Vertiv CYBEX™ SC820DPH, SC840DPH, SC920DPH, SC940DPH, SC840DPHC, SC940DPHC, SC840DVI, SC940DVI Firmware Version 44404-E7E7 Peripheral Sharing Devices

Common Criteria Guidance Supplement

Doc No. 2149-001-D105C3
Version: 1.7
17 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

1 PREPARATION OF THE OPERATIONAL ENVIRONMENT 1
1.1 OPERATIONAL ENVIRONMENT 1
2 SECURE ACCEPTANCE PROCEDURES 2
3 SECURE INSTALLATION PROCEDURES 3
3.1 SECURE INSTALLATION 3
3.2 REMOTE CONTROL 3
4 SECURE OPERATION 4
4.1 USER ROLES 4
4.2 SELF TESTS 4
4.3 ERROR STATE 4
4.4 SELECTED CHANNEL AT STARTUP 5
4.5 TIMESTAMPS 5
4.6 NUMBER OF SUPPORTED DISPLAYS 5
4.7 TAMPER EVIDENCE AND RESPONSE 5
5 USE OF TERMINAL MODE 7

LIST OF TABLES

Table 1 – Procedure to Initiate Self-Test Failure Mode 4
Table 2 – Number of Supported Displays by Device 5
Table 3 – Applicable Sections of The Cybex™ SC/SCM Switching System Additional Operations and Configuration Technical Bulletin 8

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
- Special analog data collection cards or peripherals such as analog to digital interface, high performance audio interface, or a component with digital signal processing or analog video capture functions may not be used with the secure peripheral sharing device
- Microphones must not be plugged into the TOE audio output interfaces

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 back 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 Guides.

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 on the remote 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 Peripheral Sharing Devices.

4.1 USER ROLES

Instructions for users may be found in the Quick Installation Guides. Instructions for Administrators may be found in the Cybex™ SC/SCM Switching System Additional Operations and Configuration Technical Bulletin.

Users may access switching capabilities. All functions noted in the Technical Bulletin are limited to Administrators.

4.2 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. When a self test fails, the device enters an error state (See Section 4.3). Following a successful self test, the device operates normally. 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.

Model	Procedure
SC820DPH SC840DPH SC920DPH SC940DPH SC840DPHC SC940DPHC SC840DVI SC940DVI	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 audio, video, and keyboard/mouse USB ports are disabled. 2. To exit self-test failure mode, cycle the power.

Table 1 – Procedure to Initiate Self-Test Failure Mode

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

4.3 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 or pass output to any peripheral device.

4.4 SELECTED CHANNEL AT STARTUP

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

4.5 TIMESTAMPS

Each device includes a real-time clock powered by a battery. The time is set during production.

4.6 NUMBER OF SUPPORTED DISPLAYS

The number of supported displays is shown in the following table:

Device	Number of Supported Displays
SC820DPH	1
SC840DPH	1
SC920DPH	2
SC940DPH	2
SC840DPHC	1
SC940DPHC	2
SC840DVI	1
SC940DVI	2

Table 2 – Number of Supported Displays by Device

4.7 TAMPER EVIDENCE AND RESPONSE

The KVM switches are equipped with anti-tampering features. Opening the device will cause it 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. 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.

5 USE OF TERMINAL MODE

The Cybex™ SC/SCM Switching System Additional Operations and Configuration Technical Bulletin, 590-1741-501 Rev. B provides guidance on the user of Terminal Mode. Not all of the Terminal Mode functions are supported in the Vertiv CYBEX™ SC820DPH, SC840DPH, SC920DPH, SC940DPH, SC840DPHC, SC940DPHC, SC840DVI, and SC940DVI devices. The applicable sections are as follows:

Section	Applicability
2.2 Terminal Mode	An Administrator may enter and exit terminal mode. This is the administrative interface for the device. An Administrator may power cycle the KVM using Terminal Mode, or by unplugging the device's power cable from the power outlet and plugging it back in. This is not a security function related to any Security Functional Requirement (SFR) in the Vertiv CYBEX™ SC820DPH, SC840DPH, SC920DPH, SC940DPH, SC840DPHC, SC940DPHC, SC840DVI, SC940DVI Security Target.
2.2.1 Asset Management	This function is not supported. This is not a security function related to any SFR.
2.2.2 Firmware Versions	Although this may be used to verify the firmware version, this is not a security function related to any SFR.
2.2.3 Configure DPP	This function is not supported. The devices do not have a Dedicated Peripheral Port (DPP).
2.2.4 Configure SC	This function is not supported.
2.2.5 Account Management	An administrator may use these options to create and delete administrator accounts. Administrators can change their own passwords.
2.2.6 Reset to Factory Defaults	This is used to reset the device to factory defaults.
2.2.7 Logs and Events	This is used to access the logs created in accordance with FAU_GEN.1. The logs include the outcome of the event, the date and time of the event and, where applicable, the user that initiated the event.

Section	Applicability
2.2.8 Configure Peripheral Devices	This function is not supported.

Table 3 – Applicable Sections of The Cybex™ SC/SCM Switching System Additional Operations and Configuration Technical Bulletin