

4 Port VGA USB IP KVM Switch with Virtual Media

SV441DUSBI



DE: Bedienungsanleitung - de.startech.com

FR: Guide de l'utilisateur - fr.startech.com

ES: Guía del usuario - es.startech.com

IT: Guida per l'uso - it.startech.com

NL: Gebruiksaanwijzing - nl.startech.com

PT: Guia do usuário - pt.startech.com

For the most up-to-date information, please visit: www.startech.com

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
Package Contents.....	1
Hardware Guide	2
Front Panel	2
Installation.....	4
Device Connection.....	4
Initial Power-Up.....	5
Operation	6
Initial IP-OSD Setting.....	6
Mouse Setting.....	9
KVM Switch OSD Operation.....	10
Data-Transfer Rule.....	11
USB Port Rule.....	12
Using the Web Interface	13
The Login Screen.....	13
Web Interface Introduction.....	14
Main Menu Selections	15
Network Configuration	19
User Accounts	20
System Identification.....	21
Security.....	21
Compatibility.....	22
SNMP	22
RADIUS.....	22

Modem.....	23
Serial Ports.....	23
Time / Date	23
Firmware.....	23
Purchase Options.....	24
Status.....	24
Port Numbers.....	25
Help Menu.....	25
Site Map Menu	25
Copyright Menu.....	25
Using the Terminal Interface via Serial Port.....	25
Accessing the VNC Interface	26
Web Interface.....	26
Native VNC Client.....	27
SSH Tunnel (with Native VNC client)	28
Using the VNC Menu	28
Bribar Feature	28
Main Menu.....	29
VirtKeys Menu	31
Video Tuning menu	32
Accessing KVM Features	33
OSD Operations.....	34
OSD Function Keys.....	34
Hot Key Commands	36
Changing Your Configuration	37
Optimizing video performance.....	37
Choose the best video mode.....	37
Noisy video cards	37
Network performance	37
Using the Advanced Video Tuning Feature	38

Using the Modem feature.....	39
Background.....	39
Connecting a Modem.....	39
Modem configuration.....	40
Configuring the Remote Connection	41
Accessing the Web Interface	42
Modem Troubleshooting Guide	43
Serial Remote Control operation.....	43
Background.....	43
Connecting Serial Remote Control Modules.....	44
Using the Web Interface.....	44
Advanced Configuration Using the Integrated SSH Shell	45
Remote Login via SSH.....	46
Operating Notes.....	46
About Security Certificate Warnings.....	47
Installing the New Certificate.....	47
Troubleshooting.....	48
Specifications.....	49
General Specifications	49
Supported Protocols.....	50
Technical Support.....	51
Warranty Information.....	51

Introduction

The SV441DUSBI 4 Port USB VGA IP KVM Switch with Virtual Media allows for secure local and remote control of up to 4 computers over a LAN or the Internet. Featuring 2 additional USB ports for peripheral sharing (USB storage, CD ROM, etc.), allowing file transfers and disk emulation for remote application and OS installs.

The IP KVM Switch enables BIOS level control and full boot process interaction, and includes several security features (SSH, SSL, RADIUS and a configurable firewall) to keep your network safe.

This IP KVM can interact with virtually any device that uses an RS-232 serial terminal (routers, switches, PDUs, etc.), using the RPORT Module (sold separately). While the 1U rack-mountable metal chassis makes installation into a rack easy with the 1110EXTRACK.

Features

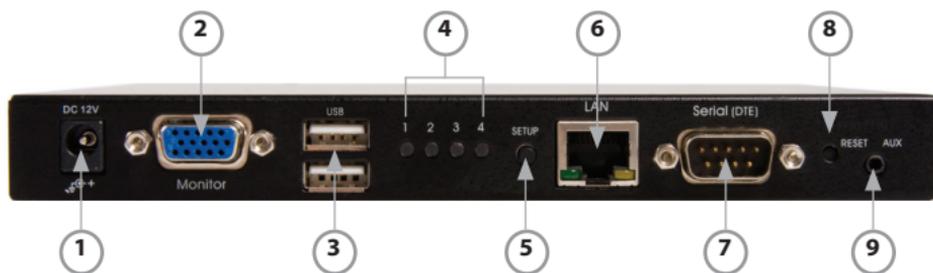
- Remote, BIOS level access to all connected systems
- Works with PC, Mac, Linux and Sun Systems
- Supports DHCP or manual IP configuration
- User ID and SSL password secure web console
- Supports 32 user accounts with SSL encrypted session and web communication data
- Integrated Web Server for browser-based configuration and administration

Package Contents

- 1 x SV441DUSBI
- 1 x User's Manual
- 4 x KVM Cables
- 1 x Package of screws
- 1 x Power Adapter
- 1 x Power Cord

Hardware Guide

Front Panel

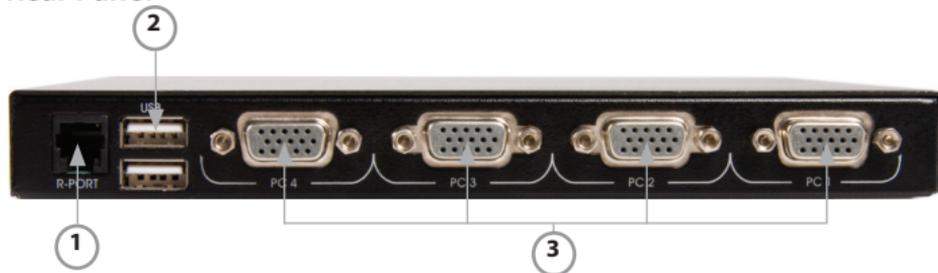


- 1. Power Supply**
Connects to a DC 12V power adapter.
- 2. HDB15 Connector**
Connect to the console monitor.
- 3. USB Type A Connectors**
Connect to the console keyboard and mouse ports.
- 4. Port LED Indicator**
Displays the status of connected PCs (for more specific instructions, see the table below).
- 5. Setup Button**
Press this button to bring up the IP-OSD menu.
- 6. RJ-45 Connector**
Connects to the LAN.
- 7. RS-232 Connector**
Connects to a PC for initial setup.
- 8. Reset Button**
This dual-function button selects Power Reset or Restore Factory Defaults.
- 9. Auxiliary Input Link**
Reserved for multimedia module.

LED Color	Meaning
Green	Connected to a PC that is powered on.
Red	Port selected.
Blue	Data-transfer function is enabled.

LED Color	Meaning
Green + Blue (Light Blue)	Connected to a PC that is powered on and possesses the data-transfer function.
Red + Blue (Light Purple)	The selected port possesses the data-transfer function.
Red + Green (Yellow)	The PC that is powered on is selected.
Red + Green + Blue (White)	The selected and powered on PC possesses the data-transfer function.

Rear Panel



- 1. R-Port**
For serial device management with Serial Supervisor.
- 2. USB Type A Connectors**
Two additional ports for any USB devices (e.g. memory, printer, etc.).
- 3. HDB15 Connectors**
Connect to 4 servers (or PCs)

Installation

Device Connection

1. Connect the USB keyboard, mouse, and monitor to the console connectors on the SV441DUSBI.



2. Connect a Cat5 cable to the LAN port of the SV441DUSBI.



3. Power up the monitor and the SV441DUSBI. The IP-OSD menu should come up automatically. Follow the on-screen instructions to finish the initial setup.



Initial Power-Up

You must power up the SV441DUSBI with a keyboard, mouse, and monitor connected before turning on any other devices.

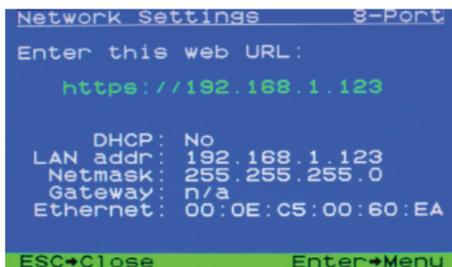
Ensure that the devices you are connecting are powered off before connecting them to the unit.

Operation

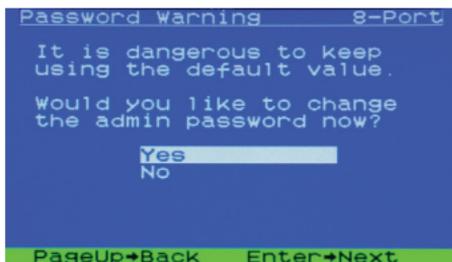
Initial IP-OSD Setting

Power on the monitor and the SV441DUSBI. The IP-OSD menu will automatically appear. Follow the on-screen instructions to complete the initial setup.

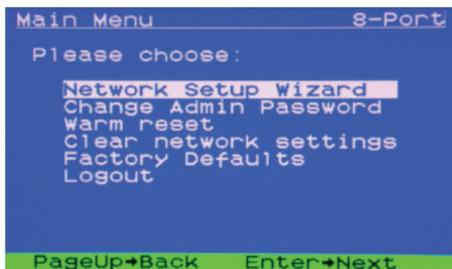
Press the **Enter** key to enter the Advanced Settings Menu. Once the desired settings have been achieved, press **ESC** to close the Menu.



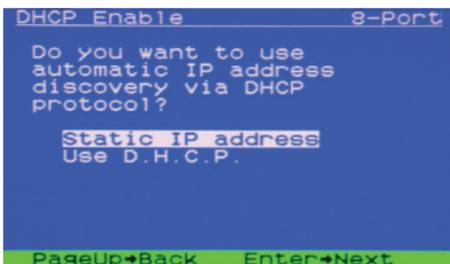
It is recommended that you change the password immediately and make a note of it.



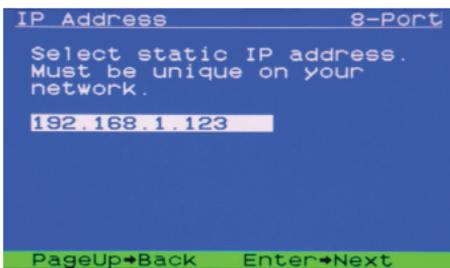
Press **Enter** to go to the next menu.



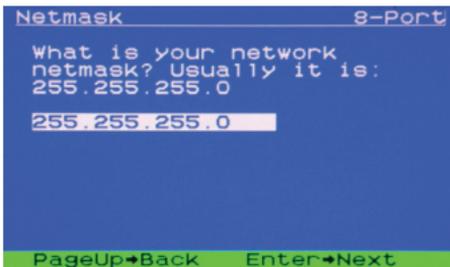
The IP KVM can have its IP address assigned dynamically, or it can be given a fixed IP address. If you are unaware of the IP address, obtain it from the network administrator.



Press **Enter** to go to the next menu.



Enter the **Netmask** (Consult your network administrator if necessary).



Enter the **Gateway** (Consult your network administrator if necessary).



Mouse Setting

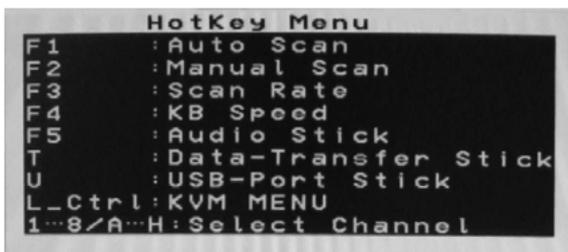
Many operating systems offer a feature called mouse acceleration that allows the user to adjust the responsiveness of the cursor on the screen to the physical movements of the mouse. While this is usually a beneficial interface enhancement, it can interfere with the operation of the unit and should be disabled on the managed computers before a remote session is attempted. Follow the instructions below to disable mouse acceleration for the operating system installed on each managed computer.



1. Open the **Mouse Properties** application located in the Control Panel.
2. Under the **Motion** heading, center the arrow used to modify the pointer speed.
3. Disable the **Enhance Pointer Precision** setting by unchecking its respective checkbox.

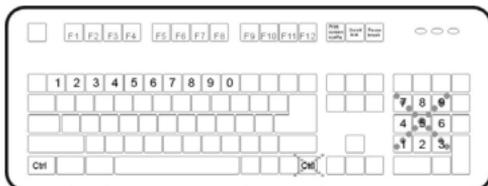
KVM Switch OSD Operation

To enter the Hotkey Menu, press the Ctrl key twice within two seconds.



- L-CTRL is the Ctrl key located on the left side of the keyboard.
- 1~8/A~H are the number keys 1-8 located in the upper row of the keyboard, and the character keys A-H (not case sensitive).

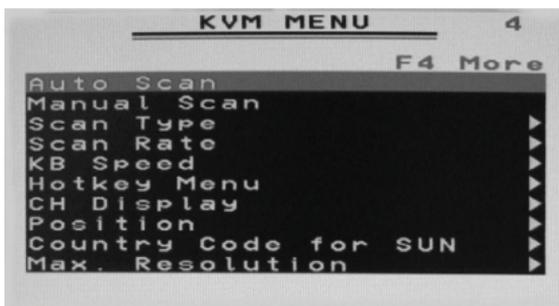
Please Note: Do not use the keypad at the right of the keyboard.



To enter the KVM Menu, press the Ctrl key three times within two seconds. Once entered, the menu will display a list of the connected computers with corresponding port numbers, names, and statuses, as shown below.



To access additional menu functions, press the F4 key. A new screen will appear displaying more functions, as shown below.



To access the remaining menu functions, press the F4 key again. This will bring you to the screen shown below.

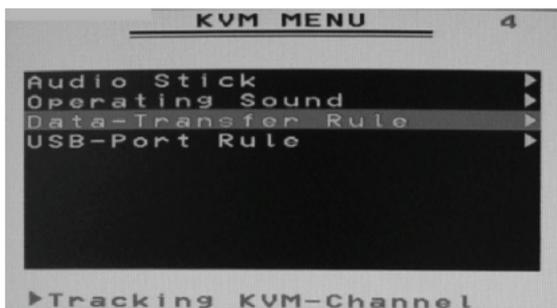


Data-Transfer Rule

Manual stick-on: Data-Transfer function resides in one particular KVM-Channel, pressing Ctrl + Ctrl + T to switch to the next KVM-Channel.



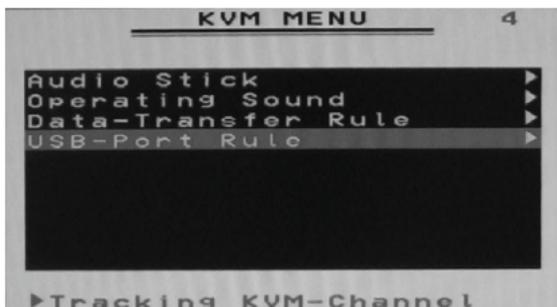
Tracking KVM-Channel: Data-Transfer function tracks the selected KVM-Channel.



USB Port Rule

Manual stick-on: USB-Port resides in one particular KVM-Channel, pressing Ctrl + Ctrl + U to switch to the next KVM-Channel.

Tracking KVM-Channel: USB-Port tracks the selected KVM-Channel.



Using the Web Interface

The Web interface is the most intuitive way to configure the SV441DUSBI, offering 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 SV441DUSBI you wish to access/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

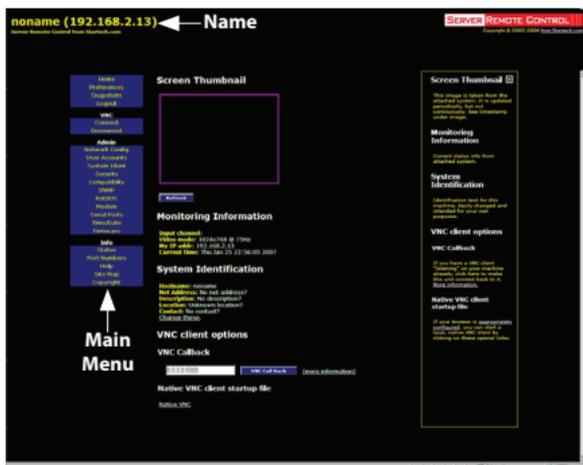


Before you can access the Web configuration interface, you must enter a username and password. The default username and password as shipped from the factory is username admin, with a password of admin.

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

Web Interface Introduction

After the initial login screen, the screen is divided into several sections, a number 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 the screen at all times. Selected categories will be displayed in the center of the screen.

File Transfer

The SV441DUSB1 is able to emulate a virtual USB disk drive on any host connected using the USB Server Interface Module (SV5USBS). Depending on configuration, it will appear to the host as a floppy drive (1.44MB), an 8MB RAM Disk or a CD-ROM. The host computer does not require any special drivers or other configuration. You can transfer files to the virtual disk at any time.

The screenshot shows a web interface with a dark blue background and white text. On the left is a vertical navigation menu with categories: Home, VNC, Admin, and Info. The main content area is divided into sections: 'Current Status' with disk details, 'Change Disk Type' with a table of options, 'CD-ROM ISO Image' with a URL input, 'Access Raw Floppy/Ramdisk Images' with a file browser, and 'Insert/Eject Disk' with a button.

Home
Thumbnails
Preferences
File Transfer
Logout

VNC
Connect
Disconnect

Admin
Network Config
User Accounts
System Ident
Security
Compatibility
SNMP
RADIUS
Modem
Time/Date
Firmware

Info
Status
Port Numbers
Help
Site Map
Copyright

Current Status

[Browse disk contents here.](#)

Disk type: Generic RAM disk (8 MiBytes)
Access: Read-write (Inserted)
Binary disk image: [Ramdisk](#)

Change Disk Type

1.44M Floppy	Ramdisk	CD-ROM
Format as floppy	Format as ramdisk	CD-ROM image

CD-ROM ISO Image

Access Raw Floppy/Ramdisk Images

[Download current raw disk image.](#)

Insert/Eject Disk

This command is not generally required:

SV441DUSB1 will wait until the host is not using the disk, and add or remove the files.

When the host computer next looks at the drive, it will notice the changes. You can read files from the virtual disk at any time, as long as the host is not actively writing to the disk. All of this happens in the background, and you may treat the virtual disk as a shared drive without any restrictions.

- Access to the files is performed through the web interface. Contents of the root directory are shown on the home page. You can download files as you would any file on the web (right-click and Save target as).
- To upload a file, click Browse, select a file, and then click Upload.
- Files and directories may be deleted using the Delete button situated to their right.

When emulating a floppy disk or RAM Disk, the data is stored in RAM on the SV441DUSBI itself. In order to emulate a CD-ROM disk drive, a web server is required to provide the CD-ROM image data. The Web server must be accessible to the unit, which communicates with it constantly as data is needed.

Floppy mode: Choose the Format as floppy button to switch to floppy mode. Under Windows, the drive will be identified as a “high density floppy” and will typically be assigned a drive letter of B:

The capacity is limited to 1.44 megabytes in this mode. The purpose of supporting floppy mode is to permit the use of floppy-disk images generated by other systems (e.g. the flash BIOS upgrade process is performed with a special floppy and is bootable, emergency repair disks are often floppy-based etc.). You can transfer bits from that floppy to the SV441DUSBI (use the upload disk image form) and boot from the special floppy.

CD-ROM Mode: The SV441DUSBI does not store any data in this mode. Instead, it emulates a USB CD-ROM drive with a disk inserted. The data from that disk must be provided by an external web server. You will need a copy of the CD-ROM contents that you want to emulate as an ISO file. This is a byte-for-byte copy of track one (the data track) of a data CD-ROM. The ISO file must be made available on a web server that can be accessed by SV441DUSBI. To switch to this mode, type in a URL pointing to the ISO image, and click on Commit. The system will connect to the web server and test the file for access. If successful, you will be shown a short report on the file contents, and the disk will be ready to use.

Please note that the only way to preview or browse the contents of the CD-ROM image, is from the host.

CD-ROM Web Server Requirements:

- Data must be hosted on a web server that the SV441DUSBI can access directly.
- An image of a bootable CD-ROM disk can be used by the BIOS to boot an operating system.
- The image file itself may be any size, but it will typically be less than 700Mb. Normally this file will be an ISO image (an ISO-9660 file system) but any disk image may be used.
- The web server must support “byte ranges”. Persistent connections are used, if available, as this greatly improves performance. “Read-only” access is provided; writing is not supported.
- CD-Rom block size must be 2048 bytes. XA-Data type tracks are not supported.

RAM Disk mode: Choose the **Format as RAM Disk** button to switch to RAM Disk mode. This mode is intended to facilitate simple data transfer between the remote user and the host computer. It will be recognized by Windows as an 8MB removable disk and assigned a drive letter. You can easily drag and drop files up to 8MB in size to this device.

Disk Formats: When you choose the **Format as...** button, the disk image stored in RAM is formatted as an empty MS-DOS disk, with a single file called **Put files here...TXT**.

SV441DUSBI is able to read most MS-DOS/Windows formatted disks and presents the files via the Web interface. However, disk emulation occurs at the lowest level, so other disk formats can be used if you have the tools needed to create and read the disk images.

At the bottom of the page are the upload and download options for the entire disk image. Any image that is exactly 1,474,560 bytes long will be treated as a floppy. Images of other sizes are supported up to 8MB.

Booting from USB Disk:

If the host computer's BIOS supports USB boot devices, it is possible to boot from the emulated CD-ROM or floppy - allowing complete operating system replacement without any on-site intervention.

The first step is getting a bootable disk image onto the emulated floppy or CD-ROM. For CD-ROM images, you will need an .ISO image from a disk that contains special bits to enable booting ("El Torito" standard). Nothing special is needed when reading the ISO from a working, bootable CD-ROM.

Please note that each BIOS manufacturer offers varying levels of support for USB boot devices and may require configuration methods that are unique (to the manufacturer) in order to utilize this feature. Similarly, please note that many BIOS's provide a simplified USB host stack and offer drivers that may not offer suitable reliability.

To create a bootable floppy, you can format the emulated floppy from the target system, or read the data from a working boot floppy. This can be done from Windows using **Disk Copy** (right click on the drive letter in the Windows Explorer) or by using a program like "RAWRITE".

Once you have a bootable image (CD-ROM or floppy) working on the Enterprise Class KVM unit, you must adjust your BIOS settings to tell it to boot from a USB device.

Please note: You must select USB CD-ROM as the boot device for the BIOS, if using a CDROM image and USB Floppy if using a floppy image.

Network Configuration

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: 10.0.0.123,10.0.3.34):

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

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 the SV441DUSBI so the new settings take effect immediately.

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

Dynamic DNS Configuration: Dynamic DNS (DDNS) is a method, protocol, or network service that allows a networked device using the Internet Protocol Suite to notify a domain name server to change, in real time, the active DNS configuration of its configured hostnames, addresses or other information stored in DNS.

Today, numerous providers, called Dynamic DNS service providers, offer such technology and services on the Internet. They provide a software client program that automates this function. The client program is executed on a computer or device in the private network. It connects to the service provider's systems and causes those systems to link the discovered public IP address of the home network with a hostname in the domain name system. Depending on the provider, the hostname is registered within a domain owned by the provider or the customer's own domain name.

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 may change the password for that user.

#	Username	Password	Delete user
	(None yet)		

Edit User Details

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

Username:

Password:

System Identification

Machine Name: This is the name that is used to uniquely identify this machine. You may wish 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.sys Contact 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.

The screenshot shows a web interface for configuring system identification. It has a dark background with white text and input fields. The sections are: **Machine Name** with a text input field containing 'hostname'; **Other identification details** with a sub-section **Location** containing a text input field with 'Unknown location?'; **Contact Name** with a text input field containing 'No contact?'; **Network Address** with a text input field containing 'No net address?'; and **Description** with a text input field containing 'No description?'. Below these fields is a message: 'You must click here to save your changes:' followed by a 'Commit Changes' button.

Security

This menu allows you to configure a number of settings, including the admin password. Be careful when making any changes remotely, as altering these features could make the unit inaccessible through Web configuration (i.e. due to firewall filtering). Note that any password changes you make will have to be entered twice to protect against user error.

The screenshot shows the 'Security Profile' configuration page. It has a dark background with white text. The sections are: **Administrator Password** with a text input field; **Idle Session Timeout** with a dropdown menu set to 'Infinite'; **Internal Firewall Setup** with a 'Disable' button and a 'Warning' message; **VNC Password Policy** with a 'Disable' button; **Trust SSH Tunnels** with a 'Disable' button; **Access Sharing Policy** with a 'Disable' button; and **Local User Lockout** with a 'Disable' button.

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.

Keyboard Mapping (for localization)

Select keyboard layout:

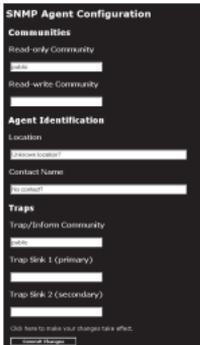
External Power Bar

Select mode:

Should all users, or only the admin user be able to control power to attached systems?

SNMP

The **SNMP** menu allows you to configure the SV441DUSBI so it can be recognized and managed using industry standard Simple Network Management Protocol software.



SNMP Agent Configuration

Communities

Read-only Community:

Read-write Community:

Agent Identification

Location:

Contact Name:

Traps

Trap/Inform Community:

Trap Sink 1 (primary):

Trap Sink 2 (secondary):

Click here to make your changes take effect.

[Cancel Changes](#)

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.

RADIUS Configuration

Use RADIUS for login:

Servers

Priority	Server IP Address	Port	Shared Secret	New Secret (twice)
# 1	<input type="text" value="0.0.0.0"/>	<input type="text" value="1812"/>	<input type="text"/>	<input type="text"/>
# 2	<input type="text" value="0.0.0.0"/>	<input type="text" value="1812"/>	<input type="text"/>	<input type="text"/>
# 3	<input type="text" value="0.0.0.0"/>	<input type="text" value="1812"/>	<input type="text"/>	<input type="text"/>

Request timeout period (seconds):

Number of retries (per server):

Click here to save your RADIUS changes and apply them:

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 SV441DUSBI.

Time / Date

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

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

Modem Option

Enable modem connections (PPP) via serial port/modem: **Enabled**

Press (tab) to see left/right navigation to between us and the modem only:
115200 (default), noxoncrtsndio

Init string: ATDT004433

Save changes by clicking here:

How To Use Modem

- Configure your client machine to dial the phone number that the modem is connected to when it connects. It should immediately start the negotiation. This is the default under windows when it thinks it connecting to a local ISP. No log stripping is required.
- RAP must be used to authenticate (not CHAP). Any username/password defined on this system may be used for this purpose, including the admin password.
- When the PPP link is established, the machine will be given the IP address 19.19.19.99, and your client machine will get 19.19.19.100. You can then point your web browser at 19.19.19.99, and your client machine will get 19.19.19.100. You can then point your web browser at 19.19.19.99, and your client machine will get 19.19.19.100.
- Hang up to end the connection.
- Crashable sites is enabled when using the modem. This will affect other users of the system as well.

Serial Consoles Attached

ID	Name / Description	Host (baud)	Mode	Force DCD	Console Lag	IPM	BNC Password	Connect...
1	No console was loaded. Plug Serial at now.							

Set Date and Time

Current time

Tue Jan 23 20:56:17 2007

Change time/date

Firmware

The firmware on the Server Remote Control is field upgradeable. To upgrade to another version:

1. Login your IPKVM as "admin"
2. Click "Firmware"
3. Click "Get latest version"
4. Click [http://18235253.net/.....](http://18235253.net/)
5. Save the latest firmware file to your computer. It will take a few minutes for downloading, depends on the speed of your network.
6. Upload the latest firmware file from your computer to the IPKVM. It will take more than 5 minutes for uploading and writing it to the flash memory of the SV441DUSBI.

Version Numbers

Component	Version / Path
System	1.0.0.0
Web	1.0.0.0
Modem	1.0.0.0
Serial	1.0.0.0
Console	1.0.0.0
IPM	1.0.0.0
BNC	1.0.0.0
Connect	1.0.0.0

Unit Numbers

Unit	IP
1	19.19.19.100
2	19.19.19.101

Auto Self Upgrade

Use the auto upgrade option.

Upload New Firmware

WARNING: Do not turn off power before upgrade completes.

Upload File:

System Reboot

Purchase Options

Get the 3-1000-0000-00-00

Custom Certificate Upload

Upload Certificate File:

Port Numbers

Port Numbers provides a table allowing you to change TCP port values for services available on the SV441DUSBI. By default, they are factory-set to common Internet values. You may wish to enhance security by disabling services that you will not use with the unit. To disable a service, change its port number to 0. When you have made any necessary changes, click **Commit changes** to use the settings the next time the SV441DUSBI restarts. To force the unit to restart immediately, click **Restart Servers**.

Network Servers and Their Port Numbers

LAN: Main Ethernet Port (192.168.2.169)

Service	Description	Default	Current Port
ssh	Secure Shell	22	22
http	Web redirector (to https)	80	80
snmp	SNMP Agent (UDP)	161	161
https	SSL Encrypted web control	443	443
vnc	VNC/RFB Protocol Server	5900	5900
vncs	SSL-terminated VNC	15900	15900

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

[Commit Changes](#)

Click here to save your changes, and restart all network servers.

[Restart Servers](#)

Localhost (127.0.0.1)

Service	Description	Port Number
http	The real web server	80
snmp	SNMP Agent (UDP)	161
vnc	VNC/RFB Protocol Server	5900

Help Menu

Provides a FAQ (Frequently Asked Questions) listing to assist you with the features and operation of the SV441DUSBI.

Site Map Menu

This menu provides a 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 SV441DUSBI.

Using the Terminal Interface via Serial Port

The terminal interface can be accessed via the serial port for the configuration of the basic settings of the SV441DUSBI. While not intended to be a substitute for the Web interface, it does allow you to configure some of the same 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.

Accessing the VNC Interface

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

Web interface: The integrated Web server includes a Java-based VNC client. This allows easy browser-based remote control.

Native VNC client: There are several third-party software programs that use the standard VNC protocol, available in open source and commercial VNC clients.

SSH access: By default, there is a standard SSH server running on port 22 (the standard SSH port). Once connected via SSH, the VNC traffic is tunneled through the SSH connection and encrypts the VNC session. Each method will be discussed briefly in the following section. The type of encryption method or client used is not critical.

Web Interface

Using SV441DUSBI's web interface requires a browser, with cookies and JavaScript enabled. To start the Java VNC client, login to the Web configuration interface and click on the thumbnail of the desktop on the **Home** menu, or click on the **Connect** button, located in the Main Menu.

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

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

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

Native VNC Client

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

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

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

SSH Tunnel (with Native VNC client)

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

```
ssh -f -l admin -L 15900:127.0.0.1:5900 10.0.0.34 sleep 60  
vncviewer -bgr233 127.0.0.1::15900
```

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 SV441DUSBI without using the web interface or a custom client.

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

Bribar Feature

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

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.

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

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

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

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

Menu: Shows the main menu.

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

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

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

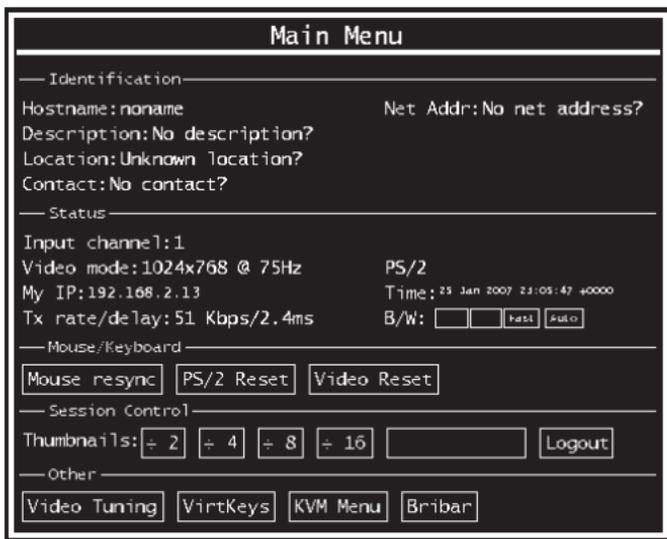
X: Click this button to close the Bribar and hide it. This can be very useful on a client machine that has a screen size the same as the remote machine. No vertical screen space is wasted with the Bribar. Use double-F7 to start the main menu, then click on the Bribar to restore the feature.

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

Main Menu

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

The main menu window may be moved by clicking and dragging on the title bar. It can be closed by pressing **Escape**, or by clicking on the red **X** in the top right corner. Here is a guide outlining various fields from the Main Menu. Most of the functions operate immediately. Other functions require a response to a confirmation prompt first before performing



the requested function.

- **Identification:** Fixed text label that is defined by the user in the Web interface. This does not affect the operation of the system and is intended to assist with administration.
- **Status:** Current status of the attached system and the status of the unit.
- **B/W Min/Avg/Max/Auto:** Bandwidth control, 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.
- **Take Control:** When multiple users are connected to the same system, use this button to take control away from another user. Only one user may control the keyboard and mouse at any time. All users see the same picture.
- **Thumbnails:** Switch to smaller thumbnail size screen images (click anywhere on thumbnail to restore it). Each button corresponds to a different sized image, from half size to one-sixteenth.
- **Logout:** End the VNC login session and disconnect.
- **Video Tuning:** Sub-menu with video adjustments, to be used when automatic picture adjustment does not provide a good quality picture.
- **VirtKeys:** Virtual keyboard provides a menu with special keys that are often hard to generate but needed by the remote system. The most common key sequence is the [Ctrl] – [Alt] – [Del].
- **KVM Menu:** Generates the key sequence used to access the on-screen menu for an enterprise-class KVM switch. When these conventional KVM switches are combined with the SV441DUSBI, this key makes accessing their built-in menu easier, especially from the Java client. This button will only be shown when an external KVM has been enabled via the web interface.
- **Bribar:** Closes or reopens the Bribar window along the bottom of the screen.

VirtKeys Menu



Clicking any button in the top half of the window simulates pressing and releasing the indicated key. In the bottom area of the screen, clicking will simulate the indicated Meta key being pressed. You may then click in the top part to send another key and release the Meta key at the same time. Alternatively, you may move the mouse outside this window, press the regular key, and then choose -RESET- to release all depressed keys. The VirtKeys menu can be left open while using the host system. You can then click the required button at the suitable time, and still interact with the host in a normal fashion.

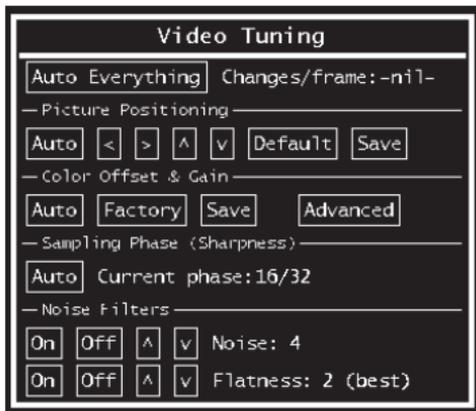
Examples:

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

Video Tuning menu

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

Changes/frame indicates the number of 16x16 blocks of video that are being sent, on average, for every frame of video. With a static image being displayed by the server, this number will be zero (shown as -nil-).



Moving the mouse, for example, will cause the number to jump to about 2 or 3. You may use this number to judge the picture quality as you adjust the controls on this menu.

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

Color Offset is a fine tuning adjustment that requires the use of a test pattern. There is a copy of the test pattern available on the **Help!** menu of the integrated web server. You must arrange for that image to be shown on the host computer. Do not allow scaling, cropping or any other changes to that image. Press the **Auto** button and the system will calibrate color for the best possible picture in approximately one minute. If the system cannot find the test pattern on the screen, it will say so. Check that the pattern isn't scaled or covered up. It's important to do this operation in 24-bit or 32-bit color video mode (i.e. truecolor). Although the algorithm may work in 16-bit or 8-bit color video modes, the results will not be optimum and usually it won't be able to recognize the test pattern.

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

Sampling Phase does not normally need to be used since the SV441DUSBI 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 use the on-screen display (OSD) system to manage your computers. Once you have established a VNC session with the SV441DUSBI, you can access the KVM features as though you were at a local console.

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 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.
- 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.

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. Each 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.

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.

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 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.

Function key <F4>

More functions are available by hitting <F4>. A new screen pops up displaying the functions described below. Most of them are marked with a triangle indicating there are options to choose from. 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.

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.

Eye Only: In Scan mode, scans only computers that have been eyemarked.

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.

Hotkey Menu

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

CH Display

Auto Off: After you select a computer, the 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 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, which is determined by the KVM connection. For a computer connected to the switch, the address is represented by the PC port number (1~4). For example, to access the PC plugged into port 4 of the Master KVM switch, type: **left Ctrl + left Ctrl + 4**.

Auto Scan

Auto Scan automatically scans through powered computers at a fixed interval:

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.

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. **Note:** 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 60Hz refresh rate and 1024x768 resolution. Using a smaller resolution like this allows you to fit multiple windows on your remote desktop. Higher refresh rates stress the video card's quality 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 (on the Video Tuning menu) to mitigate noise issues.

Network performance

- The SV441DUSBI 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 your network connection and VNC client allow.
- Network latency, which is the total time it takes for a packet to get to the SV441DUSBI 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 SV441DUSBI to automatically configure the video properties, you can use this menu to exercise a great deal of control over the settings if you wish.

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. Note that the Factory preset is always available. Simply click on the appropriate button and those settings will be restored.

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 the 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

Background

The modem feature allows the SV441DUSBI 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 SV441DUSBI and the computer you are using to manage the host computer that is essentially private, as it bypasses 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 SV441DUSBI will work with virtually any Hayes-compatible modem that recognizes the standard AT command set. Some modem manufacturers offer “enterprise” grade modem products (at a premium price) 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 SV441DUSBI.

It is important to note that modems that offer “56K” (or 57,000 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 57,000 bps do not indicate a problem with the modem or the SV441DUSBI, 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 SV441DUSBI 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 SV441DUSBI.

Modem configuration

Although most connections will work appropriately with the default settings on SV441DUSBI, 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.

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

The baud rate dictates the connection speed between the SV441DUSBI'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 SV441DUSBI will send to the modem to activate it. The string included 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 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). You may wish to test the connection with the default init string first, before making changes specific to your modem model or situation, to simplify the troubleshooting process.

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 SV441DUSBI. 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** and 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 SV441DUSBI'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**.
Beside **Username** enter the username of any valid user created using the Web interface of the SV441DUSBI. Beside **Password** and **Confirm password** enter the password that the user you entered above uses to access the Web interface.
11. This screen also includes 3 checkboxes. **Uncheck all 3 checkboxes**.
12. Click **Next**.
13. 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 SV441DUSBI.
 - 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 SV441DUSBI, 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 (see immediately above for instructions on what type of cable to use for the port you are accessing on the SV441DUSBI) 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 SV441DUSBI. 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: xxxxxxxxx

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

Background

The SV441DUSBI 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 SV441DUSBI 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

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 to the **R-Port** on the rear panel of the SV441DUSBI. 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 SV441DUSBI, 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.

Using 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 SV441DUSBI 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 R-Port 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 SV441DUSBI 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 make as many changes as needed on this menu at one time, before applying your changes. Once you are satisfied with the changes you have made, 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 SV441DUSBI 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 its 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)
```

```
1 - Show last 10 log entries
```

```
other - Return to connection
```

```
Press key ->
```

To execute the desired command, simply 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 SV441DUSBI 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 SV441DUSBI 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 SV441DUSBI, but may need to be enabled on the other end of the connection. For Unix systems, the command is:
stty -crtscts < /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 plug-in and 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 SV441DUSBI?

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 SV441DUSBI. 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 SV441DUSBI 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 SV441DUSBI 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 SV441DUSBI onto your local computer (in this case, when using Internet Explorer with Windows XP).

1. Open your Web browser and go to the SV441DUSBI 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 it should be. Normally a slight video positioning error is perceived as a mouse sync issue. A video positioning error is visible as a black line along the top or bottom (and right or left) edges of the remote screen. Remember to save your position changes!

Cannot login via SSH.

Remember to use either **admin** or a username created in the system as the user name you give your SSH client.

If you see a warning about **identity of host cannot be verified**, and a question about saving the host's fingerprint, this is normal for the first time you connect to any machine running SSH. You should answer **yes** so that your SSH client saves the public key of this host and doesn't re-issue this warning.

Certificate warning shown when connecting via HTTPS.

It is normal for a warning dialog to be shown when connecting via HTTPS. The SSL certificate S 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 left-most settings (lowest possible).

Specifications

General Specifications

Maximum Supported Video Mode	1600 x 1200 @ 85Hz
Standard Video Modes Supported	640x400 @ 85Hz 720x400 @ 85Hz 640x480 @ 60Hz, 72Hz, 75Hz, 85Hz 800x600 @ 56Hz, 60Hz, 72Hz, 75Hz, 85Hz 1024x768 @ 60Hz, 70Hz, 75Hz, 85Hz 1152x864 @ 75Hz 1280x960 @ 60Hz, 85Hz 1280x1024 @ 60Hz, 75Hz, 85Hz 1600x1200 @ 60Hz, 65Hz, 70Hz, 75Hz, 85Hz
Maximum Power Consumption	18 Watts (12VDS, 1.5A) Centre Positive
Input Connectors	Video In USB Keyboard USB Mouse LAN (RJ45) R-Port (RJ14) DB9 RS-232 Male DC IN
Regulatory Certifications	FCC Class A, CE, ROHS, VCCI

Source code for the unit operating system is available upon request. Please contact us by phone, live chat, or email to make your request. This offer is valid for three years from the date of purchase and/or for as long as parts or customer support is offered for this product. Charges for the reasonable cost of copying and/or conveying may apply.

Supported Protocols

Service	Description	Benefit
SSH	Secure Shell	May be used to securely "tunnel" VNC and HTTP protocols.
HTTP	Web Redirector (to HTTPS)	Convenience server to redirect all web traffic to encrypted port. Clear-text HTTP is not supported.
SNMP	SNMP Agent (UDP)	Allows integration with existing SNMP network management systems.
HTTPS	SSLTLS Encrypted Web Control	Secure control and management of the device and attached system. Screen snapshots may be downloaded. Integrated Java VNC client (with or without encryption) allows control from any Java enabled browser. Password protected.
VNC	VNC/RFB Protocol Server	Standardized real-time KVM network protocol. Compatible with existing VNC client software.
VNCS	SSL-tunneled VNC	VNC protocol tunneled via SSLTLS encryption. For secure real-time control of the server over public networks.
DHCP	Dynamic IP Setup Config	Eases network setup by fetching IP address and other network settings from a centralized server.
RADIUS	Centralized authentication	Allows integration with existing RADIUS servers, so that user management can be centralized. Supports challenge response authentication using hardware tokens (like SecurID) and conventional passwords.
SYSLOG	System event logging to another system	MIT-LCS UDP protocol. Must be configured via DHCP option.
DNS	Domain Name Service	Converts text name into IP Address Only used in the URL specification needed to emulate a CDROM. Use is optional.

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 three 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

Hard-to-find **made easy**®

Hard-to-find made easy. At StarTech.com, that isn't a slogan. It's a promise.

StarTech.com is your one-stop source for every connectivity part you need. From the latest technology to legacy products — and all the parts that bridge the old and new — we can help you find the parts that connect your solutions.

We make it easy to locate the parts, and we quickly deliver them wherever they need to go. Just talk to one of our tech advisors or visit our website. You'll be connected to the products you need in no time.

Visit **www.startech.com** for complete information on all StarTech.com products and to access exclusive resources and time-saving tools.

StarTech.com is an ISO 9001 Registered manufacturer of connectivity and technology parts. StarTech.com was founded in 1985 and has operations in the United States, Canada, the United Kingdom and Taiwan servicing a worldwide market.