

Common Criteria Certification Report

CYBEX SC Series Secure Micro Switches SC825SFF, SC925SFF, SC845SFF, SC945SFF, SC885SFF, SC985SFF, SCMV245SFF, SC825SFF-B-DP, SC825SFF-B-H, SC925SFF-B-DP, SC925SFF-B-H, SC845SFF-B-DP, SC845SFF-B-H, SC945SFF-B-DP, SC945SFF-B-H, SC885SFF-B-DP, SC885SFF-B-H, SC985SFF-B-DP, SC985SFF-B-H, SCMV245SFF-B-DP, SCMV245SFF-B-H Firmware Version 44044-M7M7



CAN-680-EWA

6 August 2026

v1.0



Communications Security
Establishment Canada
Canadian Centre
for Cyber Security

Centre de la sécurité des
télécommunications Canada
Centre canadien
pour la cybersécurité

Canada

Foreword

This certification report is an UNCLASSIFIED publication, issued under the authority of the Chief, Communications Security Establishment (CSE).

The Information Technology (IT) product identified in this certification report, and its associated certificate, has been evaluated at an approved testing laboratory established under the Canadian Centre for Cyber Security (a branch of CSE). This certification report, and its associated certificate, applies only to the identified version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the Canadian Common Criteria Program, and the conclusions of the testing laboratory in the evaluation report are consistent with the evidence adduced.

This report, and its associated certificate, are not an endorsement of the IT product by Canadian Centre for Cyber Security, or any other organization that recognizes or gives effect to this report, and its associated certificate, and no warranty for the IT product by the Canadian Centre for Cyber Security, or any other organization that recognizes or gives effect to this report, and its associated certificate, is either expressed or implied.

If your organization has identified a requirement for this certification report based on business needs and would like more detailed information, please contact:

Canadian Centre for Cyber Security

Contact Centre and Information Services

contact@cyber.gc.ca | 1-833-CYBER-88 (1-833-292-3788)



Overview

The Canadian Common Criteria Program provides a third-party evaluation service for evaluating the security of IT products. Evaluations are performed by a commercial Common Criteria Testing Laboratory (CCTL) under the oversight of the Certification Body, which is managed by the Canadian Centre for Cyber Security.

A CCTL is a commercial facility that has been approved by the Certification Body to perform Common Criteria evaluations; a significant requirement for such approval is accreditation to the requirements of ISO/IEC 17025, the General Requirements for the Competence of Testing and Calibration Laboratories.

By awarding a Common Criteria certificate, the Certification Body asserts that the product complies with the security requirements specified in the associated security target (ST). A security target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the ST, in addition to this certification report, to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, the evaluated security functionality, and the testing and analysis conducted by the CCTL.

The certification report, certificate of product evaluation and ST are posted to the [Common Criteria portal](#) (the official website of the International Common Criteria Program).



TABLE OF CONTENTS

Foreword.....	1
Overview	2
Executive Summary CAN-680-EWA.....	4
Identification of Target of Evaluation	5
Common Criteria Conformance	5
TOE Description	5
TOE Architecture.....	6
Security Policy	8
Assumptions and Clarification of Scope	9
Usage and Environmental Assumptions	9
Clarification of Scope.....	9
Evaluated Configuration.....	10
Documentation	10
Evaluation Analysis Activities	11
Development	11
Guidance Documents.....	11
Life-Cycle Support	11
Testing Activities	12
Assessment of Developer tests	12
Conduct of Testing.....	12
Independent Testing.....	12
Vulnerability Analysis	13
Vulnerability Analysis Results	13
Results of the Evaluation	14
Recommendations/Comments	14
Supporting Content.....	15
List of Abbreviations	15
References	16



Executive Summary CAN-680-EWA

CYBEX SC Series Secure Micro Switches SC825SFF, SC925SFF, SC845SFF, SC945SFF, SC885SFF, SC985SFF, SCMV245SFF, SC825SFF-B-DP, SC825SFF-B-H, SC925SFF-B-DP, SC925SFF-B-H, SC845SFF-B-DP, SC845SFF-B-H, SC945SFF-B-DP, SC945SFF-B-H, SC885SFF-B-DP, SC885SFF-B-H, SC985SFF-B-DP, SC985SFF-B-H, SCMV245SFF-B-DP, SCMV245SFF-B-H Firmware Version 44044-M7M7 (hereafter referred to as the Target of Evaluation, or TOE), from **Vertiv Group Corp.**, was the subject of this Common Criteria evaluation. The results of this evaluation demonstrate that the TOE meets the following conformance claim: **Protection Profile for Peripheral Sharing Device, Version 4.0; PP-Module for Keyboard/Mouse Devices, Version 1.0; PP-Module for Video/Display Devices, Version 1.0; PP-Module for User Authentication Devices, Version 1.0**

EWA-Canada is the CCTL that conducted the evaluation. This evaluation was completed on **6 August 2026** and was conducted in accordance with the rules of the Canadian Common Criteria Program.

The scope of the evaluation is defined by the Security Target, which identifies assumptions made during the evaluation, the intended environment for the TOE, and the security functional/assurance requirements. Consumers are advised to verify that their operating environment is consistent with that specified in the security target, and to consider the comments, observations, and recommendations in this Certification Report.

The Canadian Centre for Cyber Security, as the Certification Body, declares that this evaluation meets all the conditions of the Arrangement on the Recognition of Common Criteria Certificates and that the product is listed on the [Certified Products list](#) for the Canadian Common Criteria Program and the [Common Criteria portal](#) (the official website of the International Common Criteria Program).



Identification of Target of Evaluation

The Target of Evaluation (TOE) is identified as follows:

Table 1: TOE Identification

TOE Name and Version	CYBEX SC Series Secure Micro Switches SC825SFF, SC925SFF, SC845SFF, SC945SFF, SC885SFF, SC985SFF, SCMV245SFF, SC825SFF-B-DP, SC825SFF-B-H, SC925SFF-B-DP, SC925SFF-B-H, SC845SFF-B-DP, SC845SFF-B-H, SC945SFF-B-DP, SC945SFF-B-H, SC885SFF-B-DP, SC885SFF-B-H, SC985SFF-B-DP, SC985SFF-B-H, SCMV245SFF-B-DP, SCMV245SFF-B-H Firmware Version 44044-M7M7
Developer	Vertiv Group Corp.

See the [Evaluated Configuration](#) section for more details on the evaluated configuration of the TOE.

Common Criteria Conformance

The evaluation was conducted using the following methodology:

Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5

The TOE claims the following conformance:

Protection Profile for Peripheral Sharing Device, Version 4.0; PP-Module for Keyboard/Mouse Devices, Version 1.0; PP-Module for Video/Display Devices, Version 1.0; PP-Module for User Authentication Devices, Version 1.0

TOE Description

The TOE allows users to securely share keyboard, mouse video, and Universal Serial Bus (USB) authentication device peripherals between up to 8 connected computers. The TOE natively supports High-Definition Multimedia Interface (HDMI) and DisplayPort (DP) video protocols. Security features ensure isolation between computers and peripherals to prevent data leakage between connected systems. These products are KVM switches with anti-tampering.

TOE Architecture

A diagram of the TOE architecture is as follows:

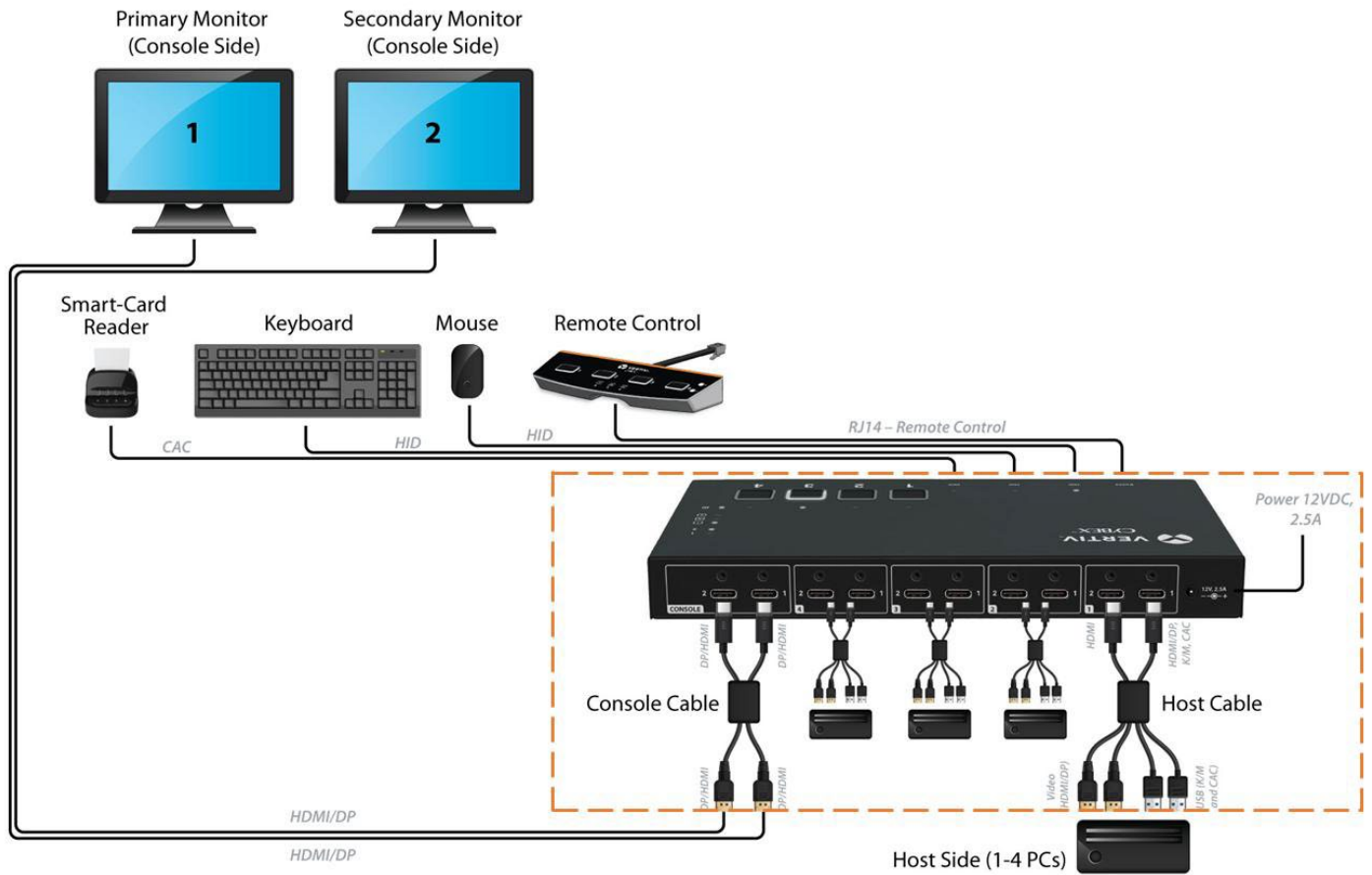


Figure 1: TOE Architecture (KVM)

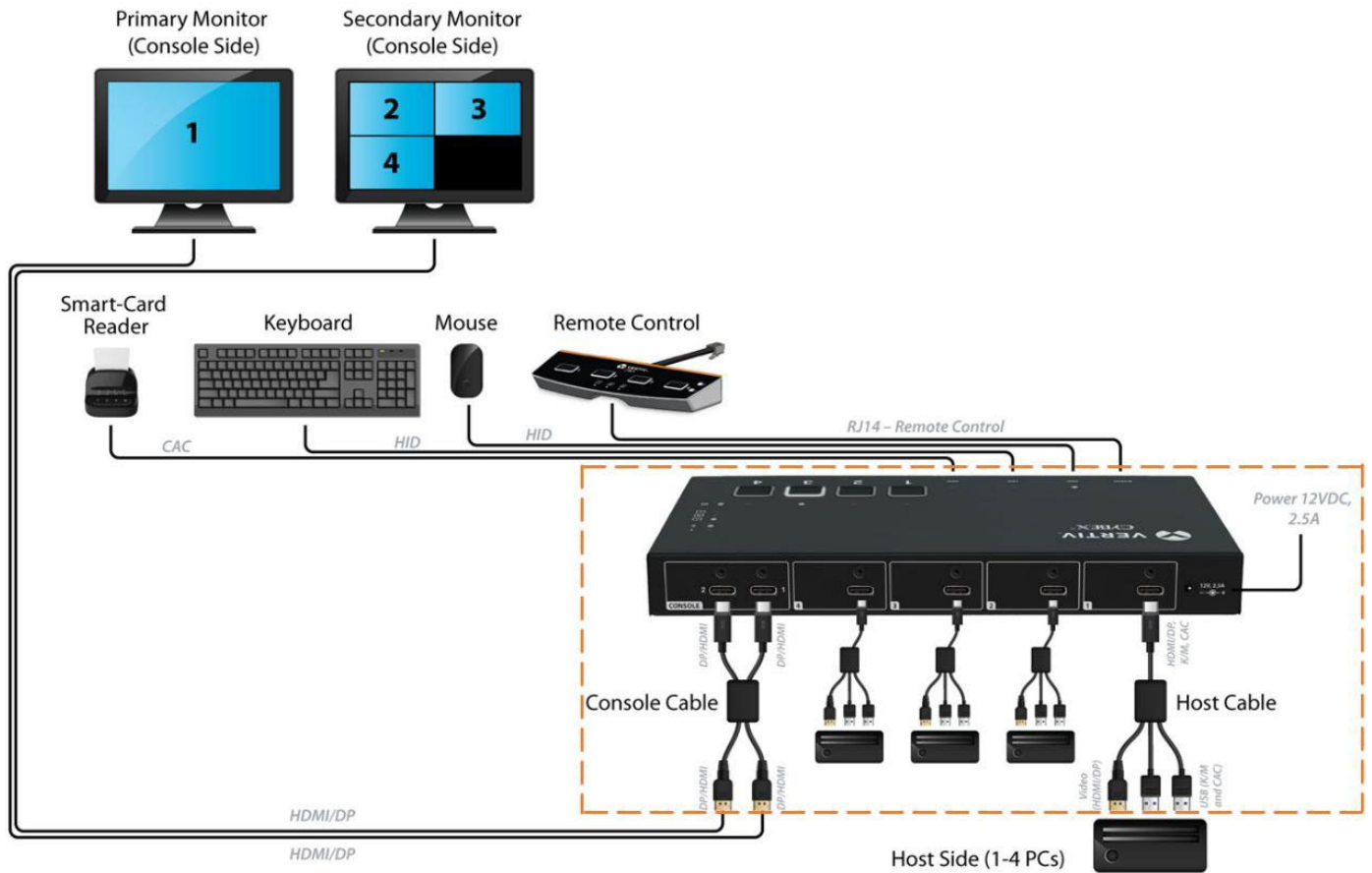


Figure 2: TOE Architecture (Multi-Viewer)

Security Policy

The TOE implements and enforces policies pertaining to the following security functionality:

- User Data Protection
- TOE Access
- Protection of the TSF

Complete details of the security functional requirements (SFRs) can be found in the [Security Target](#).



Assumptions and Clarification of Scope

Consumers of the TOE should consider assumptions about usage and environmental settings as requirements for the product's installation and its operating environment. This will ensure the proper and secure operation of the TOE.

Usage and Environmental Assumptions

The following assumptions are made regarding the use and deployment of the TOE:

- Computers and peripheral devices connected to the PSD are not TEMPEST approved.
- The environment provides physical security commensurate with the value of the TOE and the data it processes and contains.
- The environment includes no wireless peripheral devices.
- PSD Administrators and users are trusted to follow and apply all guidance in a trusted manner.
- Personnel configuring the PSD and its operational environment follow the applicable security configuration guidance.
- All PSD users are allowed to interact with all connected computers. It is not the role of the PSD to prevent or otherwise control user access to connected computers. Computers or their connected network shall have the required means to authenticate the user and to control access to their various resources.
- The computers connected to the TOE are not equipped with special analog data collection cards or peripherals such as analog to digital interface, high performance audio interface, digital signal processing function, or analog video capture function.

Clarification of Scope

Only the functionality covered by the Protection Profiles/Modules claimed in the [Common Criteria Conformance](#) section are included within the scope of the evaluation.



Evaluated Configuration

The evaluated configuration for the TOE comprises:

Table 2: Evaluated Configuration

TOE Software/Firmware	Firmware Version 44044-M7M7			
TOE Hardware	TOE Models:	• SC925SFF	• SC845SFF	• SC945SFF
	• SC985SFF	• SCMV245SFF	• SC825SFF-B-DP	• SC825SFF-B-H
	• SC925SFF-B-H	• SC845SFF-B-DP	• SC845SFF-B-H	• SC945SFF-B-DP
	• SC885SFF-B-DP	• SC885SFF-B-H	• SC985SFF-B-DP	• SC985SFF-B-H
	• SCMV245SFF-B-H	• SC885SFF	• SC925SFF-B-DP	• SC945SFF-B-H
	• SCMV245SFF-B-DP	• SC825SFF		
	TOE Remotes:	• AFPM0002	• AFPM0004	• AFPM0008
	TOE Cables:	• CBLMHSHDP0100T	• CBLMHDHDP0101T	
	• CBLMHDHH0103T	• CBLMCSHDP0105T	• CBLMCDHDP0106T	
	• CBLMCSSH0107T	• CBLMCDHH0108T	• CBLMSHSH0102T	
Environmental Support	• Any standard USB smart card reader/authentication device (only USB Type A connections) • General purpose mouse/keyboard			

Documentation

The following documents are available to the consumer to assist in the configuration and installation of the TOE:

- CYBEX™ SC Series Secure Micro Switches SCMV245SFF Multiviewer Quick Installation Guide, HLT36723, Rev. 1.7
- CYBEX™ SC Series Secure Micro Switches SC825SFF, SC925SFF, SC845SFF, SC945SFF, SC885SFF, SC985SFF Quick Installation Guide, HLT36621, Rev. 1.2
- CYBEX™ SC Series Secure Micro Switches SC825SFF, SC925SFF, SC845SFF, SC945SFF, SC885SFF, SC985SFF, SCMV245SFF, SC825SFF-B-DP, SC825SFF-B-H, SC925SFF-B-DP, SC925SFF-B-H, SC845SFF-B-DP, SC845SFF-B-H, SC945SFF-B-DP, SC945SFF-B-H, SC885SFF-B-DP, SC885SFF-B-H, SC985SFF-B-DP, SC985SFF-B-H, SCMV245SFF-B-DP, SCMV245SFF-B-H
Firmware Version 44044-M7M7 Common Criteria Guidance Supplement, Version 1.0



Evaluation Analysis Activities

The evaluation activities comprised a structured assessment of the TOE. Documentation and processes related to Development, Guidance Documentation, and Life-Cycle Support were reviewed and analyzed.

Development

The evaluators analyzed the documentation provided by the vendor; they determined that the design completely and accurately describes the TOE security functionality (TSF) interfaces and how the TSF implements the security functional requirements. The evaluators determined that the initialization process is secure, that the security functions are protected against tamper and bypass, and that security domains are maintained.

Guidance Documents

The evaluators examined the TOE preparative user guidance and operational user guidance and determined that it sufficiently and unambiguously describes how to securely transform the TOE into its evaluated configuration and how to use and administer the product. The evaluators exercised the preparative and operational guidance and determined that they are complete and sufficiently detailed to result in a secure configuration.

Life-Cycle Support

An analysis of the TOE configuration management system and associated documentation was performed. The evaluators found that the TOE configuration items were clearly marked.

The evaluators examined the delivery documentation and determined that it described all the procedures required to maintain the integrity of the TOE during distribution to the consumer.



Testing Activities

Testing consists of the following three steps: assessing developer tests, performing independent tests, and performing a vulnerability analysis.

Assessment of Developer tests

The evaluators verified that the developer has met their testing responsibilities by examining their test evidence, and reviewing their test results, as documented in the Evaluation Test Report (ETR). The correspondence between the tests identified in the developer's test documentation and the functional specification was complete.

Conduct of Testing

The TOE was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The detailed testing activities, including configurations, procedures, test cases, expected results and observed results are documented in a separate proprietary test results document.

Independent Testing

During this evaluation, the evaluator developed independent functional and penetration tests by examining design and guidance documentation.

All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. The following testing activities were performed:

- a. PP Assurance Activities: The evaluator performed the assurance activities listed in the claimed PP.

Independent Testing Results

The testing produced the expected results, supporting the conclusion that the TOE correctly implements the functional requirements specified in the ST and the TOE functional specification.



Vulnerability Analysis

The evaluators conducted an independent review of all evaluation evidence, public domain vulnerability databases, and technical community sources. Additionally, the evaluators used automated vulnerability scanning tools to discover potential network, platform, and application layer vulnerabilities. Based upon this review, the evaluators formulated flaw hypotheses, which they used in their vulnerability analysis.

Public domain searches were conducted on **21 July 2026** and included the following search terms:

HDMI	EDID	HEC
DisplayPort	HSL	Vertiv
HDMI CEC	High Sec Labs	Highseclabs
Highseclabs KVM	Highseclabs switch	TOE models and Firmware
Peripheral sharing	STM32F44	STM32C07
GD25Q16	MIMXRT1052	MDIN
W25Q512	HDMI ARC	MCCS

Vulnerability searches were conducted using the following sources:

National Vulnerability Database https://nvd.nist.gov/vuln/search	CISA Known Exploited Vulnerabilities Catalog https://www.cisa.gov/known-exploited-vulnerabilities-catalog
--	---

Vulnerability Analysis Results

The vulnerability analysis did not uncover any security relevant residual exploitable vulnerabilities in the intended operating environment.



Results of the Evaluation

The Information Technology product identified in this certification report, and its associated certificate, has been evaluated at an approved testing laboratory established under the Canadian Centre for Cyber Security. This certification report, and its associated certificate, apply only to the specific version and release of the product in its evaluated configuration.

The overall verdict for this evaluation is **PASS**. These results are supported by evidence in the ETR.

Recommendations/Comments

It is recommended that all guidance be followed to configure the TOE in the evaluated configuration.



Supporting Content

List of Abbreviations

Term	Definition
ACVP	Automated Cryptographic Validation Protocol
CAVP	Cryptographic Algorithm Validation Program
CCTL	Common Criteria Testing Laboratory
CEC	Consumer Electronics Control
CMVP	Cryptographic Module Validation Program
CSE	Communications Security Establishment
EAL	Evaluation Assurance Level
EDID	Extended Display Identification Data
ESV	Entropy Source Validation
ETR	Evaluation Technical Report
HDMI	High-Definition Multimedia Interface
HEC	HDMI Ethernet Channel
IT	Information Technology
PP	Protection Profile
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function



References

Reference
Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5.
Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 5.
Evaluation Technical Report CYBEX SC Series Secure Micro Switches SC825SFF, SC925SFF, SC845SFF, SC945SFF, SC885SFF, SC985SFF, SCMV245SFF, SC825SFF-B-DP, SC825SFF-B-H, SC925SFF-B-DP, SC925SFF-B-H, SC845SFF-B-DP, SC845SFF-B-H, SC945SFF-B-DP, SC945SFF-B-H, SC885SFF-B-DP, SC885SFF-B-H, SC985SFF-B-DP, SC985SFF-B-H, SCMV245SFF-B-DP, SCMV245SFF-B-H Firmware Version 44044-M7M7, 6 August 2026, v0.8.
Security Target CYBEX SC Series Secure Micro Switches SC825SFF, SC925SFF, SC845SFF, SC945SFF, SC885SFF, SC985SFF, SCMV245SFF, SC825SFF-B-DP, SC825SFF-B-H, SC925SFF-B-DP, SC925SFF-B-H, SC845SFF-B-DP, SC845SFF-B-H, SC945SFF-B-DP, SC945SFF-B-H, SC885SFF-B-DP, SC885SFF-B-H, SC985SFF-B-DP, SC985SFF-B-H, SCMV245SFF-B-DP, SCMV245SFF-B-H Firmware Version 44044-M7M7, 5 August 2026, v1.0
Assurance Activity Report CYBEX SC Series Secure Micro Switches SC825SFF, SC925SFF, SC845SFF, SC945SFF, SC885SFF, SC985SFF, SCMV245SFF, SC825SFF-B-DP, SC825SFF-B-H, SC925SFF-B-DP, SC925SFF-B-H, SC845SFF-B-DP, SC845SFF-B-H, SC945SFF-B-DP, SC945SFF-B-H, SC885SFF-B-DP, SC885SFF-B-H, SC985SFF-B-DP, SC985SFF-B-H, SCMV245SFF-B-DP, SCMV245SFF-B-H Firmware Version 44044-M7M7, 6 August 2026, v0.8.

