Belkin F1DN002MOD-KM-4, F1DN004MOD-KM-4, F1DN-FLTR-HID-4 Firmware Version 40404-0E7 Peripheral Sharing Devices

Common Criteria Guidance Supplement

Doc No. 2149-001-D105B4
Version: 1.4
1 October 2021

Belkin International, Inc.
12045 E. Waterfront Drive
Playa Vista, CA 90094 USA

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

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

Upon receipt of the Belkin 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 Belkin 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.

4 SECURE OPERATION

This section describes the steps necessary for the secure operation of the Belkin Peripheral Sharing Devices with Keyboard and Mouse.

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 initiate a self test by following the procedures outlined in Table 1 for the applicable device type. In the case of a self test failure, users are directed to contact Belkin Technical Support.

Device Model	Procedure
F1DN002MOD-KM-4 F1DN004MOD-KM-4	1. To enter self test 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/mouse USB ports are disabled. 2. To exit self test mode, cycle the power.
F1DN-FLTR-HID-4	1. To enter self test mode, connect an unauthorized peripheral device, and power on the TOE device. The LED on the front panel flashes. 2. To exit self test mode, cycle the power.

Table 1 – Procedure to Initiate a Self Test

4.2 SELECTED CHANNEL AT STARTUP

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