Communications Security Establishment
Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR CYBER SECURITY

COMMON CRITERIA CERTIFICATION REPORT

Market Central SecureSwitch® Fiber Optic Switch Models: A, B, C, D, 1:1, 2:1, 3:1, 4:1, 5:1, 6:1, 7:1 and 8:1

21 January 2025

657-LSS

V1.1

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 determining the trustworthiness of Information Technology (IT) security 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. 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 security target, 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 security target are posted to the Common Criteria portal (the official website of the International Common Criteria Program).

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

Market Central SecureSwitch® Fiber Optic Switch Models: A, B, C, D, 1:1, 2:1, 3:1,4:1, 5:1, 6:1, 7:1 and 8:1 (hereafter referred to as the Target of Evaluation, or TOE), from **Market Central, Inc.** , was the subject of this Common Criteria evaluation. A description of the TOE can be found in Section 1.2. The results of this evaluation demonstrate that the TOE meets the requirements of the conformance claim listed in Section 1.1 for the evaluated security functionality.

Lightship Security is the CCTL that conducted the evaluation. This evaluation was completed on **21 January 2025** and was carried out 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 give due consideration to 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 (CPL) for the Canadian Common Criteria Program and the Common Criteria portal (the official website of the International Common Criteria Program).

1   IDENTIFICATION OF TARGET OF EVALUATION

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

Table 1:   TOE Identification

TOE Name and Version	Market Central SecureSwitch® Fiber Optic Switch Models: A, B, C, D, 1:1, 2:1, 3:1,4:1, 5:1, 6:1, 7:1 and 8:1
Developer	Market Central, Inc.

1.1   COMMON CRITERIA CONFORMANCE

The evaluation was conducted using the 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:

EAL 4+ with ALC_FLR.1

1.2   TOE DESCRIPTION

The TOE is an optical switch that allows a single host to connect to multiple networks, one at a time, while maintaining separation between the networks. The TOE user manually switches between networks.

The TOE uses an internal mirror switch to allow optical communications to travel between the common port and one of the selected network ports. Due to the use of fiber-optic signals and the mirrored switching mechanism design, the TOE provides an isolation of a minimum of 75dB between all unselected ports.

1.3   TOE ARCHITECTURE

A diagram of the TOE architecture is as follows:
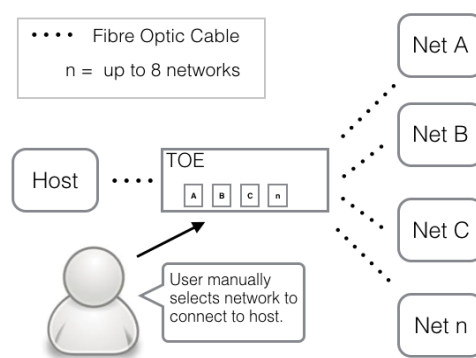
Figure 1: TOE Architecture

2   SECURITY POLICY

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

- Switching
- Isolation

Complete details of the security functional requirements (SFRs) can be found in the Security Target (ST) referenced in section 8.2.

2.1   CRYPTOGRAPHIC FUNCTIONALITY

The TOE does not utilize cryptography for any of its functions.

3 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.

3.1 USAGE AND ENVIRONMENTAL ASSUMPTIONS

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

- The User has connected up to eight (depending on TOE model) distinct networks to the TOE Network Ports. The User has connected a computer on the Common Port that has a full-duplex network interface.

- The User is non-hostile.

- The User follows all user guidance when using the TOE.

- The TOE will be located in an environment that provides physical security, uninterruptible power, and temperature control required for reliable operation of the hardware. TOE-connected optical cabling and equipment shall be protected from unauthorized physical access.
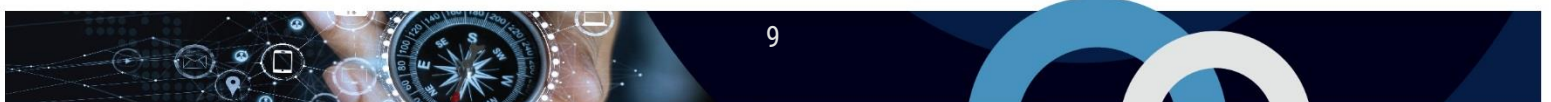
4   EVALUATED CONFIGURATION

The evaluated configuration for the TOE comprises of the following models:

Model	Part #
SecureSwitch® Revision A	5101180
	5101180-1U
	5101182
	5101182-1U
	5101183
	5101184
SecureSwitch® Revision B	5101185
	5101185-60
	5101185-1U
	5101185-1U-60
	5101186
	5101186-60
SecureSwitch® Revision C	5101191
	5101191-60
	5101191-1U
	5101191-1U-60
	5101192
	5101192-60
SecureSwitch® Revision D	5101177
	5101177-60
	5101177-1U
	5101177-1U-60
	5101178

Model	Part #
	5101178-60
SecureSwitch® 1:1 Fiber Optic Switch	5101720
	5101721
	5101722
	5101723
	5101753
	5101754
	5101755
	5101756
	5101766
	5101767
	5101782
	5101783
SecureSwitch® 2:1 Fiber Optic Switch	5101724
	5101725
	5101726
	5101727
	5101757
	5101758
	5101759
	5101760
	5101768
	5101769
	5101784
	5101785
SecureSwitch® 3:1 Fiber Optic Switch	5101728

Model	Part #
	5101729
	5101730
	5101731
	5101761
	5101762
	5101763
	5101764
	5101770
	5101771
	5101786
	5101787
SecureSwitch® 4:1 Fiber Optic Switch	5101700
	5101701
	5101702
	5101703
	5101733
	5101734
	5101735
	5101736
	5101772
	5101773
	5101788
	5101789
SecureSwitch® 5:1 Fiber Optic Switch	5101704
	5101705
	5101706

Model	Part #
	5101707
	5101737
	5101738
	5101739
	5101740
	5101774
	5101775
	5101790
	5101791
SecureSwitch® 6:1 Fiber Optic Switch	5101708
	5101709
	5101710
	5101711
	5101741
	5101742
	5101743
	5101744
	5101776
	5101777
	5101792
	5101793
SecureSwitch® 7:1 Fiber Optic Switch	5101712
	5101713
	5101714
	5101715
	5101745

Model	Part #
	5101746
	5101747
	5101748
	5101778
	5101779
	5101794
	5101795
SecureSwitch® 8:1 Fiber Optic Switch	5101716
	5101717
	5101718
	5101719
	5101749
	5101750
	5101751
	5101752
	5101780
	5101781
	5101796
	5101797

4.1   DOCUMENTATION

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

a) SecureSwitch® Fiber Optic A/B/C Switch Revision A Manual v1.3
b) SecureSwitch® Fiber Optic A/B/C Switch Revision B Manual v1.3
c) SecureSwitch® Fiber Optic A/OFF/C Switch Revision C Manual v1.3
d) SecureSwitch® Fiber Optic A/B/C Switch Revision D Manual v1.3
e) SecureSwitch® n:1 Fiber Optic Switch Products Manual v2.4

5 EVALUATION ANALYSIS ACTIVITIES

The evaluation analysis activities involved a structured evaluation of the TOE. Documentation and process dealing with Development, Guidance Documents, and Life-Cycle Support were evaluated.

5.1 DEVELOPMENT

The evaluators analyzed the documentation provided by the vendor; they determined that the security architecture description depicts the self-protection, domain separation, non-bypassability principles; the functional specification accurately describes and categorizes the TOE security functionality (TSF) interfaces, the implementation representation captures the detailed internal workings of the TSF, and the TOE design description provides appropriate level of decomposition. 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.

5.2 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 examined and tested the preparative and operational guidance and determined that they are complete and sufficiently detailed to result in a secure configuration.

Section 4.1 provides details on the guidance documents.

5.3 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 development security included appropriate security measures to protect the TOE and its parts, and an effective life-cycle model is in place.

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.
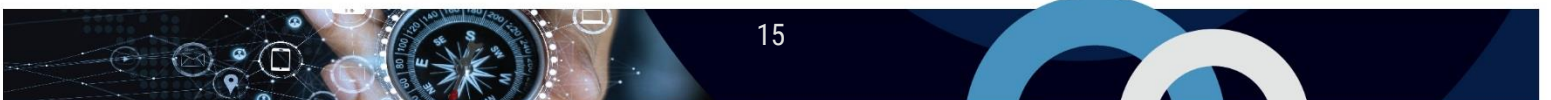
6 TESTING ACTIVITIES

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

6.1 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.

6.2 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 Test Results document.

6.3 INDEPENDENT TESTING

During this evaluation, the evaluator developed independent functional & 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. Repeat of Developer's Tests: The evaluator repeated a subset of the developer's tests

b. Testing of isolation functions: The evaluator confirmed that the switching function properly connects the common port to the selected network port and that the isolation function properly isolates the unselected network ports from the common port and network ports from each other.

6.3.1 INDEPENDENT TESTING RESULTS

The developer's tests and the independent tests yielded the expected results, providing assurance that the TOE behaves as specified in its ST and functional specification.
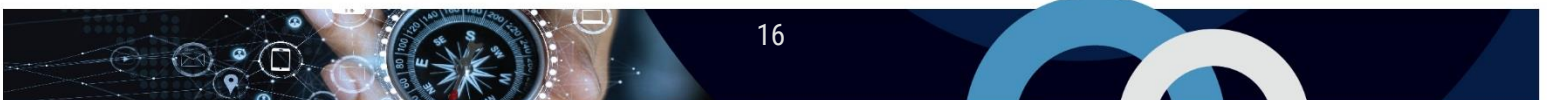
6.4   VULNERABILITY ANALYSIS

The vulnerability analysis focused on 4 flaw hypotheses.

- ⚙ Public Vulnerability based (Type 1)
- ⚙ Technical community sources (Type 2)
- ⚙ Evaluation team generated (Type 3)
- ⚙ Tool Generated (Type 4)

The evaluators conducted an independent review of all evaluation evidence, public domain vulnerability databases, technical community sources, and published literature (Type 1 & 2). Based upon this review, the evaluators formulated flaw hypotheses (Type 3), which they used in their vulnerability analysis.

Type 1 & 2 searches were conducted on **17 December 2024** and included the following search terms:

Market Central SecureSwitch
SecureSwitch

Vulnerability searches were conducted using the following sources:

Common Vulnerabilities and Exposures (CVE)	National Vulnerability Database
https://cve.mitre.org	https://nvd.nist.gov/vuln
CERT	Google
https://www.kb.cert.org/vuls/	https://www.google.com

6.4.1   VULNERABILITY ANALYSIS RESULTS

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

7   RESULTS OF THE EVALUATION

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. This certification report, and its associated certificate, apply only to the specific version and release of the product in its evaluated configuration.

This evaluation has provided the basis for the conformance claim documented in Section 1.1. The overall verdict for this evaluation is **PASS**. These results are supported by evidence in the ETR.

7.1   RECOMMENDATIONS/COMMENTS

It is recommended that all guidance outlined in Section 4.1 be followed to configure the TOE in the evaluated configuration.

8 SUPPORTING CONTENT

8.1 LIST OF ABBREVIATIONS

Term	Definition
CAVP	Cryptographic Algorithm Validation Program
CCTL	Common Criteria Testing Laboratory
CMVP	Cryptographic Module Validation Program
CSE	Communications Security Establishment
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
PP	Protection Profile
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function

8.2 REFERENCES

Reference
Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017.
Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 5, April 2017.
Market Central, Inc. SecureSwitch® Fiber Optic Switch Models: A, B, C, D, 1:1, 2:1, 3:1, 4:1, 5:1, 6:1, 7:1 and 8:1 Security Target Version 2.1, 8 July 2024
Market Central, Inc. SecureSwitch® Fiber Optic Switch Models: A, B, C, D, 1:1, 2:1, 3:1, 4:1, 5:1, 6:1, 7:1 and 8:1 Evaluation Technical Report, Version 1.1, 21 January 2025