

K202/204 2/4-Port DVI-I Secure KVM Switch



User Manual

Models:

K202E – Secure 2-port DVI-I KVM Switch w/audio and DPP

K204 - Secure 4-port DVI-I KVM Switch w/audio

K204E - Secure 4-port DVI-I KVM Switch w/audio and DPP

Rev: 2.3

Doc No : HDC06148



Table of Content

Section 1 – Introduction	2
Package Content.....	2
Section 2 – Overview	2
Security Features.....	3
Operational Features.....	5
Equipment Requirements.....	6
Safety Precautions.....	9
Front Panel Features – K202E.....	10
Front Panel Features – K204/K204E.....	11
Rear Panel Features – K202E.....	12
Rear Panel Features – K204/K204E.....	13
Tamper Evident Labels.....	14
Active Anti-Tampering System.....	14
Product Specifications.....	15
Section 3 – Installation	16
Before Installation.....	16
Installation.....	17

Section 4 – Operation	22
Operation.....	20
DPP Operation (K20xE only).....	21
Section 5 – Troubleshooting	23
Troubleshooting Guide.....	23
High Sec Labs Warranty Programs.....	26
High Sec Labs Limited Warranty Terms and Conditions.....	26
High Sec Labs Security Procedures.....	28
COPYRIGHT AND LEGAL NOTICE.....	29

Record of Revisions

Rev	Date	Description of changes
1.0	Nov 11, 2010	Initial release
1.1	Nov 20, 2011	Internal review for CC evaluation
2.1	Dec 30, 2011	Released for customers
2.2	Feb 4, 2012	Added security procedures text
2.3	April 19, 2012	Added support for composite devices

Introduction

Thank you for purchasing this HSL Secure DVI-I KVM Switch. This KVM Switch is designed for use in secure defense and intelligence environments across wide security gaps. This 3rd Generation Secure KVM Switch offers optical data diode per channel. Optical data diodes are used to prevent data transfer between connected computers running at different security levels even if these computers attempts to attack the KVM. This product provides the highest security safeguards and features that meet today's and will meet future cyber prevention requirements.

This User Manual provides all the details you'll need to install and operate your new Switch, in addition to troubleshooting guidance—in the unlikely event of a problem.

Package Contents

Inside product packaging you will find the following:

- HSL Secure DVI-I KVM Switch unit
- 12V 1.5A DC Power Supply
- DVI to VGA adapter plug
- This User Manual

Important: This product is equipped with always-on active anti-tampering system. Any attempt to open the product enclosure will activate the anti-tamper triggers and render the unit inoperable. If the unit's enclosure appears disrupted or if all the channel-select LEDs flash continuously, please remove product from service immediately and contact HSL Technical Support.

Security Features

HSL Secure KVM Switch is the most advanced and secure commercially available KVM Switch available today. This product is a derivative of high security KVM product used in newest NATO nuclear submarines. Below is a summary of some of the security features incorporated into the product.

Unidirectional Data Paths

Optical diodes used to enforce unidirectional data flow from the peripheral devices to computers preventing potential leakage paths between computers even in the severe threat of two infected computers attacking the KVM.

No Shared Resources

This KVM Switch designed to securely operate even when peripheral devices are vulnerable to signaling attacks. This KVM Switch does not allow computer access to any shared resource and does not share controllable power sources.

Dedicated Processors for Emulation

The Switch features a dedicated processor per computer port to emulate peripheral devices. This keeps each computer running on different security levels physically separated and secure at all times, and prevents any unintended data leakage between computers.

Non-Reprogrammable Firmware

The Switch features custom firmware that is not reprogrammable, preventing the ability to remotely attack the KVM control logic.

EDID Emulation and Firewall

HSL Secure KVM Switch blocks the computer access to the shared display by using isolated EDID emulators. This arrangement together with the internal EDID firewall protects from KVM attacks targeting the external memory effect of the shared display.

USB Ports Protection

Console USB ports are protected from the use of storage and other unsafe USB devices through strong filtering (independent of computer protection means). Unqualified devices are rejected when connected to the Switch. Only mouse and keyboard data are passed through.

Heavy-duty Steel Enclosure

HSL Secure KVM Switches uses thick steel components to protect the product from physical tampering and to minimize radiated electromagnetic emissions that can be snooped or intercepted.

Active Always-On Anti-Tamper

Active chassis anti-tamper system prevents the KVM electronic circuitry from being accessed and tampered with by permanently disabling the product once tampering is detected.

Holographic Tamper-Evident Labels

Four serially numbered holographic security tamper-evident labels are placed on the enclosure surface to provide a visual indication if the Switch has been opened or compromised.

High Inter-Channel Analog Isolation

HSL Secure KVM Switches offers exceptionally high isolation between computer channels to prevent analog leakages across the KVM.

Dedicated Peripheral Port

HSL patented Dedicated Peripheral Ports enables secure use of not only CAC or smart-card readers but also fingerprint readers, face recognition and iris recognition devices. Separate cables used for this port enable further protection and isolation of this function.

Secure Packaging

“Tear away” packaging ensures secure delivery of the Switch as it is routed to the end user.

Common Criteria EAL-4 Listing

The Switch is listed by the Common Criteria organization. It is Common Criteria validated to EAL 4+ (Evaluation Assurance Level 4) to assure the highest level of protection. Product complies with standard higher than NIAP Protection Profile 2.1.

Operational Features

The HSL Secure KVM Switch was designed with the user in mind for today's IT environment. Below is a summary of some of the features incorporated into the Product.

USB Support

HSL Secure KVM Switch product designed and tested to support the widest variety of USB keyboards and mice.

Dedicate Peripheral Port

HSL K20xE Secure KVM Switch products supports parallel switching of wide set of user authentication devices including CAC, smart-card and biometric readers.

Dedicate Peripheral Port Host Detection and Freeze Functions

HSL patented Host detection function enables simple switching of display, keyboard audio and mouse without disconnecting user authentication session through detection of unconnected computer and through the use of freeze push-button.

Keyboard Shortcuts Support

HSL Secure KVM Switch is the only Secure KVM that supports keyboard shortcuts switching mode while providing highest level of isolation.

DVI-I and HDMI Support

The Switch supports both digital (DVI-D and HDMI) and analog video (VGA) displays and video cards.

Dual-link Video Support

HSL Secure KVM Switch supports dual-link digital video signals to enable highest available display quality and resolutions.

Audio Support

Switch support audio out switching. Microphone switching not supported to prevent analog leakages through audio ports.

RDC Support

HSL Secure KVM Switch products support patented Remote Desktop Controller device to enable easy and intuitive KVM operation at the user's desktop. Channel names may be programmed into the RDC display to improve usability and security.

Display Diagnostic LED

Special display diagnostic LED near console display connector provides essential guidance during installation.

KVM Extenders Support

HSL Secure KVM Switch supports most copper and fiber KVM extenders connected to the console port.

Equipment Requirements

Cables

HSL highly recommends you use HSL Cable Kits for your Switch to help ensure superior security and performance. These cables offer the highest quality possible to ensure optimal data and video transmission.

One Cable Kit is required per connected computer.

Smart Cables from Belkin enables video conversion from computer VGA output to DVI-D KVM input to enable legacy video mix with newer DVI computers and display.

Note: If VGA display will be used then all computers must be connected through VGA interface. If one computer is VGA only then all other computers must be connected through VGA and display must support DVI-I or VGA.

How to order?

To connect:	Use:	Order No.
Computer keyboard, mouse, DVI-D single-link display	KVM Cable short (1.8 m), DVI-D to DVI-D Single-Link, USB, Black	CPN05485
Computer keyboard, mouse, DVI-D Dual-link display	KVM Cable short (1.8 m), DVI-D to DVI-D Dual-Link, USB, Black	CPN05486
Computer VGA video	KVM Cable short (1.8 m),	CPN05489

output	DVI-A to VGA, USB, Black	
Computer CAC or other user authentication USB device	KVM Cable short (1.8 m), CAC, Black-Yellow	CPN05487
Computer keyboard and mouse USB	KVM Cable short (1.8 m), USB Type-A to USB Type-B, Black	CPN05493
Computer audio output	KVM Cable short (1.8 m), Audio Out, Black-Green	CPN05490
Computer VGA output (display and other computers are DVI)	KVM Smart-Cable VGA PC to DVI KVM converter cable with USB type A to USB type B, 6ft (1.8 m), black	CPN06011
KVM DVI-I video output to VGA only display (one unit provided in the packaging)	DVI-I to VGA display adapter	CPN05492

Important: The use of cables other than those provided by HSL is not recommended. Use of other cables may affect system security, may permanently damage the product and may void product warranty.

Computers

The Switch is compatible with computers, thin-clients, servers and laptops running on, but not limited to, the following OS platforms:

- Windows® 2000
- Windows XP (Home/Professional)
- Windows 2003 Server
- Windows 7
- Windows Vista®
- Red Hat® Linux®
- Ubuntu® Linux®
- Other Linux distributions
- Mac OS® X v10.3 and higher.

Laptop docking stations having DVI, VGA or HDMI display output are supported.

For latest compatibility list see HSL website or contact HSL support.

USB Keyboard console port

The Switch USB keyboard console port is compatible with the following types of devices:

- Standard USB keyboard (excluding devices having other internal functions such as USB hub, or composite device); and:
- Bar-code readers emulating USB keyboard.

PS/2 Keyboard console port

The Switch PS/2 keyboard console port is compatible with the following types of devices:

- Standard PS/2 keyboard; and:
- Bar-code readers emulating USB keyboard.

USB Mouse console port

The Switch mouse USB console port is compatible with the following types of devices:

- Standard USB mouse (excluding USB hubs or other USB functions in composite device); or
- Standard USB keyboard or Standard KVM Extender composite device having a keyboard/mouse functions

PS/2 Mouse console port

The Switch PS/2 mouse console port is compatible with the following types of devices:

- Standard PS/2 mouse.

User Authentication Devices (K20xE only)

The Switch is compatible with the following types of user authentication devices plugged into the product Dedicated Peripheral Port (DPP):

- USB smart-card reader (or Common Access Card reader); or:
- USB biometric device such as fingerprint recognition device; or:
- USB authentication token.

For latest compatibility list see HSL website or contact HSL support.

User Display

The Switch is console display port is compatible with the following types of displays:

- VGA; or:
- DVI-D Single-link; or:
- DVI-D Dual-link; or:
- HDMI (adapter to DVI needed); or:
- DVI-I.

Note that all computers connected must support the same video interface selected for the user display.

User Audio Devices

The Switch is compatible with the following types of user audio devices:

- Stereo headset; or:
- Amplified stereo speakers.

Remote Desktop Controllers

The Switch is compatible with the following types of Remote Desktop Controller device:

- HSL RDC440 device connected to the switch RDC port.

RDC must be connected through standard CAT-5 and higher LAN cable.

Important: Do not use LAN cables longer than 8 meters. Do not use crossed cables. Do not connect either cable ends to LAN switch, PoE power injector or other LAN ports. Immediate permanent damage to the switch or to the RDC may be resulted.

Remote User Extension

The Switch is compatible with the following types of Remote Fiber Extender device:

- HSL RFE720 Secure Remote Fiber Extender device connected to the switch console ports; or:
- HSL RFE740 Secure Remote Fiber Extender device connected to the switch console ports.

Note: use of other copper or fiber extender is not recommended. While other solutions may work, it would not support RDC. Using the Secure KVM Switch remotely without having user indications of channel selected violates product security certification.

Power Supply

Use only HSL power supply that provided with the switch. In case of a power supply failure, order a replacement unit from HSL.

Order No.:

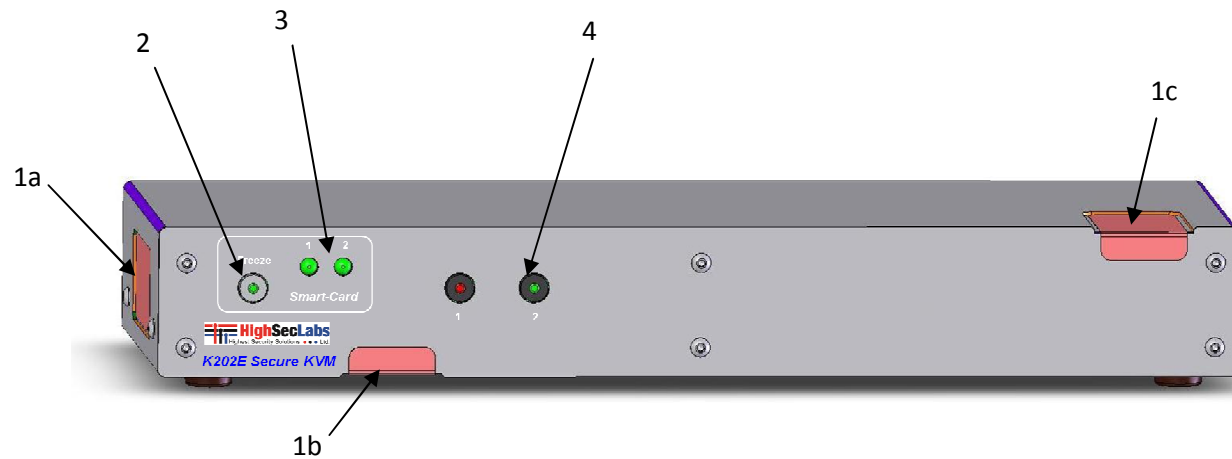
- EU – CPS05296
- US – CPS05500
- UK - CPS05499

Safety Precautions

Please read the following safety precautions carefully before using the product:

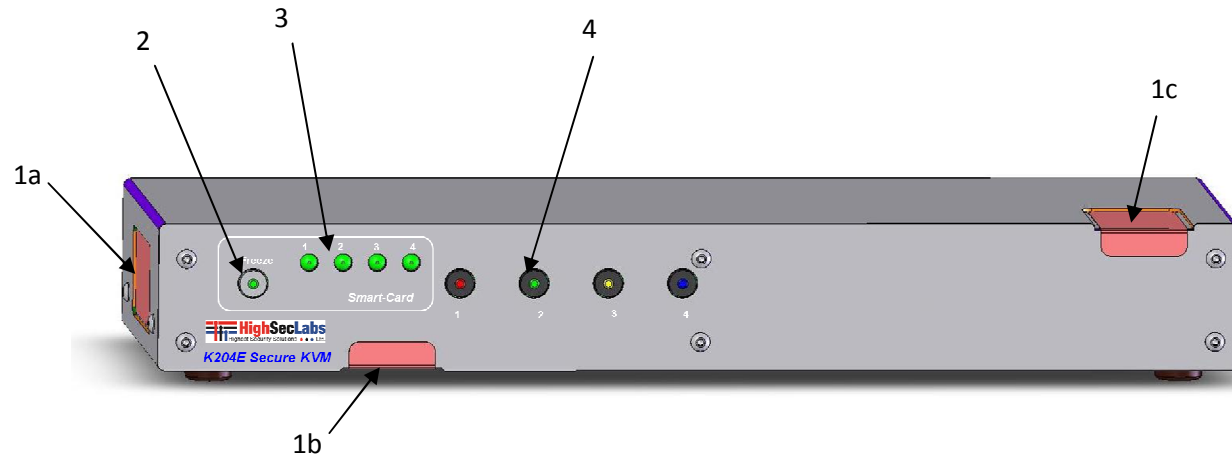
- Before cleaning, disconnect the product from DC power.
- Be sure not to expose the product to excessive humidity.
- Be sure to install the product on a clean secure surface.
- Do not place the DC power cord in a path of foot traffic.
- If the product is not used for a long period of time, remove the product's wall-mount power supply from the mains jack.
- If one of the following situations occurs, get the product checked by a qualified service technician:
 - The product's power supply is overheated, damaged, broken, causes smoke or shortens the mains power socket.
 - Liquid penetrates the product's case.
 - The product is exposed to excessive moisture or water.
 - The product is not working well even after carefully following the instructions in this user's manual.
 - The product has been dropped or is physically damaged.
- The product has obvious signs of breakage or loose internal parts.
- The product should be stored and used only in temperature and humidity controlled environments as defined in the product's environmental specifications.
- The wall-mount power supply used with this product should be the model supplied by the manufacturer or an approved equivalent provided by HSL or an authorized service provider. The use of improper power source will void product warranty.

Front Panel Features – K202E



- 1a-1c – Holographic Tamper Evident Labels
- 2 – DPP (Dedicated Peripheral Port) Freeze push-button and Status LED
- 3 – DPP channel select LEDs
- 4 – Channel Select push-buttons and LEDs

Front Panel Features – K204/K204E



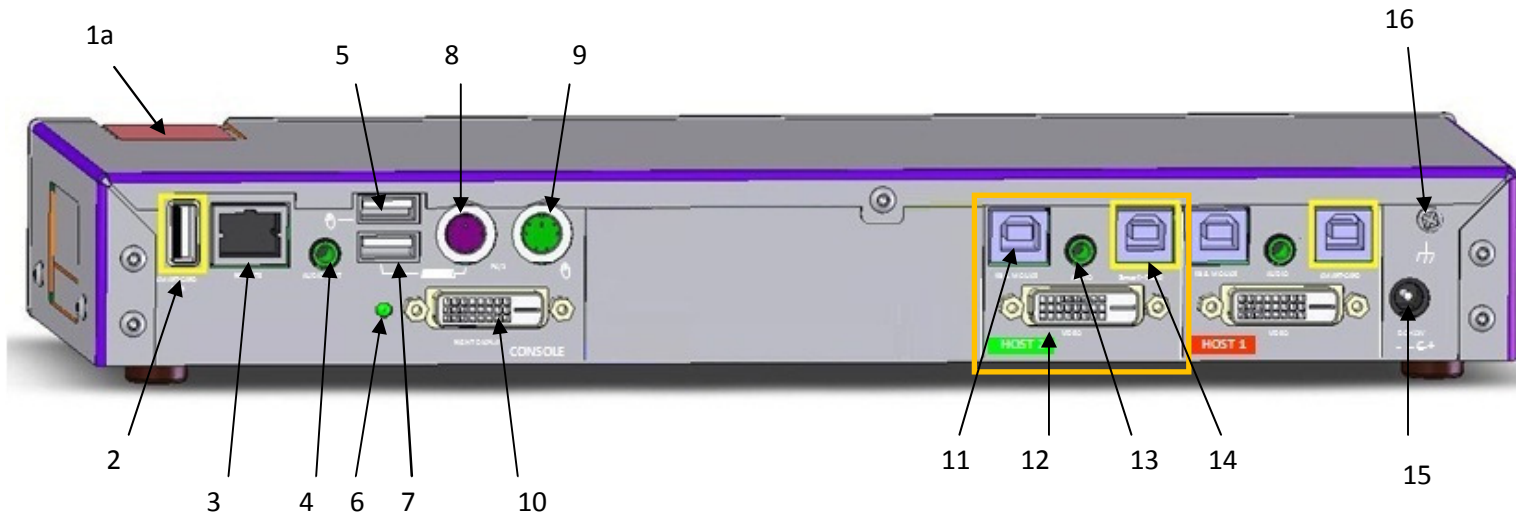
1a-1c – Holographic Tamper Evident Labels

2 – DPP (Dedicated Peripheral Port) Freeze push-button and Status LED [K204E only]

3 – DPP channel select LEDs [K204E only]

4 – Channel Select push-buttons and LEDs

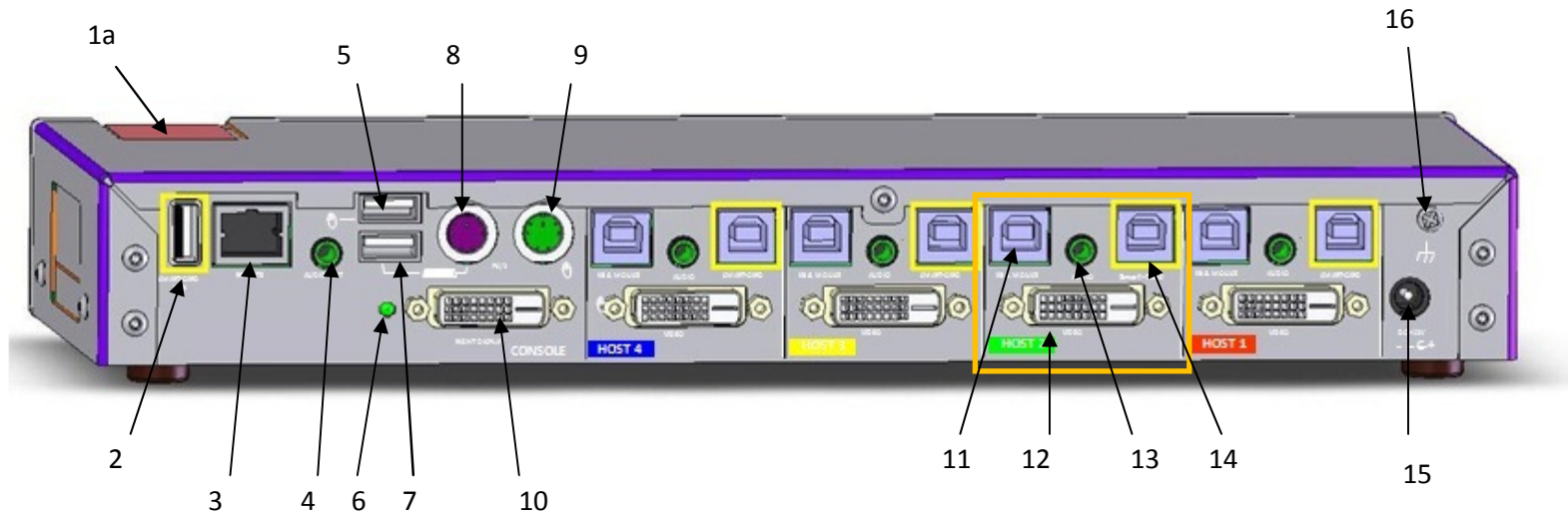
Rear Panel Features –K202E



- 1a – Holographic Tamper Evident Label
- 2 – DPP (Dedicated Peripheral Port) console USB jack
- 3 – RDC (Remote Desktop Controller) port RJ-45
- 4 – Audio console output 3.5 mm stereo jack
- 5 – USB Mouse jack
- 6 – Display diagnostic LED
- 7 – USB Keyboard jack
- 8 – PS/2 Keyboard jack (Mini-DIN)

- 9 – PS/2 Mouse jack (Mini-DIN)
- 10 – User display console output DVI-I connector
- 11 – Computer #2 group Keyboard/Mouse USB jack
- 12 - Computer #2 group DVI-I video input jack
- 13 - Computer #2 group audio input jack 3.5 mm stereo
- 14 – Computer #2 group DPP USB jack
- 15 – DC Power input jack – barrel type
- 16 – Chassis ground connection screw

Rear Panel Features – K204/K204E



- 1a – Holographic Tamper Evident Label
- 2 – DPP (Dedicated Peripheral Port) console USB jack [K204E only]
- 3 – RDC (Remote Desktop Controller) port RJ-45
- 4 – Audio console output 3.5 mm stereo jack
- 5 – USB Mouse jack
- 6 – Display diagnostic LED
- 7 – USB Keyboard jack
- 8 – PS/2 Keyboard jack (Mini-DIN)

- 9 – PS/2 Mouse jack (Mini-DIN)
- 10 – User display console output DVI-I connector
- 11 – Computer #2 group Keyboard/Mouse USB jack
- 12 - Computer #2 group DVI-I video input jack
- 13 - Computer #2 group audio input jack 3.5 mm stereo
- 14 – Computer #2 group DPP USB jack
- 15 – DC Power input jack – barrel type
- 16 – Chassis ground connection screw

Tamper Evident Labels

HSL Secure KVM Switch uses 4 holographic tamper evident labels to provide visual indications in case of enclosure intrusion attempt. These labels indicate white dots or the text “VOID” once removed. When opening product packaging inspect the 4 tampering evident labels.

If for any reason one or more tamper-evident label is missing, appears disrupted, or looks different than the example shown here, please call HSL Technical Support and avoid using that product.



HSL Holographic Tampering Evident Label

Active Anti-Tampering System

HSL Secure KVM Switch is equipped with always-on active anti-tampering system. If mechanical intrusion is detected by this system, the Switch will be permanently disabled and LED will blink continuously.

If product indication tampered state (all LEDs blinking) - please call HSL Technical Support and avoid using that product.

Product Specifications

Part No.	K202E - CGA05267 K204 - CGA06009 K204E - CGA05269	Console Audio Out	3.5mm stereo jack
Enclosure	Steel metal enclosure	CPU Keyboard/Mouse Ports	USB Type-B jack
Power Requirements	12V DC, 1A (maximum) power adapter with center-pin-positive polarity	CPU DPP Ports	USB Type-B jack
AC Input	100 to 240VAC	CPU Audio Input	3.5mm stereo jack
No. of Secure Channels	2 (K202E), 4 (K204x)	CPU Video Input Port	DVI-I dual-link female
No. of Users Supported	1	Port Selectors	2 (K202E), 4 (K204x)
No. of Computers Supported	2 (K202E), 4 (K204x)	LED Indicators	2 (K202E), 4 (K204x) additional 2 / 4 for DPP (K20xE only)
Displays Supported	1 single-link / dual-link digital DVI-D display; analog VGA display or HDMI with adapter	Operating Temp	32° to 104° F (0° to 40° C)
Resolution Support	Up to 2560x1600	Storage Temp	-4° to 140° F (-20° to 60° C)
Console Keyboard Input	USB Type-A female connector or PS/2 Mini-DIN 6 pin female connector	Humidity	0-80% RH, non-condensing
Console Mouse Input	USB Type-A female connector or PS/2 Mini-DIN 6 pin female connector	Warranty	2 years; can be extended to up to 7 years at cost.
Console DPP Input	USB Type A (K20xE only)	Dimensions	80 (W) x 158 (D) x 34 (H) mm / 3.15 (W) x 6.22 (D) x 1.34 (H) inches
Console Display Port	1 DVI-I dual-link female connector	Weight	1 Kg. (2.2 lbs.)
		Security Accreditation	Common Criteria EAL 4+
		Made in	Israel
		Product design life-cycle	10 years per MIL-HDBK-217E

Before Installation

Unpacking the Product

Before opening the product sealed packaging inspect the seal condition to assure that product was not accessed or tampered during delivery. If packaging seal looks suspicious contact HSL support team and do not use the product.

After seal removal inspect packaging content to verify that required components included. See packaging content list in page 4 above.

After the Secure KVM Switch removed from its packaging materials inspect the 4 tampering-evident labels to assure that product is properly sealed. If one or more label is damaged or missing contact HSL support and do not use that product.

Where to locate the Switch?

The enclosure of the Switch is designed for desktop or under the table configurations. An optional Mount Kit is available.

Product must be located in a secure and well protected environment to prevent potential attacker access.

If longer set of cables or if a Secure Fiber Extender (RFE) are used, KVM Switch may be remotely located in a locked down facility to prevent unauthorized users access.

Consider the following when deciding where to place the Switch:

- User access to the front panel push-buttons (not needed if keyboard shortcut or RDC are used to switch channels).
- Keyboard and mouse cables length. Cables typically may be extended to a distance of 4 meters.
- Display cable length. Typically may be extended to around 10 meters without video quality degradation (still depends on display and cables quality and must be tested prior to fixed installation).
- The location of the computers in relation to the switch and the length of available KVM cables (typically 1.8 m)

Note: Due to USB and DVI signal limitations, the cable length cannot exceed 4.6 m (15 feet).

Warning: Avoid placing cables near fluorescent lights, air-conditioning equipment, RF equipment or machines that create electrical noise (e.g., vacuum cleaners).

Installation

Step 1 Connecting the Console devices to the Switch

See figures in pages 12-13 above for connector locations.

Note: for installation instructions with Remote Fiber Extender (RFE) – refer to the RFE product User Manual.

- Connect the user display.

Note: If user display is only VGA

- Verify that all computers are having either VGA or DVI-I display output.
- Use supplied DVI to VGA adapter.
- Connect the user keyboard (USB or PS/2).
- Connect the user mouse (USB or PS/2).

Note: If USB mouse is connected to the USB keyboard port or if USB keyboard is connected to the USB mouse port it would not work!

Note: Keyboards with integrated USB hub, card-reader, storage device or multimedia extension will be either not supported at all or only keyboard function will be operating.

- Connect the user authentication device to the DPP USB port [Optional – K20xE only].
- Connect the user headphones or amplified speakers to the switch audio output jack.

Note: In any case do not connect a microphone to the switch audio output port.

Step 2 Connecting the Computers

Connect the 2-4 computers to the Secure KVM switch through the following steps:

- Connect each computer with KVM cable (DVI and USB or VGA and USB cables – for details on cables see page 7). USB cable can be connected to any free USB port in the computer.

Note: If computer is having more than one video output connector – first test for video output availability by connecting a display directly to that port.

Note: Note: The USB cable must be connected directly to a free USB port on the computer, with no USB hubs or other devices in between.

- Connect an audio cable (CPN05490) to the computer audio output (lime green color) or line output (blue color) jacks.

Step 3 Power up

- Power up user display. Select proper input if applicable (VGA or DVI-D).
- Power up the Secure KVM Switch by connecting the power. The display diagnostic LEDs should be solid green for a few seconds after power up. This indicates the display EDID information has been captured and secured. If the display diagnostic LED remains blinking for longer than 10 seconds after power up, refer to the Troubleshooting section of this user manual.
- Power up the connected computers.

Note: When you power on your computers, the Switch emulates both a mouse and keyboard on each port and allows your computers to boot normally. The computer connected to port “1” will be displayed on the user’s display. Check to see that the keyboard, display, and mouse are working normally. Repeat this

check with all occupied ports to verify that all computers are connected and responding correctly.

If you encounter an error, check your cable connections for that computer and reboot. If the problem persists, please refer to the Troubleshooting section in this User Manual.

DPP Installation (K20xE only)

Notice: *The DPP functionality was not certified by Common Criteria. Currently, Common Criteria does not offer any guidelines for DPP peripheral support in the Peripheral Sharing Protection Profile. The inclusion of this functionality does not affect the Common Criteria certification applied to the rest of the product.*

- If computer and KVM Switch supports user authentication device, connect another USB cable CPN0444 for the DPP function. DPP USB cable can be connected to any free USB port in the computer.

Note: Do not connect DPP USB cable if user authentication device is not needed. Secure KVM Switch automatically detects this cable to program DPP port selection logic accordingly.

If not all of the channels are having DPP function (some computers not connected through DPP cable) – make sure that channel #1 is using DPP – switch channels if needed.

When KVM is powered on - once the connected device is qualified and ready for use – the DPP status LED should illuminate green.

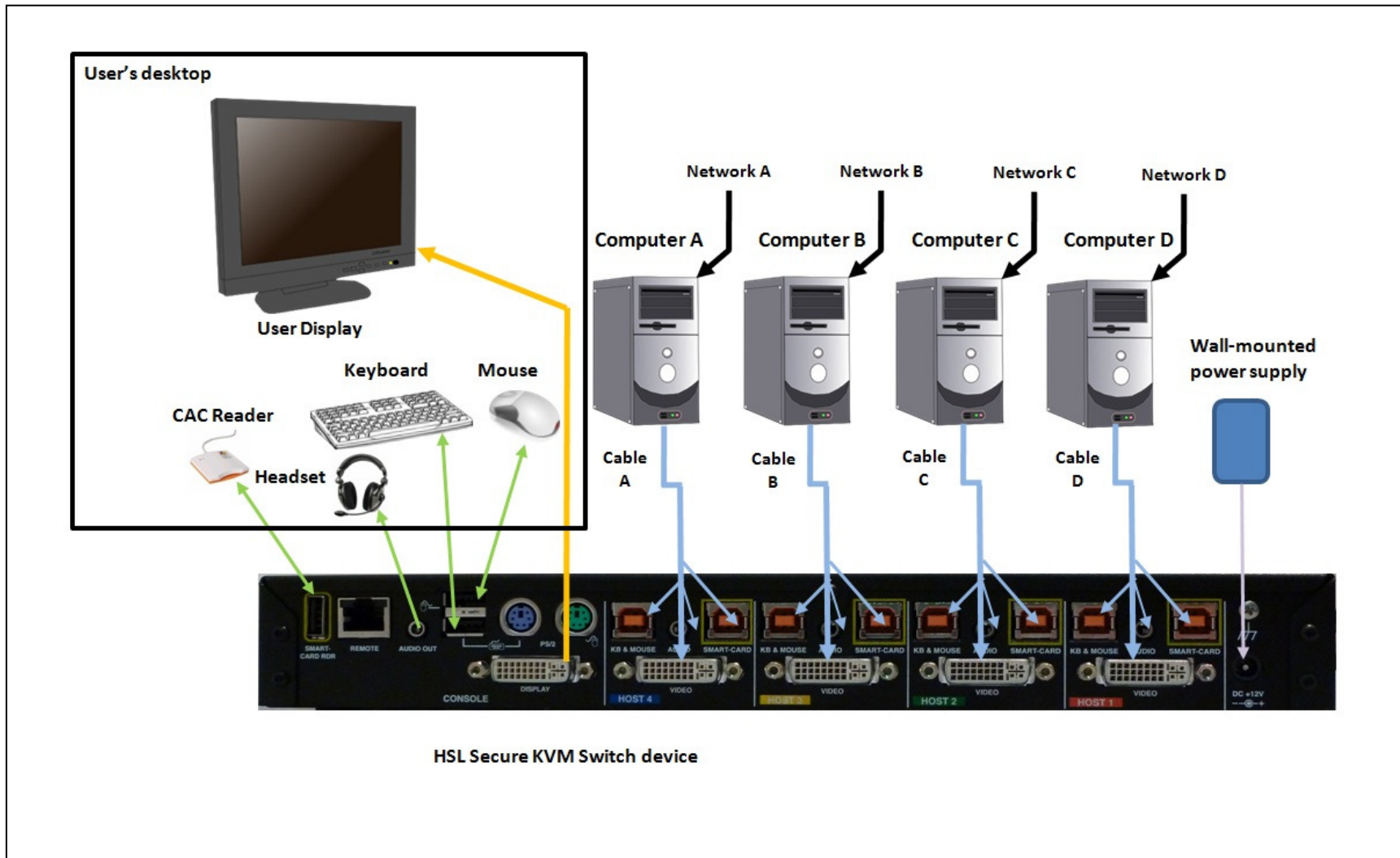
If connected device cannot be detected by the Secure KVM Switch then DPP status LED will not illuminate at all. Device must be fully compliant with USB 1.1 or USB 2.0 standard.

Possible reasons:

- Non standard USB device
- Device only operating in USB 3 mode
- Device not operating

Use other devices instead.

If the device is detected but does not match DPP qualification specification – device will be rejected as indicated by status LED illuminating steady red.



Typical system installation diagram (K204E)

Operation

Now that you have connected your console and computers to the Switch, it is ready for use. Default channel after power up is channel #1 as indicated by channel select LED #1 illumination. You can select which computer you wish to control by one of the following methods:

1. Switch between computers using front panel push-buttons

You can select which computer you wish to control by momentarily pressing the corresponding port selector push-button on the front of the Switch. The LED number will illuminate to indicate which computer (or port) is currently selected. It may take approximately 1 second for the video signal to sync after switching ports. This is normal behavior and is dependent on the display connected. This is normal operation and ensures that proper synchronization is established between the display and the connected computers.

Note that keyboard and mouse inputs can only be sent to the selected computer, and video outputs can only be received from the selected computer. The Switch also prevents any data transfer between connected computers, ensuring the security of your computers.

2. Switch between computers using keyboard shortcuts

You can select which computer you wish to control by typing key combinations on the keyboard.

To switch KVM to another channel press CNTL+CNTL+ “Channel number” for example for computer #3 press CNTL+CNTL+3.

Note: use left control key only.

3. Switch between computers using RDC

You can select which computer you wish to control by rotating the rotary channel select knob, pointing to the desired channel number as appears in the LCD and pressing the knob to confirm. New selected channel will be indicated in the LCD.

Note: The Secure KVM Switch does not have a power switch. It is highly recommended that the product will be powered continuously.

RDC Operation

For Remote Desktop Controller operation – refer to the RDC User Manual supplied with the product.

Note that when RDC is connected – the Secure KVM Switch front panel push-buttons are deactivated.

Important Security Note:

If you are aware of potential security vulnerability while installing or operating this product, we encourage you to contact us immediately at the following email address: security@highseclabs.com

DPP Operation (K20xE only)

Notice: The DPP functionality was not certified by Common Criteria. Currently, Common Criteria does not offer any guidelines for DPP peripheral support in the Peripheral Sharing Protection Profile. The inclusion of this functionality does not affect the Common Criteria certification applied to the rest of the product.

In the following examples we would use the K204E for demonstration with DPP USB cables connected in channels 1, 3 and 4 and assume that all 4 connected computers completed the boot.

If the device connected to the DPP console port is not qualified – the DPP status LED would illuminate steady red color.



In such case the device must be replaced with a qualified device.

If the device connected to the DPP console port is not standard or undetectable – the DPP status LED would not be illuminated at all. DPP is unusable.



Once the device connected to the DPP console port is qualified – the DPP status LED should illuminate steady green.

If switch just completed power up it will be switched to channel #1 (default computer) and channel select LED #1 will be illuminated.



Once the user completed logon to computer #1 and wants to keep the authentication device coupled to computer #1 the freeze mode should be activated by pressing the freeze push-button. The DPP status LED will start blinking green color. From now on the DPP channel selection will remain on channel #1 unrelated to the KVM switch channel selection.

If the user switches the KVM switch to channel #2, DPP channel select #1 will remain illuminated while KVM channel select LED will indicate channel #2.



The user may further select channel #3 and the DPP channel select LED #1 will remain illuminated while KVM Switch will indicate that channel #3 has been selected.



If DPP status LED is not illuminated green – call technical support.

Once the user presses again the DPP freeze push-button, freeze mode will be deactivated and DPP will switch to same channel as KVM switch selected channel #3 in this case. DPP status LED will return to steady green as before.



If the user switches now the KVM switch to channel #2 the DPP will automatically enter freeze mode as indicated by the blinking green DPP status LED.



If the user will now switch the KVM switch to channel #1 DPP will remain in freeze mode on channel #3 as before.



The set of rules that applies to the DPP switching are:

Note: It is assumed here that connected channel is channel that connected to the computer with DPP USB cable and that the connected computer is running (after boot completion).

1. The DPP will follow the KVM channel selection unless:
 - User has selected DPP freeze mode; or
 - KVM was switched to unconnected channel and then the device will enter DPP freeze mode automatically.
2. DPP would not release from freeze mode when KVM selected channel is unconnected.
3. Once released from freeze mode the DPP will follow the KVM selected channel.
4. If connected device is unqualified or not recognized then no switching will be possible. DPP is deactivated (indicated by DPP mode LED illuminating in steady red color).

Troubleshooting Guide

Important Note:

If you are aware of potential security vulnerability while installing or operating this product, we encourage you to contact us immediately at the following email address: security@highseclabs.com

The security@highseclabs.com email address is not intended to reach technical support on HSL products or services. Any support inquiries should be directed to support@highseclabs.com.

General

Problem: No power - No video output, none of the front panel LEDs is illuminating.

Solutions:

- Check that the power supply is properly connected to the mains socket.
- Check that DC plug is fully inserted into the switch DC jack.
- Check that the device is powered by using optical mouse with visible red light. If power not available – change power supply.

Problem: Channel select LEDs are blinking. Secure KVM Switch does not work.

Solutions: Device anti-tampering system was triggered. Change unit and call HSL technical support.

Problem: KVM does not respond to channel select push buttons. .

Solutions:

If RDC is connected then this is a normal behavior. Control the KVM through the RDC or through keyboard shortcuts.

Video

Problem: No video image in user display (all channels)

Solutions:

- Check that the display is properly powered.
- Check that DVI cable is properly secured at both sides.
- Check at the display on-screen menu that source selected matches the cable connected to the display.
- Check if display video mode is the same as PC (DVI and DVI or VGA and VGA).
- Check that display diagnostic LED is steady green – if not – change display or change display cable or call HSL support.

Problem: No video image in user display (specific channel)

Solutions:

- Reboot the computer.
- Check that the video cable connecting computer and KVM is properly secured at both sides.
- Check that PC video output is sent to the connected video connector (if PC supports multiple displays).
- Check that PC resolution matches connected display capabilities.
- Connect the display directly to the PC to confirm that video output is available and that good image is shown.

Problem: Bad video image quality (some or all channels)

Solutions:

- Check that all video cables are inserted properly to the Switch, computer, and display.
- Check that cables are original cables supplied by HSL.
- With everything connected, power-cycle the KVM Switch to reset the video. Make sure the Video Diagnostic LED is solid green.
- Check that the display that you are using supports the resolution and refresh-rate setting on your computer.
- Lower the video resolution of your PCs.
- Check that the video-cable length does not exceed 15 feet (4.6m).
- Connect the display directly into the computer you are having trouble with to see if the problem still appears

Keyboard

Problem: Keyboard and mouse are not working (two channels)

Solutions:

- Check that computer USB and video cables are not crossed (i.e. computer #1 video connected to KVM port #1 while USB cable is connected to KVM port #2).

Problem: Keyboard does not work (all channels)

Solutions:

- Check that the keyboard you are using is connected properly to the Switch.

- Check that the USB cable between the Switch and the computer is completely connected.
- Try connecting to a different USB port on the computer.
- Make sure the keyboard works when directly plugged into the computer (the HID USB driver is installed on the computer).
- Rebooting may be necessary when trying this.
- Make sure you are not using a wireless keyboard or a keyboard with an integrated USB hub or other USB-integrated devices. These are not supported by the switch due to security policy.
- If the computer is coming out of standby mode, allow up to one minute to regain mouse function.
- Try a different keyboard.

Problem: Keyboard Caps Lock and Num Lock LEDs are not working

Solutions:

This is a normal behavior – HSL Secure KVM Switch blocks all communications from computers to the keyboard to prevent certain potential data leakages.

Problem: Certain keyboard functions are not working

Solutions:

Some non-standard keyboard functions are disabled by the switch to prevent security risks. Contact HSL support for latest compatibility list.

Mouse

Problem: Mouse and keyboard are not working (two channels)

Solutions:

- Check that computer USB and video cables are not crossed (i.e. computer #1 video connected to KVM port #1 while USB cable is connected to KVM port #2).

Problem: Mouse is not working (all channels), keyboard is working.

Solutions:

- Check that keyboard is not plugged into mouse port (and mouse not plugged into keyboard port).

Problem: Mouse does not work (all channels)

Solutions:

- Check that the mouse you are using is connected properly to the Switch.
- Check that the USB cable between the Switch and the computer is completely connected.
- Try connecting to a different USB port on the computer.
- Make sure the mouse works when directly plugged into the computer (the HID USB driver is installed on the computer).
- Rebooting may be necessary when trying this.
- Make sure you are not using a wireless mouse or a mouse with an integrated USB hub or other USB-integrated devices. These are not supported by the switch due to security policy.
- If the computer is coming out of standby mode, allow up to one minute to regain mouse function.
- Try a different mouse.

DPP

Problem: DPP is not working (two channels)

Solutions:

- Check that computer DPP USB and video cables are not crossed (i.e. computer #1 video connected to KVM port #1 while DPP USB cable is connected to KVM DPP port #2).

Problem: DPP is not working (all channels)

Solutions:

- Check that device is properly plugged into the DPP port.
- Check that the DPP status LED indicating steady green. If not illuminated at all the device is not recognized by the switch.

Problem: DPP is not working (one channel only)

Solutions:

- Check that device is working properly when connected directly to the PC.
- Check that there is a DPP USB cable connected between that PC and the required DPP port in the switch.

High Sec Labs Warranty Programs

Hardware Service Coverage

All HSL hardware comes with a two-year, return-to-depot warranty at no extra charge. This limited warranty covers 100% of parts and workmanship on any required repairs. However, repair turnaround times average two weeks, so the purchase of enhanced hardware service coverage is highly recommended for all mission-critical applications. The PREMIUM program provides next day replacement service and 24x7 telephone support. Both of these programs are available in US, Canada and in Europe.

Program	Service Level	Technical Support Hours
STANDARD	Return-to-Depot Repair	Email 24/7, phone 9 am - 5:30 pm , Eastern, Monday to Friday
PREMIUM	Next Day Advance Replacement	24x7

All HSL hardware are designed and tested for at least 10 years of maintenance-free operation. HSL will be pleased to extend your STANDARD warranty for up to 7 years after purchase and to extend PREMIUM warranty for up to 10 years after purchase.

It is beneficial to purchase enhanced coverage at the same time as the hardware. Doing so ensures that the hardware is continuously protected. Although it is possible to obtain enhanced coverage at a later date, such contracts are subject to a blackout period which delays the start of any coverage by 60 days.

High Sec Labs Limited Warranty Terms and Conditions

High Sec Labs warrants that the product you have purchased from High Sec Labs or from an authorized High Sec Labs reseller is free from defects in material and workmanship under normal use during the Limited Warranty period. The warranty period commences on the date of purchase. Your sales receipt showing the date of purchase of the High Sec Labs product is your proof of the date of purchase. This warranty is not transferable to anyone who subsequently purchases the product from you. This Limited Warranty does not include expandable parts.

Never open the product's enclosure and never attempt to replace or fix any internal part! Any attempt to repair the product, install or replace components by an unauthorized person could expose that person to risk electrical shock and will cause the product warranty to be void immediately. Should the product require service during the term of the Limited Warranty, High Sec Labs would provide either mail-in or carry-in service.

High Sec Labs will repair or replace according to its own discretion the defective products or parts with new products or parts. All exchanged parts and products replaced under this warranty will become the property of High Sec Labs.

TO OBTAIN SERVICE UNDER THIS LIMITED WARRANTY for mail-in or carry-in you must return the product, freight prepaid and insured (or assume the risk of loss or damage during shipment) in the original container or an equivalent, to a High Sec Labs Service Center. If the unit was not registered, you should enclose a written receipt for the product, showing the date of purchase,

distributor's or dealer's name from whom you purchased the product, and both the model and serial number of the product. High Sec Labs will pay the return ground shipping charge within the continental United States, Canada and Europe.

Limitations of Remedy

THIS LIMITED WARRANTY COVERS repair or replacement at the discretion of High Sec Labs of the High Sec Labs product device purchased from High Sec Labs. THIS LIMITED WARRANTY DOES NOT COVER losses or damages that occurred as a result of shipping; improper installation or maintenance by anyone other than an authorized representative of High Sec Labs; acts of God or accident; misuse, neglect, or misapplication of the product; installation of options or parts by anyone other than High Sec Labs; exposure to extremes of temperature or humidity; or improper electrical power. Products returned to High Sec Labs for service, in warranty and post warranty that are diagnosed as No Fault Found will be subject to a diagnostic fee.

The Limited Warranty will be void in case of mechanical damage to the product, High voltage electrical pulse or lightning induced damage.

Product may have special Tampering Evident Labels that will provide clear indications if removed or tampered with. This will void High Sec Labs product warranty. Product may also have battery powered active anti-tampering function. Any attempt to remove enclosure screws or to open product enclosure may trigger this function and void product warranty.

This warranty excludes power supply, cables, mouse and adapters purchased with the device.

THIS LIMITED WARRANTY IS IN LIEU OF ALL OTHER WARRANTIES, REMEDIES OR CONDITIONS, WHETHER ORAL OR WRITTEN, EXPRESSED OR IMPLIED. THERE ARE NO WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

HIGH SEC LABS WARRANTY OBLIGATIONS AND BUYER'S REMEDIES ARE EXCLUSIVELY STATED HEREIN. HIGH SEC LABS LIABILITY, WHETHER BASED ON CONTRACT, TORT, WARRANTY, STRICT LIABILITY OR ANY OTHER THEORY, SHALL NOT EXCEED THE PRICE OF THE INDIVIDUAL UNIT WHOSE DEFECT OR DAMAGE IS THE BASIS FOR THE CLAIM. IN NO EVENT SHALL HIGH SEC LABS BE LIABLE FOR ANY SPECIAL OR CONSEQUENTIAL DAMAGES. HIGH SEC LABS SPECIFICALLY DOES NOT REPRESENT THAT IT WILL BE ABLE TO REPAIR ANY PRODUCT UNDER THIS WARRANTY OR MAKE A PRODUCT EXCHANGE WITHOUT RISK TO OR LOSS OF PROGRAMS OR DATA.

U.S.A. State Laws

Some states do not allow limitations on how long an implied warranty lasts, or allow the exclusion or limitation of incidental or consequential damages, so the above limitations may not apply to you. This warranty gives you specific legal rights, and you may also have other rights, which vary from state to state.

Limited Warranty Types

Mail-In Coverage

The Customer will make the initial service request to the High Sec Labs Customer Service. If High Sec Labs determines that a repair is required, the Customer will receive instructions on returning the Product to High Sec Labs. The customer will return the product in its original package or an equivalent. The Customer will pay incoming freight charges and is responsible for any loss or damage

to the Product while it is in transit. Upon completion of the repair, High Sec Labs will return the Product to the Customer, freight prepaid. A copy of your Warranty Certificate must accompany the Product. All non-High Sec Labs Product, accessories, attachments, modifications and all programs, data, and storage media must be removed from the Product before it is mailed in for service. High Sec Labs shall not be responsible for items that are not removed.

Carry-In Coverage

The Customer will make the initial service request to the High Sec Labs Customer Service depending on the product covered. If High Sec Labs determines that a repair is required, the Customer must deliver the Product to a High Sec Labs Authorized Service Provider, make arrangements and pay for the transport of Product to Customer after its repair. A copy of the Customer's Warranty Certificate must accompany the Product. All non-High Sec Labs Product, accessories, attachments, modifications and all programs, data, and storage media must be removed from the Product prior to taking Product to the High Sec Labs Authorized Service Provider. High Sec Labs or High Sec Labs Authorized Service Provider shall not be responsible for items that are not removed or that are damaged before they are received by High Sec Labs or the Service Provider.

Upgrade Commitment on behalf of Customer

In case High Sec Labs discovers some failure in its Software (e.g. Firmware, Operating System, Management Software, Plug-Ins or any other aspect of its Software), the customer might be required to upgrade his software to a specific software version within a reasonable period of time. After the specified time has passed, High Sec Labs will not be held obligated to support the product under its Warranty or Extended Warranty terms and conditions.

High Sec Labs Security Procedures

Reporting HSL Product Vulnerability

If you are aware of potential security vulnerability with any HSL product, we encourage you to contact us immediately at the following email address: security@highseclabs.com or fill out a support form at: http://www.highseclabs.com/support_form.html

After your communication is received, HSL personnel will contact you to follow up. To ensure confidentiality, HSL encourages you to use our PGP encryption key.

The security@highseclabs.com email address is not intended to reach technical support on HSL products or services. Any support inquiries should be directed to support@highseclabs.com or support web-form indicated above.

Responsible Disclosure

Notifying a vendor prior to releasing information publicly about vulnerability is standard practice in the security industry and is known as “responsible disclosure.” This advance notice allows vendors to research and fix vulnerabilities before potential attackers are notified of their existence – keeping the product install base secure. We appreciate your assistance in ensuring that HSL products and services are secure.

Receiving a notification about Product Vulnerability / Solution

HSL security policy and internal system provides quick response in case that product security vulnerability is found. Once product vulnerability is found and confirmed by HSL QA, HSL provides an email to the following list of users based on affected product:

1. All users who registered their product and provided a valid email address.
2. All users who registered for Premium product warranty coverage.
3. All users that reported same security vulnerability.
4. Users that requested information about specific product vulnerability.

Once a solution is found – HSL will send an email to the same distribution list within 24 hours.

COPYRIGHT AND LEGAL NOTICE

© 2011 High Sec Labs Ltd all rights reserved.

This product and/or associated software are protected by copyright, international treaties and various patents.

This manual and the software, firmware and/or hardware described in it are copyrighted. You may not reproduce, transmit, transcribe, store in a retrieval system, or translate into any language or computer language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual, or otherwise, any part of this publication without express written permission from High Sec Labs.

HIGH SEC LABS SHALL NOT BE LIABLE FOR TECHNICAL OR EDITORIAL ERRORS OR OMISSIONS CONTAINED HEREIN; NOR FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES RESULTING FROM THE FURNISHING, PERFORMANCE, OR USE OF THIS MATERIAL.

The information contained in this document represents the current view of High Sec Labs on the issues discussed as of the date of publication. Because High Sec Labs must respond to changing market conditions, it should not be interpreted to be a commitment

on the part of High Sec Labs, and High Sec Labs cannot guarantee the accuracy of any information presented after the date of publication. PRODUCT DESIGN AND SPECIFICATION IS SUBJECT TO CHANGES WITHOUT NOTICE

This Guide is for informational purposes only. HIGH SEC LABS MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

PATENTS AND TRADEMARKS

The products described in this manual are protected by multiple patents.

High Sec Labs, KVM Combiner, and the High Sec Labs logo are either trademarks or registered trademarks of High Sec Labs Ltd.

Products mentioned in this document may be registered trademarks or trademarks of their respective owners

The Energy Star emblem does not represent endorsement of any product or service.

U.S. GOVERNMENT RESTRICTED RIGHTS

The Software and documentation are provided with RESTRICTED RIGHTS.

You agree to comply with all applicable international and national laws that apply to the Software, including the U.S. Export Administration Regulations, as well as end-user, end-use and country destination restrictions issued by U.S. and other governments.

The information and specifications in this document are subject to change without prior notice.

Images are for demonstration purposes only.