



Quick Installation Guide

2/4/8 Ports High Security KM Switches

Introduction

Thank you for purchasing this HSL Secure KM Switch. This KM Switch is designed for use in secure defense and intelligence environments across wide security gaps.

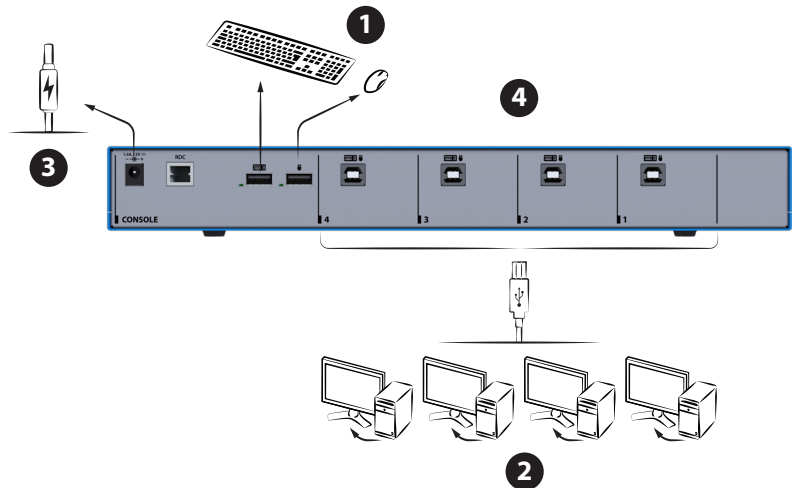
Objectives

- This guide includes instructions for installing and basic operation of HSL's Secure KM Switch **SM20N-4**, **SM40N-4**, **SM80N-4** devices.
- For further assistance please refer to HSL website: <http://www.highseclabs.com>
- The following diagram references the **SM40N-4** device but it is applicable to all devices specified in this manual.

SM40N-4 Model is shown

Rear Panel Index:

1. HID - Console Keyboard/Mouse
2. PC Keyboard/Mouse inputs
3. Power DC in
4. Remote Desktop Control port (for AFP)



Installation Precautions:

- Do not connect this product to computing devices that:
 - Are TEMPEST computers
 - Include telecommunication equipment

WARNING: Peripherals' Warning - For security reasons, this product does not support wireless keyboards. It is recommended not to connect a microphone or headset to the audio output port.

NOTE: In order to comply with the product's Common Criteria evaluation and to prevent unauthorized administrative access to the product, the default administrator username and password must be changed prior to first product use.

Installation:

- Verify that all computers are turned OFF prior to connecting them to the product.
- Connect the computers and peripherals to the HSL KM as shown in the above diagram.
- It is possible to connect an HSL AFP (remote control) to the RDC port of these devices. Please refer to the AFP datasheet on how to connect it.
- Computer Video Connection Directly connect a display to each PC. Multi-Monitor computers might require driver installation (currently available only for Windows <http://highseclabs.com/dl.phpfid=446>).

- **Power ON the PCs:** Make sure that the PCs are turned ON prior to powering ON the KM.
- **Power ON the system:** Power ON the KM by plugging it to the DC wall outlet. By default, after product power-up, the active channel will be computer #1, indicated by the applicable front panel push button LED lit.

Using the HSL KVM Switch:

Control of the HSL KVM Switch is done, primarily using the push buttons on the product front panel.

Switch between computers by pressing the corresponding front panel button on the KM. The front panel button of the selected computer will illuminate.

Important Notes:

1. **Anti-Tampering System:** This HSL high security product is equipped with an always-on active anti-tampering system. If mechanical intrusion is detected, the product is permanently disabled and abnormal LED behavior is activated, with all LEDs blinking continuously.
2. **Power ON Self-Test Procedure:** As the product powers-up, it performs a self-test procedure. In case of self-test failure for any reason, including jammed buttons, the product is inoperable and self-test failure is indicated by abnormal LED behavior.

In the above-mentioned cases, please call Technical Support and avoid using the product. For further information please refer to the product administrator and setup guides.



Front Panel LEDs :

1. Active PC channel LED
2. Keyboard LEDs Num/CAPS/SCRL

KM LED Indications:

HID LED:

- Off – no device detected
- Flicker – device rejected
- On- device approved

Keyboard LEDs:

- Each LED is ON when the associated keyboard lock of the active channel is turned ON

Safety and Regulatory Statements

Safety Symbols

This One or more of the following symbols may be included in your product documentation and/or on the product.



Instructions: This symbol is intended to alert the user to the presence of important operating and maintenance (servicing) instructions in the product user manual.



Dangerous Voltage: This symbol is intended to alert the user to the presence of uninsulated dangerous voltage within the product's enclosure that may be of sufficient magnitude to constitute a risk of electric shock to persons.



Power On: This symbol indicates the principal on/off switch is in the ON position.



Power Off: This symbol indicates the principal on/off switch is in the OFF position.



Protective Grounding Terminal: This symbol indicates a terminal which must be connected to earth ground prior to making any other connections to the equipment.

Safety Precautions

WARNING: To avoid a potentially fatal shock hazard and possible damage to equipment, please observe the following precautions.

- **Instructions:** Do not disable the power grounding plug. The grounding plug is an important safety feature.
- Plug the power cord into a grounded (earthed) outlet that is easily accessible at all times.
- Disconnect the power from the product by unplugging the power cord from either the electrical outlet or the product. The AC inlet is the main disconnect for removing power to this product. For products that have more than one AC inlet, to remove power completely, all AC line cords must be disconnected.
- This product has no serviceable parts inside the product enclosure. Do not open or remove product cover.

CAUTION: Some HSL products contain a lithium battery. This battery is not a field replaceable item, and replacement should not be attempted by a user. If errors occur when using the product and the battery is suspected, contact HSL Technical Support.

WARNING: For Service Personnel Only - There is a risk of explosion if the battery is replaced with an incorrect type. Dispose of used batteries according to the manufacturer's instructions.

This product is for use with other products that are Listed or Certified by a Nationally Recognized Testing Laboratory (NRTL).

NIAP Protection Profile

This product is certified to the NIAP Protection Profile PSD version 4.0 certification for peripheral sharing switch devices.

Security Vulnerability

If you are aware of a potential security vulnerability while installing this product, contact Technical Support immediately by:

- Web form: www.highseclabs.com/support/case/
- Email: security@highseclabs.com
- Tel: +972-4-9591191/2

CAUTION: Anti-tamper Caution - This product is equipped with an always-on, active anti-tampering system. Any attempt to open the product enclosure will activate the anti-tamper triggers, rendering the unit inoperable and voiding its warranty.

WARNING: Unit Enclosure Warning - If the unit's enclosure appears disrupted or if all LEDs flash continuously, remove the product from service immediately and contact Technical Support.

Change Management

For change management tracking, perform a quarterly log check to verify that the RFD was not improperly used to override the current device policy by an unauthorized person.