Common Criteria Certification Report

Belkin F1DN102KVM-UNN4, F1DN202KVM-UNN4, F1DN104KVM-UNN4, F1DN204KVM-UNN4, F1DN202KVMUNN4M, F1DN204KVMUNN4M, F1DN104KVMUNN4Z, F1DN204KVMUNN4Z Firmware Version 44404-E7E7 Peripheral Sharing Devices

CAN-702-EWA

2 July 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

Executive Summary CAN-702-EWA

Belkin F1DN102KVM-UNN4, F1DN202KVM-UNN4, F1DN104KVM-UNN4, F1DN204KVM-UNN4, F1DN202KVMUNN4M, F1DN204KVMUNN4M, F1DN104KVMUNN4Z, F1DN204KVMUNN4Z Firmware Version 44404-E7E7 Peripheral Sharing Devices (hereafter referred to as the Target of Evaluation, or TOE), from **Belkin International, Inc.** , was the subject of this Common Criteria evaluation. The results of this evaluation demonstrate that the TOE meets the following conformance claim: **PP-Peripheral Sharing Devices Version 4.0; PP-Module for Analog Audio Output Devices, Version 1.0; PP-Module for Keyboard/Mouse Devices, Version 1.0; PP-Module for Video/Display Devices, Version 1.0.**

EWA-Canada is the CCTL that conducted the evaluation. This evaluation was completed on **2 July 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	Belkin F1DN102KVM-UNN4, F1DN202KVM-UNN4, F1DN104KVM-UNN4, F1DN204KVM-UNN4, F1DN202KVMUNN4M, F1DN204KVMUNN4M, F1DN104KVMUNN4Z, F1DN204KVMUNN4Z Firmware Version 44404-E7E7 Peripheral Sharing Devices
Developer	Belkin International, Inc.

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:

PP-Peripheral Sharing Devices Version 4.0; PP-Module for Analog Audio Output Devices, Version 1.0; PP-Module for Keyboard/Mouse Devices, Version 1.0; PP-Module for Video/Display Devices, Version 1.0.

TOE Description

The TOE is the Belkin Universal 2nd Generation Secure KVMs family of secure peripheral sharing devices (PSDs). The TOE is a combined hardware and firmware PSD that allows users to securely share a USB keyboard, USB mouse, video display, and analog audio output device among connected computers.

Depending on model, the TOE supports two or four connected computers, either one or two connected displays using DisplayPort or HDMI interfaces and can also be used with an optional wired remote control device.

TOE Architecture

A diagram of the TOE architecture is as follows:

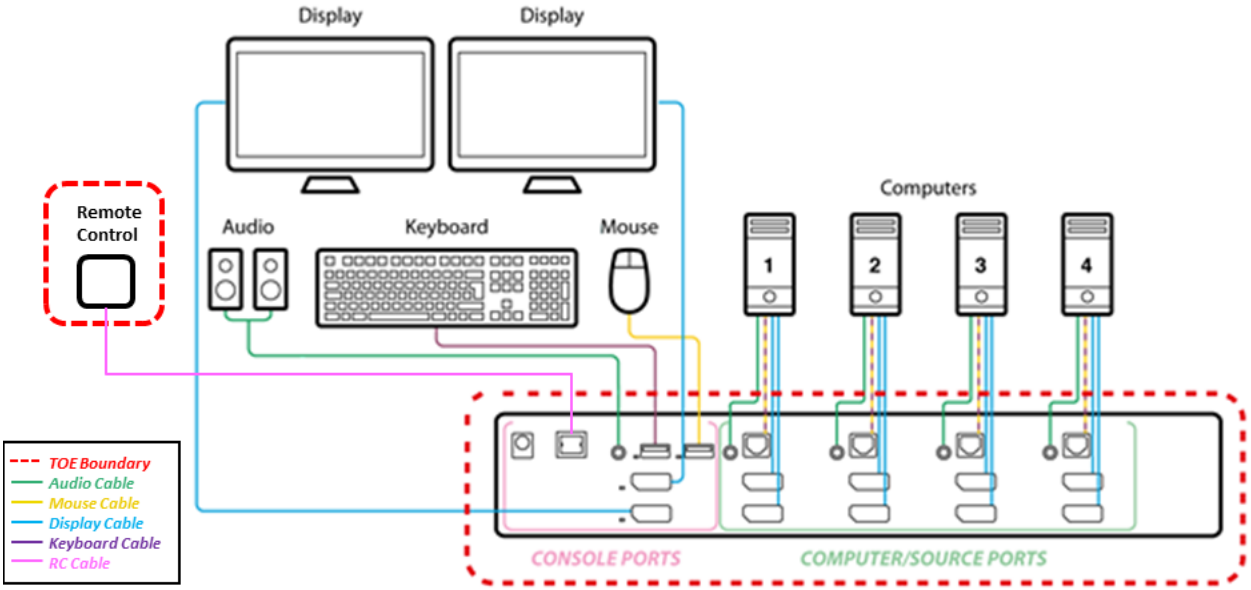

Figure 1: TOE Architecture

Security Policy

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

- Security Audit
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TSF
- TOE Access

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. For keyboard and mouse computer interfaces, the TOE may or may not isolate the USB ground, and the operational environment is assumed not to support TEMPEST red-black ground isolation.
- 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 networks, are expected to provide any required authentication and access control for their resources.
- The computers connected to the TOE are not equipped with special analog data collection cards or peripherals, such as analog-to-digital interfaces, high-performance audio interfaces, digital signal processing functions, or analog video capture functions.
- Users are trained not to connect a microphone to the TOE audio output interface.

Clarification of Scope

All security features of this product were evaluated.

Evaluated Configuration

The evaluated configuration for the TOE comprises:

Table 2: Evaluated Configuration

TOE Peripheral Sharing Devices	• F1DN102KVM-UNN4 P/N CGA18345 • F1DN202KVM-UNN4 P/N CGA18347 • F1DN202KVMUNN4M P/N CGA30643 • F1DN104KVM-UNN4 P/N CGA18346 • F1DN104KVMUNN4Z P/N CGA33050 • F1DN204KVM-UNN4 P/N CGA18349 • F1DN204KVMUNN4M P/N CGA30644 • F1DN204KVMUNN4Z P/N CGA33055
TOE Remote Control Devices	• F1DN-KVM-REM2 P/N CGA33637 • F1DN-KVM-REM4 P/N CGA33638
Environmental Support	• 2-4 general purpose computers • General purpose USB keyboard • General purpose USB mouse • Analog audio output device (speakers or headphones) with a 3.5 mm TRS connector • Standard computer display (DisplayPort 1.1, 1.2, or 1.3) • Standard computer display (HDMI 2.0)
Cables	• USB Type-A to USB Type-B cable for keyboard and mouse • DisplayPort or HDMI video cable • 3.5 mm stereo TRS audio cable

Documentation

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

a) Quick Installation Guide 2/4 Port Secure Single/Dual-Head DP/HDMI-DP/HDMI KVM Switches, 8820-02951 Rev. A02
b) Belkin Administrator Guide, LNKPG-00666 Rev. C04
c) Belkin F1DN102KVM-UNN4, F1DN202KVM-UNN4, F1DN104KVM-UNN4, F1DN204KVM-UNN4, F1DN202KVMUNN4M, F1DN204KVMUNN4M, F1DN104KVMUNN4Z, F1DN204KVMUNN4Z Firmware Version 44404-E7E7 Peripheral Sharing Devices Common Criteria Guidance Supplement, Version 1.7

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 & 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. Based upon this review, the evaluators formulated flaw hypotheses , which they used in their vulnerability analysis.

Public domain searches were conducted on **27 May 2026** and included the following search terms:

Belkin	Highseclabs	KVM-UNN4
HDMI	highseclabs KVM	KVMUNN4M
EDID	highseclabs switch	KVMUNN4Z
HEC	44404-E7E7	F1DN-KVM-REM
DisplayPort	peripheral sharing	HDMI ARC
HSL	STM32F44	HDMI-ARC
HDMI CEC	STM32C07	HDMI-CEC
High Sec Labs	STM32F07	MCCS

Vulnerability searches were conducted using the following sources:

National Vulnerability Database https://nvd.nist.gov/vuln/search	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
CCTL	Common Criteria Testing Laboratory
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

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.
Belkin F1DN102KVM-UNN4, F1DN202KVM-UNN4, F1DN104KVM-UNN4, F1DN204KVM-UNN4, F1DN202KVMUNN4M, F1DN204KVMUNN4M, F1DN104KVMUNN4Z, F1DN204KVMUNN4Z Firmware Version 44404-E7E7 Peripheral Sharing Devices Security Target, Version 1.1, 2 July 2026
Evaluation Technical Report Common Criteria Evaluation of Belkin F1DN102KVM-UNN4, F1DN202KVM-UNN4, F1DN104KVMUNN4, F1DN204KVM-UNN4, F1DN202KVMUNN4M, F1DN204KVMUNN4M, F1DN104KVMUNN4Z, F1DN204KVMUNN4Z Firmware Version 44404-E7E7 Peripheral Sharing Devices, Version 1.0, 2 July 2026
Assurance Activity Report Belkin F1DN102KVM-UNN4, F1DN202KVM-UNN4, F1DN104KVM-UNN4, F1DN204KVM-UNN4, F1DN202KVMUNN4M, F1DN204KVMUNN4M, F1DN104KVMUNN4Z, F1DN204KVMUNN4Z Firmware Version 44404-E7E7 Peripheral Sharing Devices, Version 1.0, 2 July 2026