



## Products covered by this manual - Secure KMs:

- SCKM180 (8 port KM)
- SCKM185 (8 port KM and DPP)

Rev: G  
Doc No.: HDC11607

## Table of Contents

Table of Contents .....	2
Introduction .....	3
Intended Audience.....	3
.....	3
What is a KM (Keyboard / Mouse) Switch? .....	3
Package Contents .....	3
Revision.....	3
Overview .....	4
Safety Precautions .....	4
Safety Precautions (French).....	5
User Guidance & Precautions.....	6
Main Features.....	8
Tamper Evident Labels .....	10
Active Anti-Tampering System .....	10
Product Enclosure Warning Label .....	10
What is Virtual Display Technology (VDT) .....	11
Equipment Requirements.....	12
Front Panel Features .....	14
Rear Panel Features.....	15
.....	15
Product Specifications .....	16
Before Installation.....	18
Installation .....	19
Typical system installation.....	21
Operational Setup.....	22
Other Settings .....	25
Driver Installation.....	26
Operating the Vertiv KM Switch .....	26
Troubleshooting Guide .....	29
Copyright and Legal Notice.....	32

### Introduction

Thank you for purchasing this Vertiv Secure product designed for use in secure defense and intelligence installations. 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

#### **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:

- Email: [Secure@VertivCo.com](mailto:Secure@VertivCo.com)
- Tel: +1-888-793-8763

**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.

### What is a KM (Keyboard / Mouse) Switch?

Vertiv Secure KM products are a derivative of the company's high profile KVMs. While KVMs control Keyboard, Mouse and Video, the KMs controls only Keyboard and Mouse with all displays connected directly to computers. It is suitable for users that need to simultaneously monitor multiple displays and easily interact with multiple sources.

### Package Contents

Inside product packaging you will find the following:

- Vertiv Secure KM Product
- AC Power Cord
- User Guidance Documentation

### Revision

- A – Initial Release, 24 Feb 2015
- B – Corrections, 29 March 2015
- C – Product image updates, 25 May 2015
- D – User Guidance updates, 21 June 2015
- E – Correction to Features section, 24 September 2015
- F – Updated for PP 3 Review, January 28, 2016
- G – Changing to VERTIV new branding, 20 May 2019

#### **Important note before deploying the product:**

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

Refer to the product Administrator Guide for further details.

### Overview

#### 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 a 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.

### Safety Precautions (French)

Veillez lire attentivement les précautions de sécurité suivantes avant d'utiliser le produit:

- Avant nettoyage, débranchez l'appareil de l'alimentation DC / AC.
- Assurez-vous de ne pas exposer l'appareil à une humidité excessive.
- Assurez-vous d'installer l'appareil sur une surface sécurisée propre.
- Ne placez pas le cordon d'alimentation DC en travers d'un passage.
- Si l'appareil n'est pas utilisé de longtemps, retirez l'alimentation murale de la prise électrique.
- L'appareil devra être rangé uniquement dans des environnements à humidité et température contrôlées comme défini dans les caractéristiques environnementales du produit.
- L'alimentation murale utilisée avec cet appareil devra être du modèle fourni par le fabricant ou un équivalent certifié fourni par le fabricant ou fournisseur de service autorisé.
- Si une des situations suivantes survenait, faites vérifier l'appareil par un technicien de maintenance qualifié:
  - En cas d'alimentation externe - L'alimentation de l'appareil surchauffe, est endommagée, cassée ou dégage de la fumée
  - ou provoque des court circuits de la prise du secteur.
  - Un liquide a pénétré dans le boîtier de l'appareil.
  - L'appareil est exposé à de l'humidité excessive ou à l'eau.
  - L'appareil ne fonctionne pas correctement même après avoir suivi attentivement les instructions contenues dans ce guide de l'utilisateur.
  - L'appareil est tombé ou est physiquement endommagé.
  - L'appareil présente des signes évidents de pièce interne cassée ou desserrée
  - L'appareil contient une batterie interne. La batterie n'est pas remplaçable. N'essayez jamais de remplacer la batterie car toute tentative d'ouvrir le boîtier de l'appareil entraînerait des dommages permanents à l'appareil.
  - Ce produit est équipé d'un système anti-sabotage actif. Toute tentative d'ouvrir le boîtier du produit va activer le déclencheur anti-sabotage et de rendre l'unité inutilisable et garantie.

### 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 procedure. In case of self- test failure for any reason, including jammed buttons, the product will be Inoperable. Self-test failure will be indicated by the following abnormal LED behavior:
  - a. All channel-select LEDs will be turned ON and then OFF;
  - b. A specific, predefined LED combination will be turned ON;
  - c. The predefined LED combination will indicate the problem type (jammed buttons, firmware integrity).Try to power cycle product. If problem persists please contact your system administrator or technical support.
2. Product power-up and RFD behavior:
  - a. By default, after product power-up, the active channel will be computer #1, indicated by the applicable front panel push button LED lit.
  - b. Product Restore-to-Factory-Default (RFD) function is available via a physical control button on rear panel. Use a sharp object or paper clip to hold RFD button pressed for several seconds to initiate an RFD action.
  - c. RFD action will be indicated by front panel LEDs blinking all together.
  - d. When product boots after RFD, keyboard and mouse will be mapped to the active channel #1 and default settings will be restored, erasing all user-set definitions except for administrator credentials and log information.
  - e. After RFD, the product will revert to FDF (Fixed Device Filtration) restrictive DPP mode – in this mode enables only smart-card reader USB devices to connect to the product.
3. The appropriate usage of peripherals (e.g. keyboard, mouse, display, authentication device) is described in detail in this User Manual's appropriate sections. Do not connect any authentication device with an external power source to product.
4. For security reasons products do not support wireless keyboards and mice. In any case do not connect wireless keyboard/mouse to product.
5. For security reasons products do not support microphone/line-in audio input. In any case do not connect a microphone to product audio output port, including headsets.
6. Product is equipped with always-on active anti-tampering system. Any attempt to open product enclosure will activate the anti-tamper system indicated by all channel-select LEDs flashing continuously. In this case, product will be inoperable and warranty void. If product enclosure appears disrupted or if all channel-select LEDs flash continuously, please remove product from service immediately and contact technical support.

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

7. In case a connected device is rejected in the console port group the user will have the following visual indications:
  - a. When connecting a non-qualified keyboard, the keyboard will be non-functional with no visible keyboard strokes on screen when using the keyboard.
  - b. When connecting a non-qualified mouse, the mouse will be non-functional with mouse cursor frozen on screen.
  - c. When connecting a non-qualified display, the video diagnostic LED will flash green and video will not work.
  - d. When connecting a non-qualified USB device, DPP LED will flash green and USB device will be inoperable.
8. Do not connect product to computing devices:
  - a. That are TEMPEST computers;
  - b. That include telecommunication equipment;
  - c. That include frame grabber video cards;
  - d. That include special audio processing cards.
9. Product has a remote control port in the back panel labeled RCU. Do not use this port - it is inoperable and for future use.
10. Important! Before re-allocating computers to channels, it is mandatory to power cycle product, keeping it powered OFF for more than 1 minute.
11. Product log access and administrator configuration options are described in product Administrator Guide. Note that valid administrator username and password are required to access administrator functions such as log, KM configuration and CDF (DPP) configuration loading.
12. Authentication session will be terminated once product power is down or user intentionally terminates session.
13. 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 security-controlled environments. Below is a summary of the main advanced features incorporated in product:

#### **Important note before deploying the product:**

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

Refer to the product Administrator Guide for further details.

#### **Advanced isolation between computers and shared peripherals**

The emulations of keyboard, mouse and display EDID, prevent direct contact between computers and shared peripherals. Product design achieves maximal security by keeping the video path separate with keyboard and mouse switched together, purging keyboard buffer when switching channels. 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;

#### **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. Non-reprogrammable firmware prevents the ability to tamper with product logic. Valid administrator username and password are required to access administrator functions.

#### **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.



### Main Features (Cont.)

Metal enclosure is designed to resist mechanical tampering with all microcontrollers protected against firmware-read, modification and rewrite.

#### **Filtered USB (DPP) feature (applicable models)**

DPP feature enables to connect authorized USB devices to product. Product is designed with complete isolation between DPP data, such as user authentication smart card reader data, and all other product traffic.

When product arrives from the manufacturer the DPP is configured to accept only smart-card reader (Fixed Device Filtration – or FDF mode). Later the FDF mode may be changed by identified and authenticated administrator to less restrictive CDF mode using special software application utility called UCU.

The DPP feature can be managed via Configurable Device Filtering (CDF) mechanism with configuration permissions limited to identified and authenticated administrators. (valid administrator username and password are required to load CDF to the product). For more details please refer to the "DPP Configuration Manual".

#### **"Freeze DPP" feature**

Dedicated "Freeze DPP" slider on front panel enables to lock this function to a specific channel. When locked, switching channels will not affect processes performed by the USB device connected to the locked channel.

#### **Cursor navigation: Virtual Display Technology (VDT)**

VDT allows navigation between channels once mouse cursor crosses display borders. This seamless switching enhances product usability and ease of operation.

#### **Support for multiple head**

Product operating with computers connected to multiple-displays requires installation of software driver on each multi-display computer. Every product's channel can support up to 4 displays, e.g. 8-port-KM can support up to 32 displays.

#### **Setup options & predefined presets**

The KMs arrive with a predefined preset configuration for various display positioning options. For further customization of display positioning options and other features, an easy-to-use tool is available

### Tamper Evident Labels

Product uses holographic tamper evident labels to provide visual indications in case of an 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.**



Vertiv Tamper Evident Label

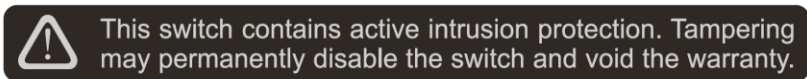
### Active Anti-Tampering System

Product is equipped with always-on active anti-tampering system. If mechanical intrusion is detected by this system, the Product will be permanently disabled and all LEDs will blink continuously.

**If product indicates "tampered state" (all LEDs blinking) - please call Technical Support and avoid using that product.**

### Product Enclosure Warning Label

Product has the following warning sticker on a prominent location on the product enclosure:

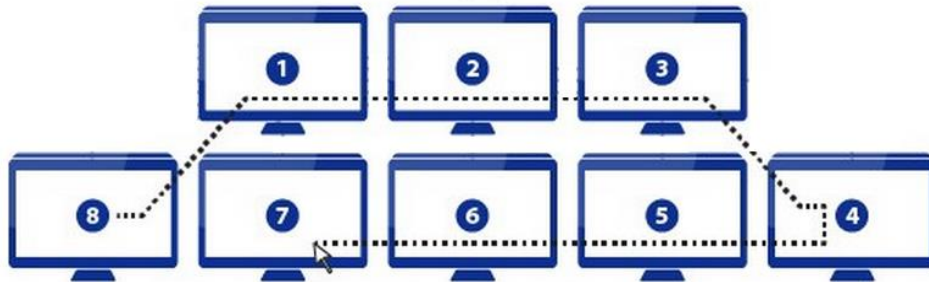


## What is Virtual Display Technology (VDT)

Virtual Display Technology (VDT) is implemented in VERTIV KM switches to enable seamless mouse and keyboard switching between multiple displays. With VDT, user simply moves mouse cursor across neighboring displays to switch between connected computers.

VDT allows to configure any desired display positioning, including displays with different sizes and resolutions.

VDT Configurator software enables to easily configure any set of display sizes, resolutions, geometry and physical arrangement.



Samples of switching between sources with VDT  
In 8-port KM

### Equipment Requirements

#### Cables

It is highly recommended to use Vertiv 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 console USB keyboard port is compatible with Standard USB keyboards.

#### Notes:

- a. 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.
- b. For security reasons products do not support wireless keyboards. In any case do not connect wireless keyboard to product.
- c. 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 console USB mouse port is compatible with standard USB mice.

#### Notes:

- a. 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.
- b. Console USB mouse port supports Standard KVM Extender composite device having a keyboard/mouse functions.
- c. For security reasons products do not support wireless mice. In any case do not connect wireless mouse to product.

#### PS/2 Mouse and Keyboard console ports

The product console PS/2 keyboard and mouse ports are compatible with standard PS/2 keyboards and mice.

#### DPP Port (applicable models)

The product operates with authorized USB devices plugged into the console DPP Port, such as USB smart-card reader or Common Access Card (CAC) reader.

By default, authentication devices such as smart card readers and CACs are authorized for use.

For authorizing additional USB devices to work with product, Configurable Device Filtering (CDF) mechanism is used with configuration permissions limited to authenticated administrators. For more details please refer to the "DPP Configuration Manual".

### **User Audio Devices**

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

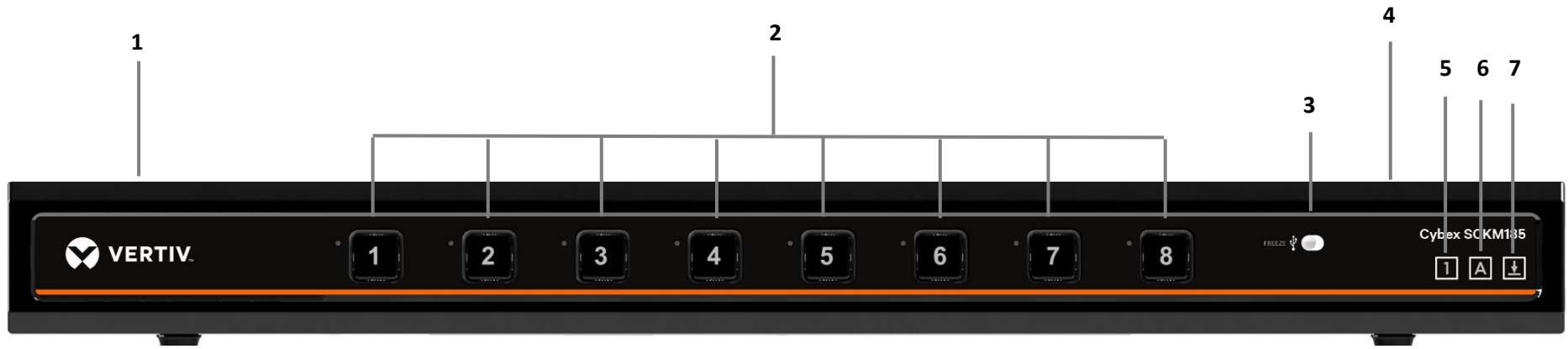
- Stereo headphones;
- Amplified stereo speakers.

Note: In any case do not connect a microphone to product audio output port including headsets.

### **Programming Cable for KM Configurator**

USB Type-A to USB Type-A Programming cable

## Front Panel Features



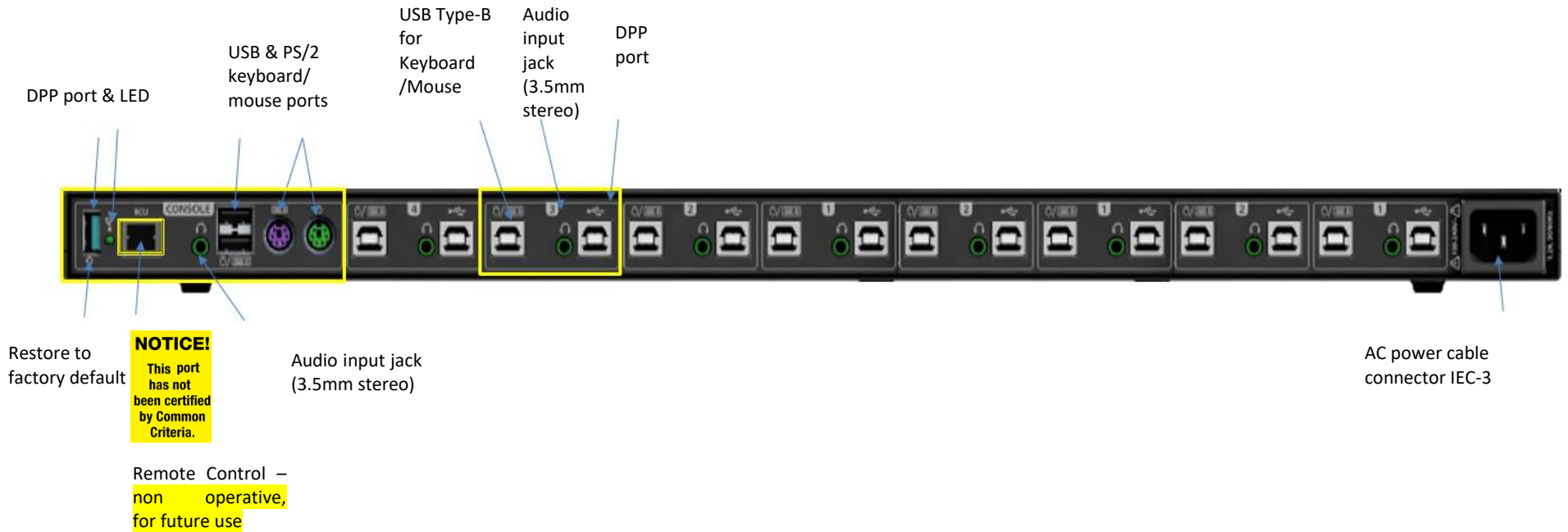
- |   |                    |
|---|--------------------|
| 1. Tamper Evident Label                                 | 5. Num Lock LED    |
| 2. No. 1-8 computer channel select push-button and LEDs | 6. Caps Lock LED   |
| 3. DPP Freeze push-button and LED                       | 7. Scroll Lock LED |
| 4. Tamper Evident Label                                 |                    |

Model illustrated above is SCKM185. SCKM180 is identical except  
For the fact it does not have DPP slider and LED

## Rear Panel Features

### Console ports group:

### Computer interface group:



Model illustrated above is SCKM185. SCKM180 is identical except For the fact it does not have DPP slider and LED

## Product Specifications

<b>Enclosure:</b>	Steel metal enclosure
<b>Power Requirements:</b>	Internal power 35W
<b>No. of Users Supported:</b>	1
<b>No. of Computers Supported:</b>	8
<b>Maximum number of Supported displays per Computer</b>	4 displays per channel (special driver must be installed)
<b>Maximum total number Of supported displays</b>	32
<b>Console Audio Input plug:</b>	1/8" (3.5mm) stereo plug
<b>Console Keyboard Input:</b>	USB Type-A female connector & PS/2 port
<b>Console Mouse Input:</b>	USB Type-A female connector & PS/2 port
<b>Console Audio input jack:</b>	1/8" (3.5mm) stereo plug
<b>Front Panel indicators</b>	CAPS LOCK, NUM LOCK, SCL LOCK Freeze DPP slider (SCKM185)

**Console DPP Input & LED** USB port & status LED (SCKM185)

**Computer Keyboard/Mouse ports:** USB Type B

**Computer DPP port:** USB Type B (SCKM185)

**Computer Audio Input plug:** 1/8" (3.5mm) stereo plug

**Port Selector illuminated push-buttons & LEDs:** 8

**User Channel Selection Methods:**

VDT, Front panel push-buttons

**Configurator Settings**

- Display physical size
- Display resolution X
- Display resolution Y
- Display orientation (Portrait / Landscape)
- Display head# (1<sup>st</sup>, 2<sup>nd</sup> ...16<sup>th</sup>)
- Display location (coordinates)
- Mouse speed (1-10)
- Mouse acceleration (1-10)
- VDT Enable / Disable
- Prevent transition while dragging feature Enable / Disable



## Section 2 - Overview

<b>Operating Temp:</b>	32° to 104° F (0° to 40° C)
<b>Storage Temp:</b>	-4° to 140° F (-20° to 60° C)
<b>Humidity:</b>	0-80% RH, non-condensing
<b>Product design life-cycle:</b>	10 years
<b>Warranty:</b>	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 Technical Support at:  
<http://www.VertivCo.com>
2. Do not connect product to computing devices:
  - a. That are TEMPEST computers;
  - b. That include telecommunication equipment;
  - c. That include frame grabber video cards
  - d. 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:

- Product front panel must be visible to the user at all times.
- 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, air-conditioning equipment, RF equipment or machines that create electrical noise (e.g., vacuum cleaners).

### Installation

#### Connecting devices to product console

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 displays directly to computers. Mark which display is coupled with which computer. It is also recommended to mark which computer is coupled with which channel.
- Connect user keyboard and mouse to console keyboard and mouse ports.
- Connect headphones/speakers to console audio out port (optional).
- If the computer uses a smart card reader/USB device, connect the smart card reader/USB device to the console DPP port (optional, model pending).

#### 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 products do not support wireless keyboards. In any case do not connect wireless keyboard to 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.

#### 2. Connecting the Computers

- Using USB cables, connect each computer to the USB type B port in "computer interface ports" area on product.
- If computer uses audio output, e.g. speakers/headphones, connect audio cable from its audio output port to the corresponding audio input port on product.
- If the computer uses a smart card reader/USB device, connect a USB cable between the DPP-enabled computer and the corresponding DPP port on product.

#### Note:

1. If the number of product channels is larger than the number of sources used, make sure the computers are connected in a row starting from computer #1. For example, if there are 3 channels used, connect computers to channels #1, #2 and then #3.
2. The USB cable must be connected directly to a free USB port on the computer, with no USB hubs or other devices in between.

#### 3. Power up

- Connect product to power.
- Power up user display/s. Select through display setup menu the appropriate video input if applicable.
- Power up the connected computers.
- Power up the product.

When you power up your computers, the KM emulates both a mouse and keyboard on each port and allows your computers to boot normally. You should be able to move the mouse cursor on the primary display connected to computer #1.

Check to see that the keyboard and mouse are working properly on each computer.

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.

#### 4. DPP Installation (applicable models)

In case computer and product support DPP functionality, such as user authentication smart card reader, do the following:

1. Connect USB device, such as smart card reader, to **DPP port on product console**
2. Connect **DPP input port** on product to any free **USB port on computer** using a USB cable.

**Note:** Do not connect the USB cable if DPP functionality is not needed for that computer.

If only some of the computers use DPP functionality, such as user authentication, make sure that **computer #1** is connected to the USB device. If needed, switch channels/computer mapping to create this configuration.

When product is powered ON and connected USB device is qualified and ready for use, the DPP status LED will illuminate steady green.

In case the connected USB device cannot be detected by the secure product, the DPP status LED will not illuminate at all.

The USB device will be detected only if it is fully compliant with USB 1.1 or USB 2.0 standard and is included in the list of recognized USB devices defined by the administrator when configuring DPP functionality.

Possible reasons for USB device not being detected:

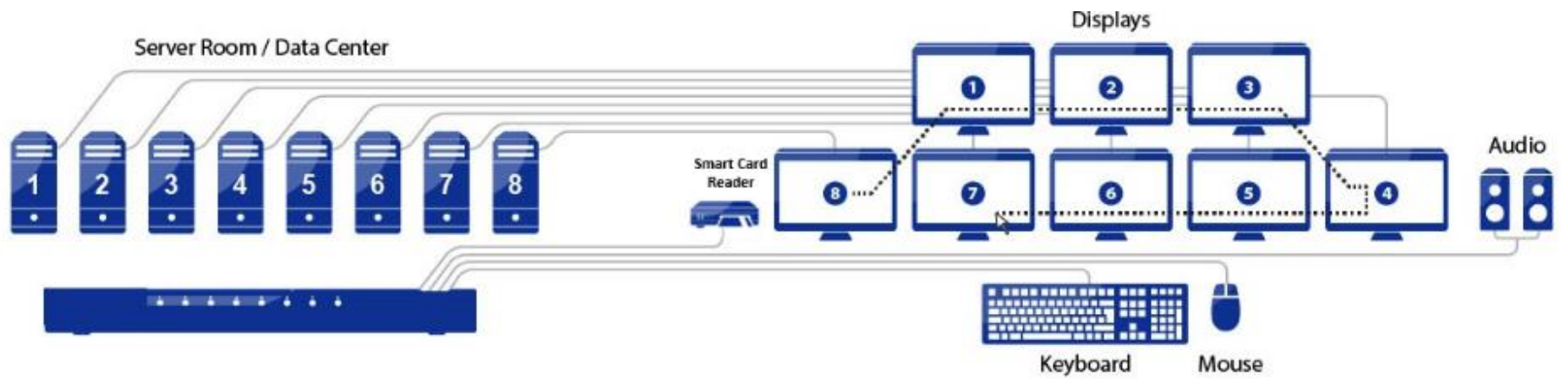
- Non-standard USB device
- Device only operating in USB 3.0 mode
- Failed USB Device

In this case you will have to use a different USB device.

If the device is detected but is not authorized, the device will be rejected for security reasons. This will be indicated by DPP status LED flashing green.

Smart card readers and CACs are included in the authorized USB devices list by default.

## Typical system installation



### Operational Setup

Now that the product is connected and powered up it is possible to setup some essential operational settings.

The first and most important setting of the KM is the display positioning. It is essential that the KM product configuration will match the actual physical positioning of displays.

There are two ways to configure the KM product with the actual display setup:

- Select one of the predefined setups
- Create a configuration file and load it to the KM

#### Option 1: Selecting one of the predefined setups

To select a default configuration type, press on the console keyboard one of the keyboard shortcuts as described in the following figures.

The configuration loaded will include the following parameters in addition to displays' arrangement:

- All displays are 1920 x 1200 resolution, same size (26" diagonal)
- Mouse acceleration is set to 6
- Mouse speed is set to 5
- VDT is enabled
- "Prevent transition while dragging" feature is Enabled

#### Option 2: Creating a custom configuration file

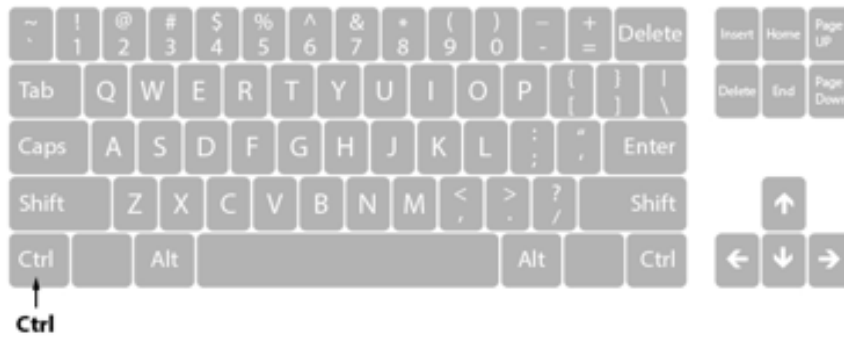
In case the required configuration does not appear on the predefined configurations list one can create a configuration file using KM Web Configuration Tool and load it to the KM. Such configuration loading is only possible for identified and authenticated administrators. For

more information about this option please refer to Vertiv's KM Configuration Tool user manual.

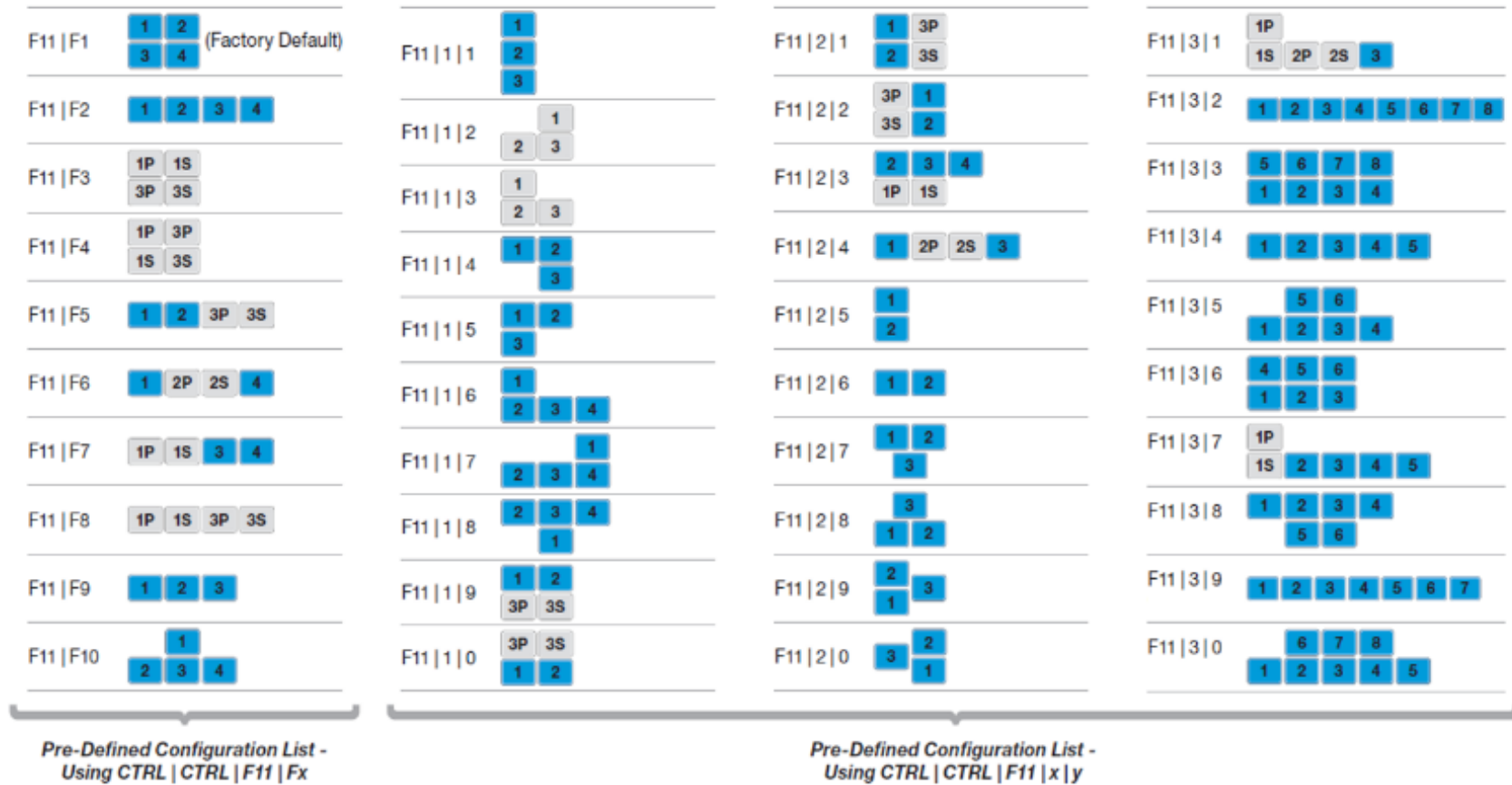
## Using Keyboard shortcuts:

**Note:**

- The CTRL key referred to in this manual is the left CTRL key.



## 8-port KM Predefined Setups





## Other Settings

### Mouse Speed Setting

Constant mouse cursor speed is essential for system usability. Having several systems each with a different cursor “ground speed” is bad for the user. Vertiv calculates and adjusts the cursor speed across different displays and computers using the geometry and display settings entered.

In addition, the KM settings include a global speed setting with input values between 1 and 10 that can be changed to adjust the cursor speed for all displays. Typical initial setting of cursor speed is 5. After initial use the exact value can be set based on user inputs.

### VDT Enabled / Disabled Setting

It is possible through the VDT enabled / disabled setting to disable the mouse cursor tracking function. Once VDT is disabled – the KM will enable channel selection only through front panel push-buttons.

This setting is enabled by default.

### Prevent transition while dragging feature

Vertiv Secure KM offers a unique feature that further improves usability – Prevent transition while dragging. When this feature is enabled, if the user drags an object on one display (while left mouse key pressed), the cursor would not leave that display.

### Notes:

1. Keyboard shortcut keys are to be pressed sequentially
2. CTRL key refers to LEFT CTRL key.



The following table describes the keyboard shortcuts available on Vertiv 's KMs:

Key Combination	Name	Description
CTRL , CTRL , F11 , r	Reset to Factory defaults	Device will reset to factory defaults with all settings and configuration deleted completely.
CTRL , CTRL , F11 , f	Freeze	Disable VDT. Switching between systems will not be possible via mouse movement.
CTRL , CTRL , F11 , U	Unfreeze	Enable VDT. Switching between systems will be again possible via mouse movement.
CTRL , CTRL , F11 , +	Increase mouse speed	Mouse speed will be increased.
CTRL , CTRL , F11 , -	Decrease mouse speed	Mouse speed will be decreased
CTRL , CTRL , F11 , d , c	Setup mode	In the next boot after pressing this key combination the device will boot into setup mode allowing him to communicate with configuration utility.
CTRL , CTRL , F12	Last loaded configuration	Revert to the last externally loaded configuration (configuration loaded via configuration utility).

### Driver Installation

To enable proper KM interaction with computers having multiple displays, mouse driver software must be installed. Driver can be loaded from Vertiv web-site. The driver is available in EXE file that installs itself at the target computer.

### Operating the Vertiv KM Switch

#### Self-Test Procedure:

As product powers-up it performs a self-test procedure. In case of self- test failure for any reason, including jammed buttons, the product will be Inoperable. Self-test failure will be indicated by the following abnormal LED behavior:

- All channel-select LEDs will be turned ON and then OFF;
- A specific, predefined LED combination will be turned ON;
- The predefined LED combination will indicate the problem type (jammed buttons, firmware integrity).

Try to power cycle product. If problem persists please contact your system administrator or technical support.

Now that product, computers and peripherals are connected and powered up, it is ready for use.

#### Default Channel

After product boots up, blue LEDs stripe will illuminate and the default active channel will be channel #1. This will be indicated by white color illumination of push-button #1.

#### Product Mapping to Sources

Product mapping to sources is indicated by stickers/labels specifying which channel is mapped to which computer.

#### Front Panel Push-Buttons

Following power up, the default channel is #1.

The user can select any other channel by pressing the appropriate front panel push button.

The mouse cursor will be positioned at the center of the selected computer display. If computer is connected to multiple displays, the cursor will be positioned at the center of the primary display.

The currently selected channel is indicated by white color illumination of the appropriate push-button.

Once a different channel is selected - keyboard, mouse, audio and DPP functions follow selected channel, unless Freeze DPP function has been activated (see below for details).

#### Cursor Tracking ("VDT-Enabled")

Following power up the cursor will be positioned at the center of the primary display of computer #1. Keyboard and audio will be coupled to the same PC where the cursor is.

When VDT is enabled - once the user moves the mouse cursor across display borders to another display connected to a different computer - keyboard, audio and DPP functions will follow.

#### "Prevent transition while dragging" feature

An enabled "Prevent transition while dragging" feature means that if user drags an object on display #1 while holding left mouse key, the cursor will remain in display #1 even if mouse cursor crosses display

borders. The purpose of this feature is to prevent unintentional loss of dragging action due to accidental crossing of display borders.

This feature is enabled by default and controlled via administrator setup.

### Cursor Acceleration and Speed

Cursor speed and acceleration are a result of several factors such as display size, resolution and additional settings. If current cursor acceleration and speed are not consistent or comfortable for use – please contact your system administrator for assistance.

### DPP Port (applicable models)

The product is equipped with DPP port enabling connectivity to external USB-devices such as smartcard reader.

The filtered USB function (DPP) enables to control which USB devices will be operative when connected to product.

For more details on configuration options, please refer to the "DPP Configuration Manual".

### Summary of rules that apply to DPP switching:

It is assumed that a "connected channel" is when:

1. Product is powered ON
2. The USB device connected to product console is qualified and ready for use, as indicated by the DPP status LED illuminating steady green.
3. The channel DPP port on product is connected via USB cable to a USB port on computer.

- When the USB device connected to the DPP console port is qualified, the DPP status LED on the front panel would illuminate steady green.
  - When connecting a USB device that is not qualified or rejected for security reasons to the product's DPP port, the DPP LED will flash green and USB device will be inoperable. In such case the USB device must be replaced with a qualified device.
  - When connecting a USB device to the product's DPP port that is undetectable for any reason (e.g. failed device, non-standard device etc.), the DPP LED will not illuminate at all and USB device will be inoperable. In such case the USB device must be replaced with a qualified device.
- Since channel #1 is the default active channel after power up and in case only some of the channels operate with a USB device, it is recommended to make sure computer #1 is connected to USB device.
- Once the user switches channels, for example to channel #3, DPP functionality will move to computer #3 and be indicated by channel #3 DPP LED turning steady green.
- In case user switches to a channel that is not connected to a USB device, the previous USB connection will be terminated and no new connection will be established.
- In case "Freeze DPP" slider was moved to activate DPP function for computer #1, for example, switching to a different channel would keep DPP function locked to channel #1. To release "Freeze DPP" function from channel #1, the user will need to move the "Freeze DPP" slider again to its original position. The release will be indicated by the channel #1 DPP LED being turned off.

- In case Restore-to-Default was performed while "Freeze DPP" slider was activated on a specific channel, after boot up this function will be locked to computer #1.

### Using "DPP Freeze" feature

Move the "DPP Freeze" slider to lock DPP function to a specific channel. The DPP status LED will indicate that this option has been activated and to which channel the DPP function is locked to at the moment. This means that switching channels would not affect the processes performed by the USB device connected to that channel.

### Keyboard Status Indication

In order to enhance usability, product provides keyboard status indications via dedicated LEDs located on product front panel. To maintain the required unidirectional connectivity between keyboard and product, these indication are not given on the keyboard itself as done with non-secure products

The keyboard status indications are given via 3 LEDs on the front panel of the product:

- CL – CAPS Lock
- SL – SCROLL Lock
- NL – NUM Lock

The indications behave the same as the LEDs on the keyboard as if it was connected directly to computer.

**Switching from channel to channel may change the status of the LEDs based on the current settings on the computer connected to the active channel.**

## 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:

- Email: [Secure@VertivCo.com](mailto:Secure@VertivCo.com)
- Tel: +1-888-793-8763

**Important:** If the unit's enclosure appears disrupted or if all LEDs flash continuously, please remove product from service immediately and contact Technical Support at <http://www.Vertiv.com>

**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.

### General

**Problem:** As product powers-up all channel-select LEDs are turned ON and then OFF. After that a specific, predefined LED combination is turned ON. 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, none of the front panel LEDs are illuminating.

#### Solutions:

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

**Problem:** Product enclosure appears disrupted or all channel-select LEDs flash continuously.

**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 (two channels)

**Solutions:**

- Check that computer USB and video cables are not crossed i.e. computer #1 video is connected to channel #1 while USB keyboard and mouse cables are connected to channel #2.

**Problem:** Keyboard does not work (all channels)

**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 USB-integrated 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 cursor does not switch from primary to secondary display.

**Solutions:** Driver supporting multiple displays was not installed or not installed properly on computer. Reinstall driver.

**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 is connected to channel #1 while USB keyboard and mouse cables are connected to channel #2.

**Problem:** Mouse does not work (all channels)

**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 not working (one channel)

**Solution:** Use computer Device Manager Utility to see product and solve problem.

**DPP**

**Problem:** DPP is not working (two channels)

**Solutions:**

- Check that computer USB and video cables are not crossed i.e. computer #1 video is connected to channel #1 while USB device is connected to channel #2.

**Problem:** DPP is not working (all channels)

**Solutions:**

- Check that the USB device is properly connected to product console.
- Check that the DPP status LED is steady green. If DPP status LED is not illuminated at all the device is not recognized by the

product. If DPP status LED is flashing green device is rejected or non-qualified for security reasons. To resolve please contact your system administrator.

**Problem:** DPP is not working (one channel only)

**Solutions:**

- Check that device is working properly when connected directly to computer.
- Check that there is a USB cable connected between the computer and the relevant DPP input port on product.

## Copyright and Legal Notice

Vertiv, Vertiv Network Power and the Vertiv Network Power logo are trademarks or service marks of Vertiv Electric

Co. Avocent and the Avocent logo are trademarks or service marks of Avocent Corporation. This document may contain confidential and/or proprietary information of Avocent Corporation, and its receipt or possession does not convey any right to reproduce, disclose its contents, or to manufacture or sell anything that it may describe. Reproduction, disclosure, or use without specific authorization from Avocent Corporation is strictly prohibited. ©2015 Avocent Corporation. All rights reserved.

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

*Images are for demonstration purposes only.*