viewing Serial Remote Control Modules through the Web Interface

Once you have one or more R-Port serial devices connected, you will be able to configure and manage them through the Web interface. You may need to modify the default settings on CABCONS1716I to match your various R-Port modules' default configuration.

Consult the documentation that came with your R-Port module to determine if you need to modify the default settings to complete the installation. To be able to configure your RPort modules, you must be logged in as **admin**. Other users will be able to view which modules are active, but cannot configure them.

Once you are logged in, choose the **Admin/Setup** option from the menu at the top of the Home screen in the Web interface. Click **External Serial consoles setup and control**.

You will be presented with the **Serial Consoles Attached** menu, and a

table with the following headings:

#: You can assign a value (1 ~ 99) to each attached serial remote control module. This does not affect the configuration or operation of the device in any way, but is simply a means to sort this list for ease of management.

Name/Description: An identifier for the R-Port module. Like the number assignment, it is for ease of administration only.

Baud (bps): This is the communication speed for the device, and the setting here must match the setting on the module itself. All common baud rates between 300 and 115,200bps are supported.

Mode: Sets the character framing scheme that the CABCONS1716I will use with the R-Port module. You can choose from the following selections:

8N1: Eight bits, no parity, one stop bit (default and most common)

7N1/7O1/7E1/7M1/7S1: Seven bits, (none/odd/even/mark/space) parity, one stop bit

8N1/8O1/8E1/8M1/8S1: Eight bits, (none/odd/even/mark/space) parity, one stop bit

8N2: Eight bits, no parity, two stop bits

Force DCD: Forces the Carrier Detect signal to be active at all times. Normally, DCD becomes active when a new user connects and is dropped when the last user disconnects (a response that is similar to many modems). When active, the device will logout and reset itself if the carrier signal is lost, increasing security. Note that this may not work with all devices and could impair proper operation in some circumstances. The default setting is off.

Console Log: Clicking this link will open a separate Web page that will display the last 200 characters committed to that device's console log. Note that existing data is overwritten automatically when the 200 character limit is reached.

You can simultaneously make any required changes on this menu, before applying your changes. Once complete, click **Commit changes** to apply the new settings. Click **Refresh** at any time to see an updated list of attached R-Port modules.

Advanced Configuration Using the Integrated SSH Shell

In most cases, configuring the CABCONS1716I to the same settings as the R-Port devices you are connecting should allow the devices to work with a minimum amount of configuration. However, you can also change the default settings on each R-Port device to fit your preferences and the needs of your application.

If you click the **Connect...** button next to the device you want to configure, two new windows will appear. The smaller of the two is a login screen; the other is an SSH terminal window. Click the login window and sign in as admin (using the same password as the Web interface) to activate the terminal window. You will see a welcome banner similar to the following:

```
Baud rate: 115200 bps, 8N1
Connected to #1: (none)... (Press Ctrl-Shift-_ for menu).
```

You are now connected to the R-Port module in a live terminal session. Commands you type will be echoed on the terminal screen. The module also offers a simple menu system that allows you to change configuration settings (similar to the function of the menus in a terminal software package). Press **[Ctrl] - [Shift] - [_]** (underscore) on the keyboard to access the menu. It will be similar to the following:

```
RS-232 Menu (#1: (none), 115200 bps, 8N1)
Q - Disconnect
# - Send break
H - Hangup line (drop DCD)
E - Send Ctrl-Shift- _
L - Low log entries (line buffer)
l - Show last 10 log entries
other - Return to connection
Press key ->
```

To execute the desired command, press the corresponding key on the keyboard. You can also execute the command and avoid the menu by pressing the **[Ctrl] - [Shift] - [_]** key combination quickly and pressing the letter of the command. To quit the menu, press **[Q]** on the keyboard when

the menu is active. These commands are not sent to the device you are managing and relate to the RPORT module itself.

Remote Login via SSH

You can also use a standard SSH client to access the R-Port options if you wish to avoid using the Java-based SSH client in the Web interface. Simply use your SSH client (several freeware packages are available for download, along with commercial applications) and connect to the IP address of the CABCONS1716I using port 22 (default).

Log in to the SSH session as admin using the same password as the Web interface. At the command prompt type connect x (where x is the number of the R-Port devices you wish to manage). Alternatively, you can enter the command connect -l to see a list of active devices.

Operating Notes:

- If the power supply to the R-Port modules you have connected becomes faulty (short, overload) then the R-Port LED on the front panel of the CABCONS1716I will show red.
- Under normal operations, this light should remain green. The R-Port connector on the rear panel also has an LED that mirrors the status of the light on the front panel.
- Hardware handshaking (CTS/RTS) is required for speeds exceeding 9600 bps. It is enabled by default on the CABCONS1716I, but may need to be enabled on the other end of the connection. For Unix systems, the command is:

stty -crtcts < /dev/[serial port]

- A maximum of four users may simultaneously login to the same module. All users may type commands at any time, and all users will see the same output. Note the following:
 - *All users have equal access to all channels.*
 - *A maximum of 16 R-Port modules may be connected at any one time.*
 - *You can plug-in or unplug any R-Port module at any time.*

When reconnected, it will automatically become available after a 15 second initialization period. Any log entries will be retained by the R-Port module while deactivated, but will not be available to users until it is re-initialized.

About Security Certificate Warnings

What is a security certificate?

Sites that employ secure TCP/IP (Internet) connections include a certificate that confirms that users are connecting to a legitimate site and are not being redirected without their knowledge. Certificates are issued by trusted third parties called Certificate Authorities (CAs) and contain essential details about a site that must match the information supplied to your Web browser.

Why do I receive a warning when I access the login screen on the CABCONS1716I?

As it redirects you to a secure (SSL) session by default, the login screen may generate a warning from your Web browser or the VNC Java client for two different reasons. First, the CA that has issued the certificate on StarTech.com's behalf may not yet be recognized as a trusted source by the computer you are using to access the CABCONS1716I. Second, since the unit could be configured in a number different ways, it is impossible to supply a generic certificate that will match your exact network settings.

Is my data safe?

Yes. The security certificate does not affect encryption effectiveness in any way, nor does it make the CABCONS1716I any more vulnerable to outside attacks.

Can I prevent the warning from occurring?

Yes. You have two options that may prevent the warning from occurring. First, if the Web browser you are using offers the option to ignore the warning for future visits, the browser will no longer generate a warning if that option is selected. Second, if you install the certificate from the CABCONS1716I onto the host computer (see below) and if the unit is configured with a domain name ending in .com, .net, .org, .gov, .edu, .us, .ca, .uk, .jp, or .tw (i.e. remotecontrol.mydomain.net) then the warning should no longer occur.

Installing the new certificate...

The following instructions detail how to install the certificate from the CABCONS1716I onto your local computer (in this case, when using Internet Explorer with Windows XP):

1. Open your Web browser and go to the CABCONS1716I login screen. Click the Update security certificate link.
2. When prompted, choose Open.
3. A Window will appear that offers information about the certificate. Click Install Certificate.
4. The Certificate Import Wizard will appear. Select Automatically select the certificate store... (default) and click Next. When the next window appears, click Finish.
5. A confirmation dialog will appear asking you if you wish to install the certificate. Click **Yes**.
6. A message should appear saying the import was successful. Click **OK**.

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.

After resync, the mouse pointers are still not aligned

Use the video adjust menu to position your video image exactly where required. 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 CABCONS1716I 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.

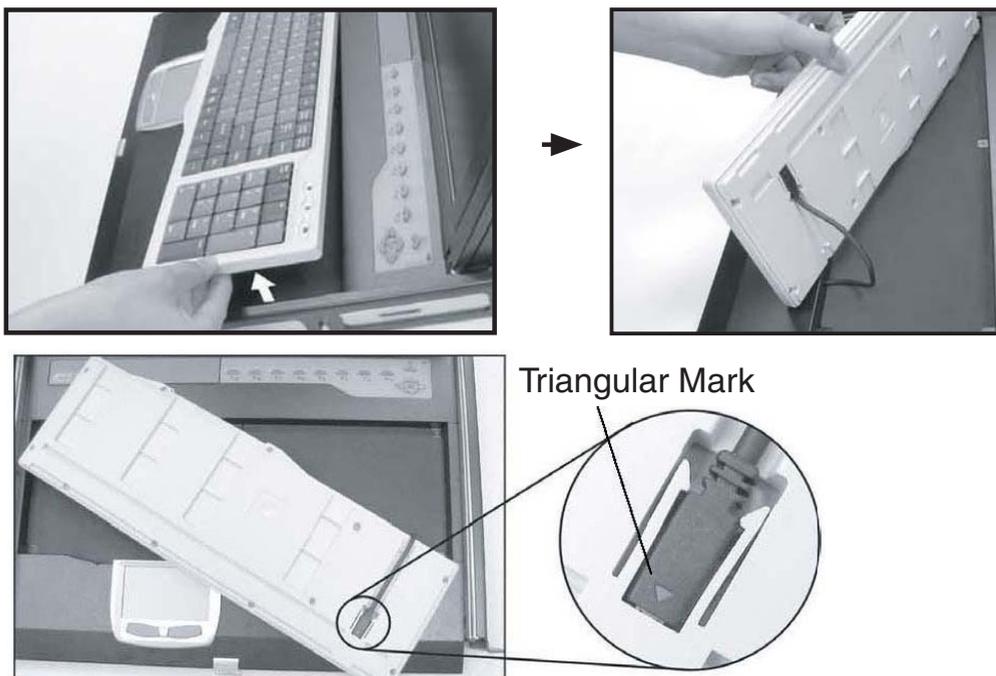
Mouse performance is erratic when using the GNOME or KDE desktop in a Linux X-Window environment

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)

Keyboard Replacement

The keyboard is replaceable, in the event of language changes or maintenance. To replace the key-board, tilt it up, locate the mini-USB cable underneath the keyboard and unplug it gently. While installing the replacement keyboard, please ensure that you extend just enough of the cable to keep the keyboard flat inside the tray.



Please note: There is a round hole under the drawer, which can be used to pass one finger through allowing for easier removal of the keyboard (pushing upwards).

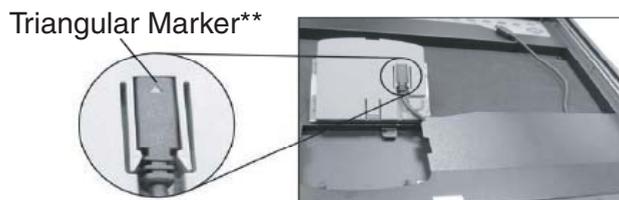
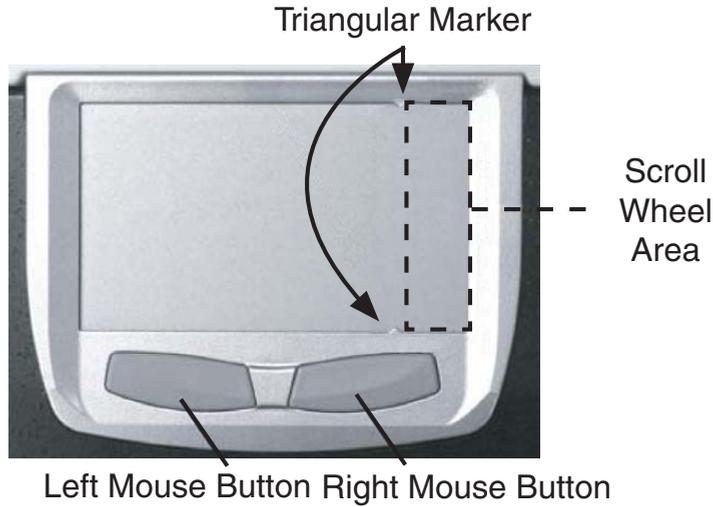
Please note: The triangular mark on the mini USB connector must face outwards.

Touchpad Replacement

The built-on Touchpad offers “wheel mouse” functionality. The area of the Touch Pad to the right side of the two small triangular marks is the simulated “wheel” as shown below:

To remove the Touch Pad, press the tab underneath it upward to release

the latch, then slide it outwards until the Touch Pad can be lifted up clear from the notches, as shown in the figure below (right side). The Touchpad is attached by a piece of mini-USB cable. To install the Touchpad, extend just enough mini-USB cable and slide the Touch Pad all the way in till you hear a click sound as it is locked in position.



Specifications

Console Connectors	VGA (1), PS/2 Mouse (1), PS/2 Keyboard (1)
Display Colors	16.2M (8 bits)
Host Computer Connectors	HD-15 female (16), supports either PS/2 or USB clients based on cable used
Input Signal	RGB analog, H/V separate
LCD Size	17" TFT
Maximum Local Resolution	1280 x 1024
Plug and Play VESA	VESA DDC 1/2B
Power Management	VESA DPMS compliant
Maximum Cascaded Computers	136
Maximum Number of Computers	16
Maximum Number of Users	1 Local, 4 Remote
On-Screen Display	Yes

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 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. StarTech.com makes it easy to complete almost any IT or A/V solution. Find out for yourself why our products lead the industry in performance, support, and value.