High Sec Labs FV11D-3 Secure KVM Isolator User Manual

Contents

High Sec Labs FV11D-3 Secure KVM Isolator

Product Information

Specifications

- Product Name: Secure KVM Isolator
- Model: HDC10352
- Revision: E
- Website: https://manual-hub.com/

Introduction

The Secure KVM Isolator is a device designed to provide secure isolation for keyboards, video monitors, and mice (KVM) connections. It ensures protection against potential security vulnerabilities during installation and operation.

Intended Audience

This user manual is intended for the following professionals:

- System Administrators/IT Managers
- End Users

Package Contents

The product packaging includes the following items:

- Secure KVM Isolator unit
- User Manual

Safety Precautions

Please read and follow these safety precautions before using the product:

- Avoid exposing the product to liquids or excessive moisture.
- If the product is not functioning properly, even after following the instructions, contact technical support.
- Do not use the product if it has been dropped or physically damaged.
- Do not use the product if it shows signs of breakage, overheating, or has a damaged cable.

User Guidance & Precautions

Please follow these user guidance and precautions when using the product:

1. During power-up, the product performs a self-test. If the self-test fails, the product will be inoperable. Contact your system administrator or technical support for assistance.
2. Restoring the product to factory defaults will erase all user-set definitions, except for administrator credentials. This can be done through the menu option in terminal mode. Refer to theAdministrator Manual for more details.
3. For security reasons, do not connect any wireless keyboard or mouse to the product.
4. The product does not support microphone/line-in audio input. Do not connect a microphone to the product's audio output port.

FAQ

Q: What should I do if I encounter a self-test failure during power-up?
A: If the self-test fails, try power cycling the product. If the problem persists, please contact your system administrator or technical support.

Q: Can I restore the product to factory defaults?
A: Yes, the product can be restored to factory defaults through a menu option in terminal mode. Please refer to the Administrator Manual for detailed instructions.

Q: Can I connect a wireless keyboard or mouse to the product?
A: No, for security reasons, it is not recommended to connect any wireless keyboard or mouse to the product.

Q: Does the product support microphone/line-in audio input?
A: No, the product does not support microphone/line-in audio input. Do not connect a microphone to the product's audio output port, including headsets.

Rev: E
Doc No.: HDC10352

- FV11D-3 – HSL Secure Isolator 1-Port Video DVI-I, PP 3.0
- FV11P-3 – HSL Secure Isolator 1-Port Video DisplayPort, PP 3.0
- FV11H-3 – HSL Secure Isolator 1-Port Video HDMI, PP 3.0
- FI11D-3 – HSL Secure 1-Port KVM Isolator DVI-I, PP 3.0
- FI11P-3 – HSL Secure 1-Port KVM Isolator DisplayPort, PP 3.0
- FI11H-3 – HSL Secure 1-Port KVM Isolator HDMI, PP 3.0

Introduction

Thank you for purchasing this High Sec Labs (HSL) Secure product designed for use in secure defense and intelligence installations.
The product offers safe centralized control, which prevents unintended data transfer between computers and peripherals running at different security levels.
The product provides the highest security safeguards and features that meet today's IA (information assurance) computing requirements as defined in the latest PSS Protection Profile Rev 3.0.
This User Manual provides all the details you'll need to install and operate your new product.

Intended Audience
This document is intended for the following professionals:

- System Administrators/IT Managers

- End Users

Package Contents

Inside product packaging you will find the following:

- HSL Secure KVM Isolator
- Power Supply
- User Manual

Revision

- **A –** Initial Release, 20 Feb 2015
- **B –** Corrections, 5 April 2015
- **C –** Rev change, 12 May 2015
- **D –** User Guidance updates, 21 June 2015
- **E –** Correction to Features section, 13 August 2015

Important Security Note:
If you are aware of potential security vulnerabilities while installing or operating this product, we encourage you to contact us immediately in one of the following ways:

- Web form: **http://www.highseclabs.com/support/case/**
- Email: **security@highseclabs.com**
- Tel: +972-4-9591191 or +972-4-9591192

Important: This product is equipped with the always-on active antitampering system. Any attempt to open the product enclosure will activate the anti-tamper triggers and render the unit inoperable and warranty void.

Operation

Safety Precautions

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

- Before cleaning, disconnect the product from any electrical power supply.
- Do not expose the product to excessive humidity or moisture.
- Do not store or use for extensive period of time in extreme thermal conditions – it may shorten product lifetime.
- Install the product only on a clean secure surface.
- If the product is not used for a long period of time, disconnect it from electrical power.
- If any of the following situations occurs, have the product checked by an HSL qualified service technician:
    - Liquid penetrates the product's case.
    - The product is exposed to excessive moisture, water or any other liquid.
    - 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 shows obvious signs of breakage or loose internal parts.

    - In case of external power supply – If power supply overheats, is broken or damaged, or has a damaged cable.
- The product should be stored and used only in temperature and humidity controlled environments as defined in the product’s environmental specifications.
- Never attempt to open the product enclosure. Any attempt to open the enclosure will permanently damage the product.
- The product contains a non-replaceable internal battery. Never attempt to replace the battery or open the enclosure.
- 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 and warranty void.

User Guidance & Precautions

Please read the following User Guidance & Precautions carefully before using the product:

1. As product powers-up it performs a self-test process. In case of self- test failure for any reason, the product will be Inoperable. Self-test success will be indicated by the illumination of the green Power/Self-test LED. In case of self-test failure this LED will be blinking.
   In case of a self-test failure, try to power cycle product. If problem persists please contact your system administrator or technical support.
2. Product behavior after performing Restore to Factory Defaults (RFD):
   - Product Restore-to-Factory-Default (RFD) function is available via a menu option in terminal mode. For more details refer to the Administrator Manual.
   - RFD action will be indicated by front and rear panel LEDs blinking all together.
   - When product boots after RFD all default settings will be restored, erasing all user-set definitions (except for administrator credentials).
3. For security reasons do not connect to the product any wireless keyboard or mouse.
4. For security reasons product does not support microphone/line-in audio input. In any case do not connect a microphone to product audio output port, including headsets.
5. Product is equipped with always-on active anti-tampering system. Any attempt to open product enclosure will activate the anti-tamper system indicated by front / rear panel LEDs blinking continuously. In this case, product will be inoperable and warranty void. If product enclosure appears disrupted or if all LEDs are blinking continuously, please remove product from service immediately and contact technical support.
6. In case a connected device is rejected in the console port group the user will have the following indications:
   - When connecting a non-qualified keyboard, the keyboard will be non-functional with no visible keyboard strokes on. In addition to that, the KB status LED will be blinking.
   - When connecting a non-qualified mouse, the mouse will be non-functional with mouse cursor frozen on screen and the mouse status LED will be blinking.
   - When connecting a non-qualified display, the video diagnostic LED will be blinking and the connected display would not show video.
7. Do not connect product to computing devices:
   - That are TEMPEST computers;
   - That include telecommunication equipment;
   - That include frame grabber video cards;

- That include special audio processing cards.

8. Product log access and administrator configuration options are described in product Administrator Guide.
9. If you are aware of any potential security vulnerability while installing or operating product, please remove product from service immediately and contact us in one of the ways listed in this manual.

Main Features

Product is designed, manufactured and delivered in securitycontrolled environments. Below is a summary of the main advanced features incorporated in product:
Advanced isolation between computers and shared peripherals
The emulations of keyboard, mouse and display EDID, prevent direct contact between the connected computer and shared peripherals.
Product design achieves maximal security by keeping the video path separate with keyboard and mouse. All these features contribute to strong isolation between computer interfaces, maintained even when product is powered off.

Unidirectional data flow: USB, audio and video
Unique hardware architecture components prevent unauthorized data flow, including:

- Optical unidirectional data flow diodes in the USB data path that filtrate and reject unqualified USB devices;
- Secure analog audio diodes that prevent audio eavesdropping with no support for microphone or any other audio-input device;
- Video path is kept separate from all other traffic, enforcing unidirectional native video flow. EDID emulation is done at power up and blocks all EDID/MCCS writes. For DisplayPort video, filtration of AUX channel exists to reject unauthorized transactions.

Isolation of power domains
Complete isolation of power domains prevents signaling attacks.

Secure administrator access & log functions
Product incorporates secure administrator access and log functions to provide auditable trail for all product security events, including battery backup life for anti-tampering and log functions. Nonreprogrammable firmware prevents the ability to tamper with product logic.

Always-on, active anti-tamper system
Active anti-tampering system prevents malicious insertion of hardware implant such as wireless key-logger inside product enclosure. Any anti-tampering attempt causes isolation of all computers and peripheral devices rendering product inoperable and showing clear indications of tampering event to user.
Holographic security tamper-evident labels are placed on the enclosure to provide a clear visual indication if product has been opened or compromised.
Metal enclosure is designed to resist mechanical tampering with all microcontrollers protected against firmware-read, modification and rewrite.

USB Support
The isolator is compatible with USB technology and supports plugand- play connectivity with USB computers, keyboards, and mice.

Video Support

- FV11D-3/FI11D-3 support DVI-I displays as well as VGA and HDMI via compatible cables.
- FV11P-3/FI11P-3/FV11H-3 and FI11H-3 support HDMI displays.

Resolutions Supported

Switches support video resolutions of up to 4K-2K Ultra HD (3840 X 2160 pixels).

Tamper Evident Labels

HSL Secure KVM Isolator uses holographic tamper evident labels to provide visual indications in case of enclosure intrusion attempt.
When opening product packaging inspect the 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 Technical Support and avoid using that product.

Active Anti-Tampering System

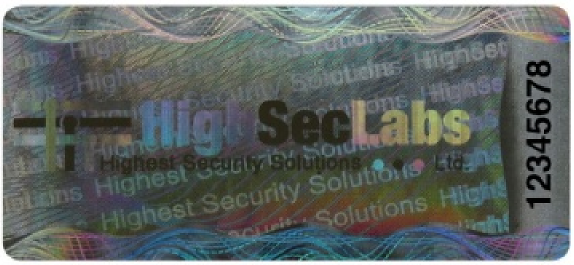
HSL Secure KVM Isolator is equipped with always-on active antitampering system. If mechanical intrusion is detected by this system, the Switch will be permanently disabled and LED will blink continuously.
If product indication tampered state (all LEDs blinking) – please call Technical Support and avoid using that product.

Product Enclosure Warning Label

HSL Secure KVM Isolator has the following warning sticker on a prominent location on the product enclosure:

WARNING!

Product protected by Anti-Tamper system. Do not Attempt to remove screws, open enclosure, or tamper with product in any way. Any attempt to tamper with product may cause permanent damage.



HSL Tamper Evident Label

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 and warranty void.

Equipment Requirements

Cables

It is highly recommended to use HSL Cable Kits for product to ensure optimal security and performance.
One Cable Kit is required per connected computer.

Operating Systems

Product is compatible with devices running on the following operating systems:

- Microsoft® Windows®
- Red Hat®, Ubuntu® and other Linux® platforms
- Mac OS® X v10.3 and higher.

USB Keyboard console port

The product USB keyboard port is compatible with Standard USB keyboards.

Notes:

- Product USB keyboard and mouse ports are switchable, i.e. you can connect keyboard to mouse port and vice versa. However, for optimal operation it is recommended to connect USB keyboard to console USB keyboard port and USB mouse to console USB mouse port.
- For security reasons products do not support wireless keyboards. In any case do not connect wireless keyboard to product.
- Non-standard keyboards, such as keyboards with integrated USB hubs and other USB-integrated devices, may not be fully supported due to security policy. If they are supported, only classical keyboard (HID) operation will be functional. It is recommended to use standard USB keyboards.

USB Mouse console port
The product USB mouse port is compatible with standard USB mice.

Notes:

- Product USB keyboard and mouse ports are switchable, i.e. you can connect keyboard to mouse port and vice versa. However, for optimal operation it is recommended to connect USB keyboard to console USB keyboard port and USB mouse to console USB mouse port.
- Console USB mouse port supports Standard KVM Extender composite device having a keyboard/mouse functions.
- For security reasons products do not support wireless mice. In any case do not connect wireless mouse to product.

Video Support

- FV11D-3/FI11D-3 support DVI-I displays as well as VGA and HDMI via compatible cables.
- FV11P-3/FI11P-3/FV11H/FI11H support HDMI displays.

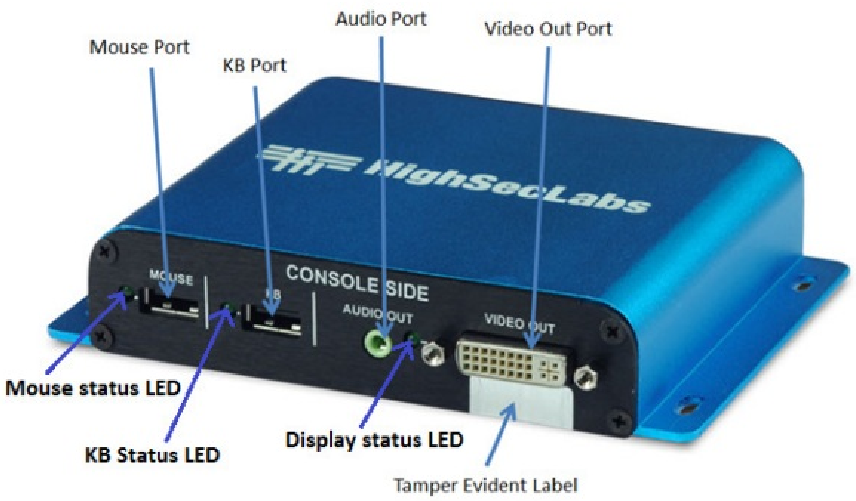
Resolutions Supported
Switches support video resolutions of up to 4K-2K Ultra HD (3840 X 2160 pixels).

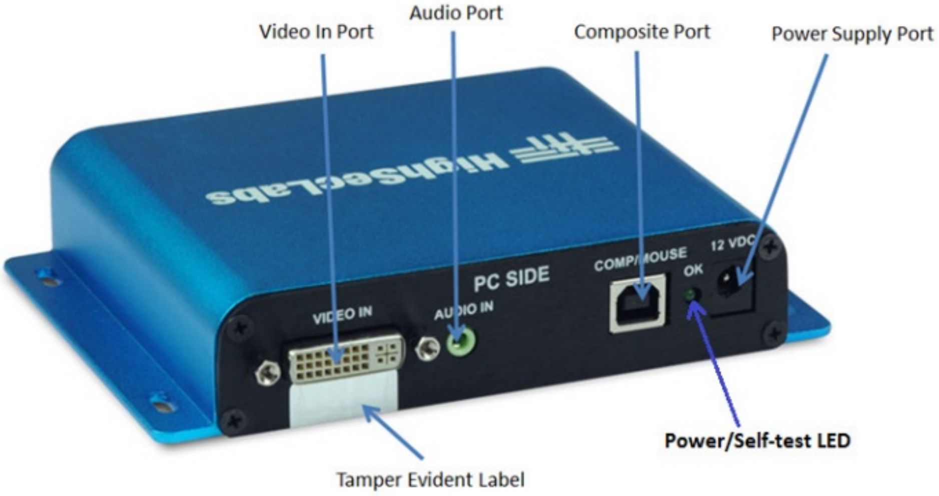
User Audio Devices
Product is compatible with the following types of user audio devices:

- Stereo headphones;
- Amplified stereo speakers.

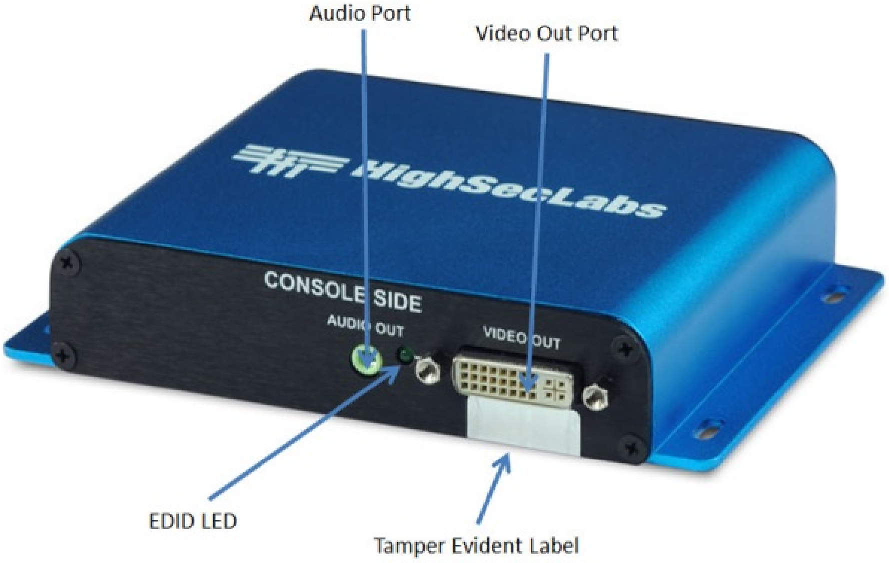
Note: In any case do not connect a microphone or headset to the product audio output port.

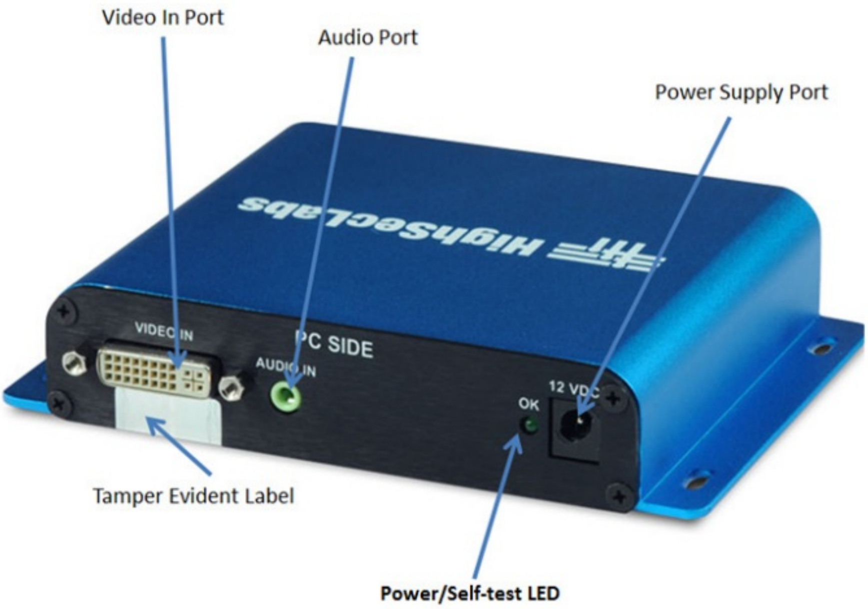
Front Panel Features – FI11D-3



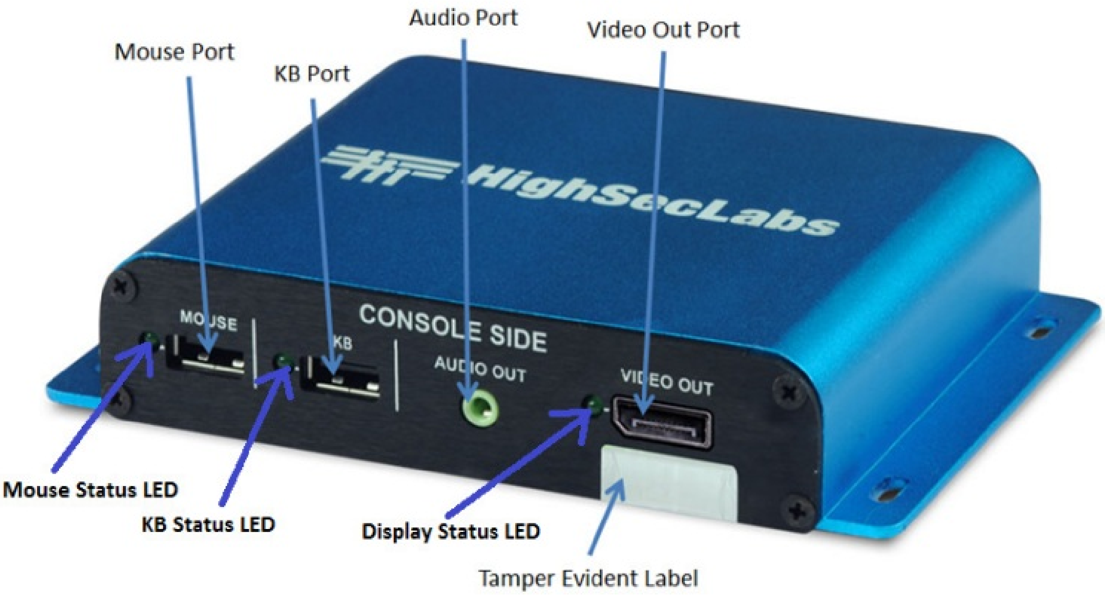


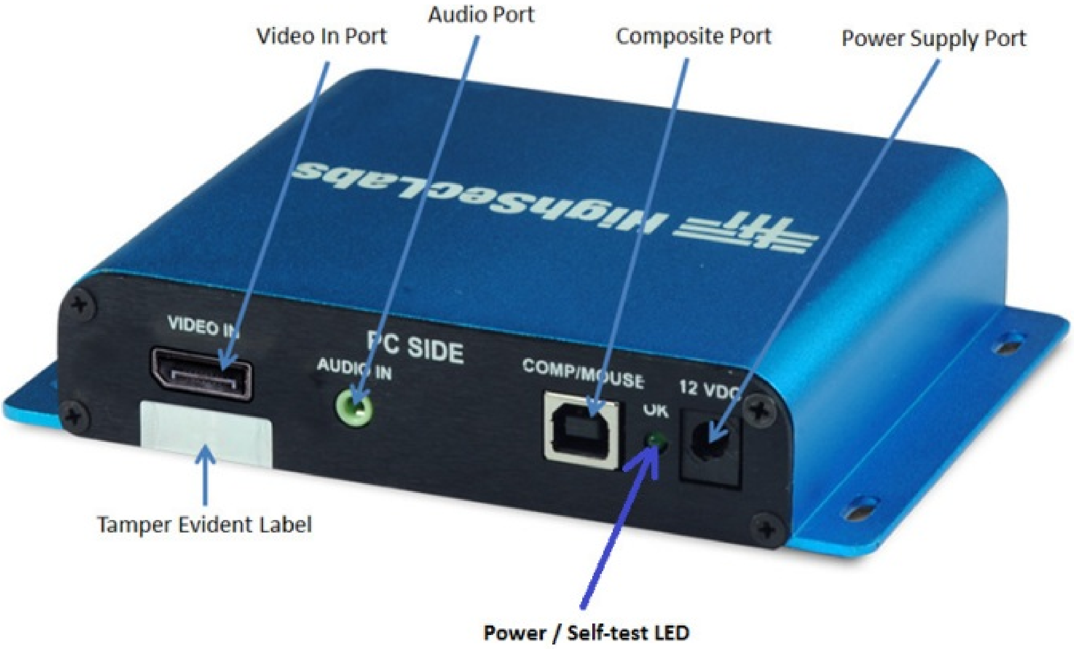
Front Panel Features – FV11D-3



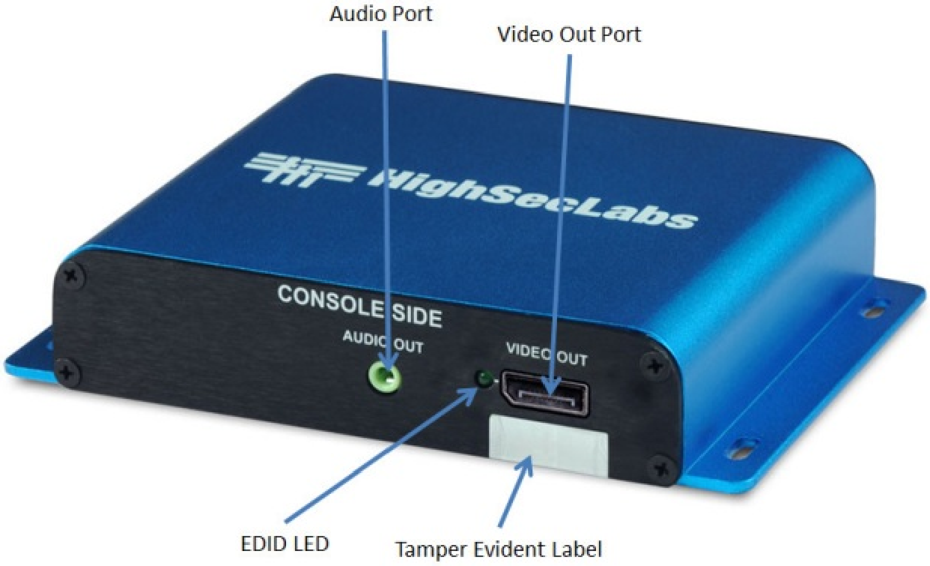


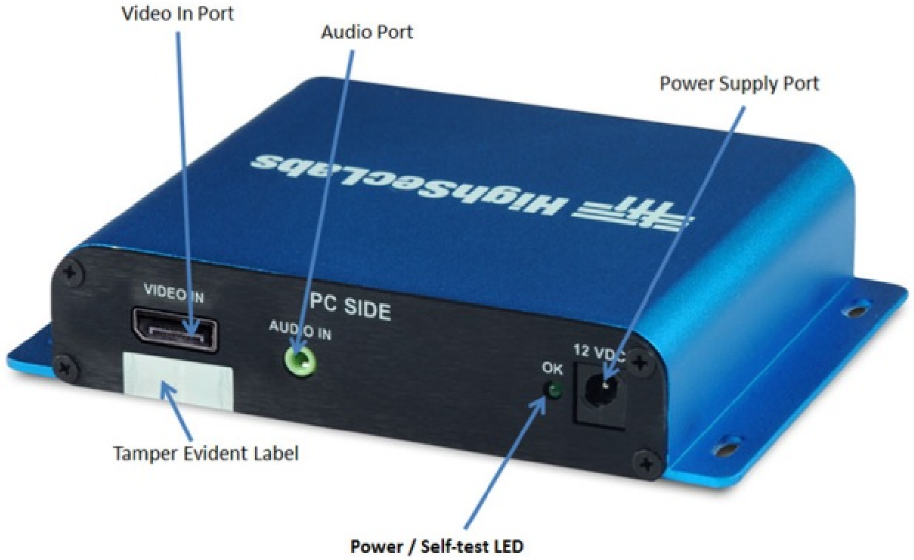
Front Panel Features – FI11P-3/FI11H-3





Front Panel Features – FV11P-3/FV11H-3





Product Specifications

- Enclosure: Extruded aluminum metal enclosure
- Power Requirements: DC input 12V / 1A maximum.
- Power Supply: Power input 90-240V AC
- Console Keyboard Input: USB Type-A female connector
- Console Mouse Input: USB Type-A female connector
- Resolution Support up to 4K-2K Ultra HD (3840 X 2160 pixels) resolutions
- Console Display Port DVI-I female connector (Fx11D-3)
- HDMI female connector (Fx11P-3 and Fx11H-3)
- Console Audio input jack: 1/8″ (3.5mm) stereo female jack
- Computer Keyboard/Mouse port: USB Type B
- Computer Audio Input plug: 1/8″ (3.5mm) stereo plug
- Computer Video Input plug:
  - 1 x DVI-I video port (FV11D-3)
  - 1 x DisplayPort video port (FV11P-3)
  - 1 x HDMI video port (FV11H-3)
- Operating Temp: 32° to 104° F (0° to 40° C)
- Storage Temp: -4° to 140° F (-20° to 60° C)
- Humidity: 0-80% RH, non-condensing
- Product design life-cycle: 10 years
- Warranty: 2 years

Before Installation

Unpacking the Product

Before opening the product packaging, inspect the packaging condition to assure that product was not damaged during delivery.
When opening the package, inspect that the product Tamper Evident Labels are intact.

Important:

1. If the unit's enclosure appears disrupted or if all channel select LEDs flash continuously, please remove product from service immediately and contact HSL Technical Support at **http://highseclabs.com/support/case/**.
2. Do not connect product to computing devices:
   - That are TEMPEST computers;
   - That include telecommunication equipment;
   - That include frame grabber video cards
   - That include special audio processing cards.

Where to locate the Product?

The enclosure of the product 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.

Consider the following when deciding where to place product:

- The location of the computers in relation to the product and the length of available cables (typically 1.8 m)

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

Installation

Step 1 Connecting the Console devices to product
Product requires connection of all devices and computers prior to powering it up.

Note: some devices such as user display would not be recognized if connected after product is already powered up.

See figures above for connector locations.

- Connect user display, keyboard and mouse.
- Connect headphones/speakers to console audio out port (optional).

Notes:

1. Console USB keyboard and mouse ports are switchable, i.e. you can connect keyboard to mouse port and vice versa. However, for optimal operation it is recommended to connect USB keyboard to console USB keyboard port and USB mouse to console USB mouse port.
2. For security reasons do not connect wireless keyboard or mouse to the product.
3. Non-standard keyboards, such as keyboards with integrated USB hubs and other USB-integrated devices, may not be fully supported due to security policy. If they are supported, only classical keyboard (HID) operation will be functional. It is recommended to use standard USB keyboards.
4. Console USB mouse port supports Standard KVM Extender composite device having a keyboard/mouse functions.
5. In any case do not connect a microphone to the switch audio output port, including headsets.

Step 2 Connecting the Computers
Connect the computers to the Secure KVM Isolator through the following steps:

- Connect each computer with KVM cable. USB cable can be connected to any free USB port on 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 and then connect via the KVM Isolator.
  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 to the computer audio output (lime green color) or line output (blue color) jacks.

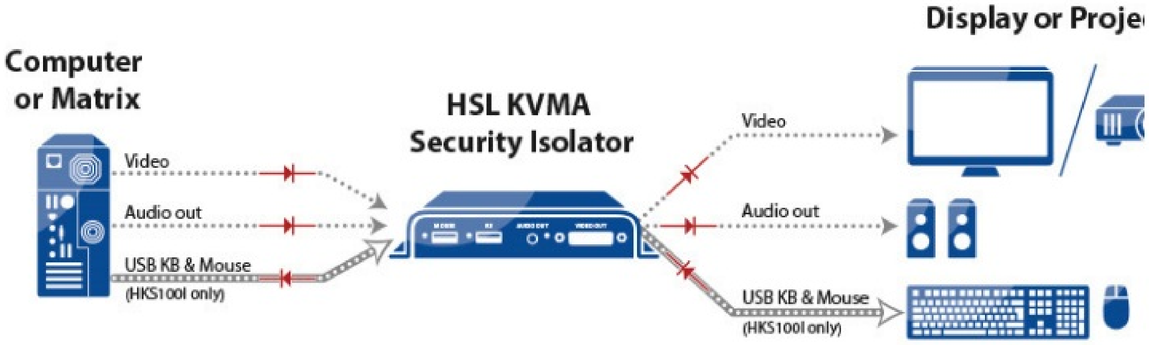
Step 3 Power up

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

- Keyboard and mouse status LEDs should illuminate few seconds after power up to indicate that connected peripherals are accepted. In case of status LED blinking – device was rejected.
  Disconnect the rejected device and replace with another one.

Note: When you power on your computer, the Isolator emulates both a mouse and keyboard to the connected PC and allows your computer to boot normally. Check to see that the keyboard, display, and mouse are working normally.

Typical system installation



Troubleshooting

Troubleshooting Guide

Important Security Note:
If you are aware of potential security vulnerability while installing or operating this product, we encourage you to contact us immediately in one of the following ways:

- Web form: http://www.highseclabs.com/support/case/
- Email: security@highseclabs.com
- Tel: +972-4-9591191 or +972-4-9591192

Important: If the unit's enclosure appears disrupted or if all LEDs are continuously blinking, please remove product from service immediately and contact HSL Technical Support at http://www.highseclabs.com/support/case/

Important: This product is equipped with always-on active antitampering system. Any attempt to open the product enclosure
will activate the anti-tamper triggers and render the unit inoperable and warranty void.

General

Problem: After product powers-up the green Power / Self-test LED is blinking or off. Product is inoperable.
Solution: The product did not pass self-test procedure. Try to power cycle product. If problem persists please contact your system administrator or our technical support.
Problem: No power – No video output, none of the front panel LEDs are illuminating.

Solutions:

- Check DC power source connection to make sure product receives power properly. Replace power-supply if needed. If problem persists, contact your system administrator or our technical support.

Problem: Product enclosure appears disrupted or all LEDs are continuously blinking.

Solution: The product may have been tampered with. Please remove product from service immediately and contact Technical Support.

Keyboard
Problem: Mouse and keyboard are not working
Solutions:
• Check that computer USB and video cables are properly connected to the required computer.

Problem: Keyboard does not work

Solutions:

- Check that the keyboard you are using is properly connected to product.
- Check that the USB cable between the product and computer is properly connected.
- Try connecting keyboard to a different USB port on computer.
- Make sure the keyboard works when directly connected to computer, i.e. the HID USB driver is installed on computer; this may require computer reboot.
- It is recommended to use standard USB keyboards and not a keyboard with an integrated USB hub or other USBintegrated devices.
- If the computer is coming out of standby mode, allow up to one minute to regain mouse function.
- Try a different keyboard.
- Do not use a wireless keyboard.

Mouse

Problem: Mouse and keyboard are not working
Solutions:

- Check that computer USB and video cables are properly connected.

Problem: Mouse does not work
Solutions:

- Check that the mouse you are using is properly connected to product.
- Check that USB cable between the product and computer is properly connected.
- Try connecting mouse to a different USB port on computer.
- Make sure the mouse works when directly connected to computer, i.e. the HID USB driver is installed on computer; this may require computer reboot.
- It is recommended to use standard USB mice.
- If the computer is coming out of standby mode, allow up to one minute to regain mouse function.
- Try a different mouse.
- Do not use a wireless mouse.

Problem: both keyboard and mouse are still not working
Solution: Use computer Device Manager Utility to see product and solve problem.

Video

Problem: No video image in user display
Solutions:

- Check that display is properly powered.
- Check that video cable is properly secured at both sides.
- Check at the displays' on-screen menu that sources selected match the cables connected to displays.
- Check if display video mode is the same as computer's video mode (e.g. DVI and DVI, etc.).
- Check that displays' status LED is steady green – if not, change displays, change displays' cables or call technical support.

Problem: Still no video image in user display
Solutions:

- Reboot product first, then disconnect and reconnect the video cable and reboot the computer.
- Check that the video cable connecting computer and product is properly secured at both sides.
- Check that computer video output is sent to the connected video connector (if computer supports multiple displays).
- Check that computer resolution matches connected display capabilities.
- Connect the display/s directly to the computer to confirm that video output is available and that a good image is shown.

Problem: Bad video image quality
Solutions:

- Check that video cables are properly connected to product, computer, and display.
- Check that cables are original cables supplied by HSL.
- With everything connected, power-cycle the product to reset the video. Make sure the display status LED is solid green.
- Check that the displays that you are using support the resolution and refresh-rate setting on computer.
- Lower the video resolution of your computer.
- Connect displays directly to computer showing bad video image to see if problem persists.

COPYRIGHT AND LEGAL NOTICE

HSL 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 HSL on the issues discussed as of the

date of publication.
Because HSL must respond to changing market conditions, it should not be interpreted to be a commitment on the part of HSL, and HSL 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. HSL MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

PATENTS AND TRADEMARKS
The products described in this manual are protected by multiple patents.
HSL Product/s and logo are either trademarks or registered trademarks of HSL.
Products mentioned in this document may be registered trademarks or trademarks of their respective owners

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.

Documents / Resources

 HighSecLabs Highest Security Solutions Ltd. Secure KVM Isolator User Manual • FV11D-3 - HSL Secure Isolator 1-Port Video DVI-I, PP 3.0 • FV11P-3 - HSL Secure Isolator 1-Port Video DisplayPort, PP 3.0 • FV11H-3 - HSL Secure Isolator 1-Port Video HDMI, PP 3.0 • FI11D-3 - HSL Secure 1-Port KVM Isolator DVI-I, PP 3.0 • FI11P-3 - HSL Secure 1-Port KVM Isolator DisplayPort, PP 3.0 • FI11H-3 - HSL Secure 1-Port KVM Isolator HDMI, PP 3.0 Rev: E Doc No.: HDC10952 1 Secure KVM Isolator User Manual	High Sec Labs FV11D-3 Secure KVM Isolator [pdf] User Manual FV11D-3 Secure KVM Isolator, FV11D-3, Secure KVM Isolator, KVM Isolator, Isolator

References

- Submit Support Case - HighSecLabs
- Submit Support Case - HighSecLabs
- Manual-Hub.com - Free PDF manuals!
- User Manual