Vertiv CYBEX™ SCKM140PP4 KM Switch

Firmware Version 40404-0E7

Common Criteria Guidance Supplement

Doc No. 2149-001-D105C4A
Version: 1.8
23 November 2021

Vertiv
1050 Dearborn Dr,
Columbus, OH 43085

Prepared by:
EWA-Canada, An Intertek Company
1223 Michael Street North, Suite 200
Ottawa, Ontario, Canada
K1J 7T2

CONTENTS

LIST OF TABLES

1 PREPARATION OF THE OPERATIONAL ENVIRONMENT

1.1 OPERATIONAL ENVIRONMENT

For secure operation, users are required to ensure the following conditions are met in the operational environment:

- TEMPEST approved equipment may not be used with the secure peripheral sharing device
- The operational environment must provide physical security, commensurate with the value of the peripheral sharing device and the data that transits it
- Wireless keyboards, mice, audio, user authentication, or video devices may not be used with the secure peripheral sharing device
- Peripheral sharing device Administrators and users are trusted individuals who are appropriately trained
- Administrators configuring the peripheral sharing device and its operational environment follow the applicable security configuration guidance

2 SECURE ACCEPTANCE PROCEDURES

Vertiv peripheral sharing devices may be purchased directly from Vertiv, or through distributors and resellers / integrators.

Upon receipt of the Vertiv peripheral sharing device, the customer can verify the configuration and revision by comparing the part number and revision on the packing list with the label on the bottom of the hardware unit. The nameplate includes the product part number (CGA) which is linked directly to the revision of the hardware components and firmware. Verification of the part number provides assurance that the correct product has been received.

The customer must download product documentation from the Vertiv website in Adobe Acrobat Portable Document Format (PDF). The customer can confirm that the documentation matches the purchased model.

Customers are instructed to check all delivered products for package container seals, and to verify that product tampering evident labels are intact. If an issue is discovered, the customer is instructed to return the product immediately.

3 SECURE INSTALLATION PROCEDURES

This section describes the steps necessary for secure installation and configuration.

3.1 SECURE INSTALLATION

Instructions for secure installation may be found in the Quick Installation Guide.

3.2 REMOTE CONTROL

Install the remote control by plugging the remote control cable into the RCU port on the TOE switch.

Pressing the button causes the device to switch to the next sequential channel. The channel is set by pressing the remote control button until the desired channel is selected. The Light Emitting Diode (LED) is illuminated when the associated channel is selected.

4 SECURE OPERATION

This section describes the steps necessary for the secure operation of the Vertiv KM Switch.

4.1 SELF TESTS

A self test is performed at power up. Self test failures may be caused by an unexpected input at power up, or by a failure in the device integrity. A self test failure may also be an indication that the device has been tampered with.

A user may enter self test failure mode by following the procedures outlined in Table 1.

Device Type	Procedure
KM Switch	1. To enter self test failure mode, press and hold the channel 1 button, and power on the device. The channel indicators on the front panel light up sequentially, and the keyboard and mouse USB ports are disabled. 2. To exit self test failure mode, cycle the power.

Table 1 – Procedure to Initiate a Self Test

In the case of a self test failure, users are directed to contact Vertiv Technical Support.

4.2 ERROR STATE

As the product powers up, it performs a self-test procedure. Following failure of a self-test, the device will enter an error state. The error state is indicated by sequential flashing of the Light Emitting Diodes and by a clicking noise. At this point, the device will be inoperable. It will not accept input from any peripheral device.

The user can cause the self-test to be rerun by unplugging the device and plugging it back in.

4.3 SELECTED CHANNEL AT STARTUP

Channel 1 is selected by default when the peripheral sharing device is started or reset.

4.4 TAMPER EVIDENCE AND RESPONSE

The KM switch is equipped with anti-tampering features. Opening the device will cause it to become permanently disabled. Depletion of the anti-tampering circuitry battery will also cause the device to become permanently disabled. If the device appears to have been tampered with, or if any of the following are observed, contact Technical Support:

- One or more tamper-evident seals has been broken or removed. If removed, the word ‘VOID’ appears on both the label and the product surface.
- The front panel LEDs blink sequentially and continuously. This indicates that the TOE has been tampered with and the device will be permanently disabled.

The remote control is also equipped with anti-tampering features. Opening the device will cause it to become permanently disabled. Depletion of the anti-tampering circuitry battery will also cause the remote control device to become permanently disabled. If the device appears to have been tampered with, or if any of the following are observed, contact Technical Support:

- The tamper-evident seal has been broken or removed. If removed, the word ‘VOID’ appears on both the label and the product surface.
- The LEDs blink sequentially and continuously. This indicates that the remote control has been tampered with and the device will be permanently disabled.