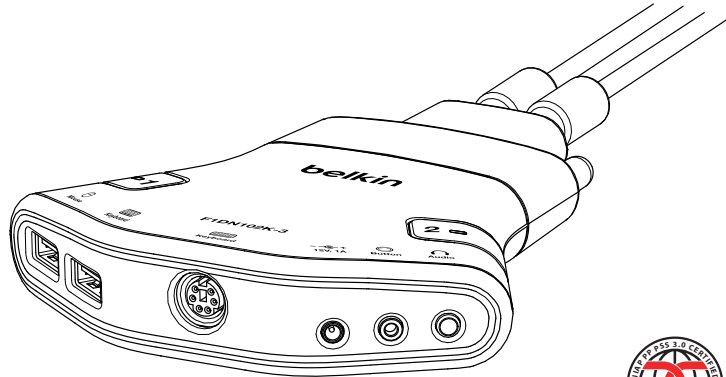




Secure Flip 2-Port Keyboard/Mouse (KM) Switch



This Belkin product is compliant with latest NIAP Protection Profile PSS Ver. 3.0, which exceeds EAL4 and PP PSS Ver. 2.1.

User Manual

F1DN102K-3 – Belkin Secure Flip 2-Port KM Switch

TABLE OF CONTENTS

Table of Contents	SECTIONS	1	2	3	4	5	6
Introduction		1					
Package Contents		1					
Overview		2					
Security Features		2					
Operational Features		3					
What is Seamless Cursor Switching?		5					
Equipment Requirements		6					
Safety Precautions		8					
User Guidance & Precautions		9					
Tamper Evident Labels		10					
Product Specifications		11					
F1DN102K-3 Features		12					
Installation							13
Before Installation							13
Setup							14
Operation							20
Operating the Secure KM Switch							20
Troubleshooting							22
Information							24

INTRODUCTION

Thank you for purchasing this Belkin Advanced Secure 2-port Flip Keyboard/Mouse (KM) Switch. This Switch is designed for use in secure environments comprised of sources with different security levels. Providing the highest security safeguards and features, this product meets all required cyber prevention requirements.

This User Manual provides all the details you'll need to install and operate your new product and to troubleshoot it in the unlikely event of a problem.

What is a KM (Keyboard / Mouse) Switch?

A KM switch is essentially a KVM switch without the video switching.

The Belkin Advanced Secure 2-port Flip KM Switch is a winning combination of cost effectiveness with an exceptionally small footprint product.

The switch targets environments with 2 sources, where each computer is connected to separate display/s. It suits scenarios where information from multiple sources must be viewed simultaneously on the different displays. Every computer can be connected to up to 4 displays.

The KM switch securely toggles control of keyboard, mouse and audio from one system to the other. Intuitive navigation is provided by Seamless Cursor Switching (SCS) - once mouse cursor crosses display borders, the Mouse, Audio and Keyboard become active on the system connected to that display. The product can be easily configured by using the KM presets.

The Belkin Secure KM supports all operating systems, from Windows to Linux and Mac OS. Multi-Displays are only supported by computers running Windows based operating systems.

Package Contents

- Belkin Secure Flip KM Switch
- 12V 1A DC Power Supply
- User Manual

Please note: Belkin Secure KM Products cannot be upgraded, serviced or fixed.

Important Security Note: If you are aware of potential security vulnerability while installing or operating this product, we encourage you to contact us immediately at the following email address: gov_security@belkin.com

Important: This product is equipped within always-on active anti-tamper system. Any attempt to open the enclosure may activate the anti-tamper system and render the unit permanently inoperable. If the unit's enclosure appears disrupted or if all the port LEDs flash continuously, please call Belkin Technical Support at **1 (800) 282-2355**

OVERVIEW

Security Features

Product is designed, manufactured and delivered in security-controlled environments. Below is a summary of the main advanced features incorporated in product:

Advanced isolation between computers and shared peripherals

The emulations of keyboard, mouse and display EDID, prevent direct contact between computers and shared peripherals. Product design achieves maximal security by keeping the video path separate with keyboard and mouse switched together, purging keyboard buffer when switching channels. All these features contribute to strong isolation between computer interfaces, maintained even when product is powered off.

Unidirectional data flow: USB, audio and video

Unique hardware architecture components prevent unauthorized data flow, including:

- Optical unidirectional data flow diodes in the USB data path that filtrate and reject unqualified USB devices;
- Secure analog audio diodes that prevent audio eavesdropping with no support for microphone or any other audio-input device;
- Video path is kept separate from all other traffic, enforcing unidirectional native video flow. EDID emulation is done at power up and blocks all EDID/MCCS writes. For DisplayPort video, filtration of AUX channel exists to reject unauthorized transactions.

Isolation of power domains

Complete isolation of power domains prevents signaling attacks.

Secure administrator access & log functions

Product incorporates secure administrator access and log functions to provide auditable trail for all product security events, including battery backup life for anti-tampering and log functions. Non-reprogrammable firmware prevents the ability to tamper with product logic.

Always-on, active anti-tamper system

Active anti-tampering system prevents hardware implants and wireless key-loggers. Any anti-tampering attempt causes isolation of all computers and peripheral devices rendering product inoperable and showing clear indications of tampering event to user.

Holographic security tamper-evident labels are placed on the enclosure to provide a clear visual indication if product has been opened or compromised.

Metal enclosure is designed to resist mechanical tampering with all microcontrollers protected against firmware-read, modification and rewrite.

Secure Packaging

“Tear away” packaging ensures secure delivery of the Switch as it is routed to the end user. The recyclable packaging also breaks down flat, simplifying the cleanup process.

OVERVIEW

Operational Features

The F1DN102K-3 was designed with the user in mind for today's IT environment. Below is a summary of some of the features incorporated into the Product.

Dedicated, cost effective design for 2 computer scenarios

The Belkin Secure 2-port Flip KM Switch is based on a dedicated design for 2-computer scenarios: cost effective and compact footprint, weighing as little as ~1 lbs., sized ~4X3X1 Inches.

Seamless Cursor Switching (SCS)

SCS allows the KM to switch automatically between computers once mouse cursor crosses display borders. The switching is seamless between multiple computers with cursor movement.

Lag-free, real-time switching

A hardware-based solution eliminates keyboard and mouse delays when switching between ports, offering a fluid and uninterrupted user experience.

Audio Support

The Belkin Secure KM Switch supports audio out switching. Microphone switching is not supported to prevent analog leakages through audio ports.

Port Coloring

The F1DN102K-3 has two illuminate channel select push buttons colored in white for easy selection and clear indication of channels.

Increased Reliability

Using a new, advanced anti-tampering battery with extremely low self-discharge rate the life expectancy of the switch has been increased dramatically to over 25 years

No Cables required

No cables are required with the F1DN102K-3 as all cables are part of the product making it an easy to install and a cost effective product.

Bloomberg Keyboard Support

The F1DN102K-3 has one additional PS/2 keyboard port for easy support for Bloomberg keyboards required for financial traders.

Multi monitor support and easy setup

user can choose between 25 pre-defined monitor setups to reflect actual physical display positioning.

OVERVIEW

Table of Contents

SECTIONS

1

2

3

4

5

6

Top security

Achieved by dedicated processors with emulators for every port creating isolated port paths for video, audio and peripherals to prevent data leaks between computers.

Unidirectional data paths

Optical data diodes prevent peripherals from being used to breach systems.

Peripheral management

USB device detection prevents unauthorized peripheral usage.

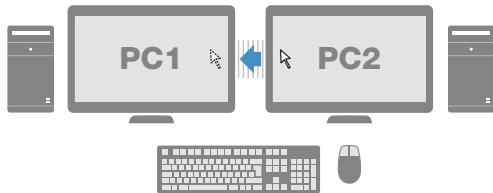
OVERVIEW

What is Seamless Cursor Switching?

Seamless Cursor Switching (SCS) is implemented in Belkin Advanced Secure KM Switch to enable seamless cursor and keyboard switching between multiple displays. Simply move the mouse cursor across neighboring displays to switch between connected computers.

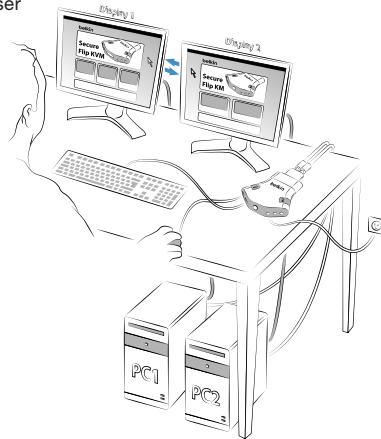
Every system is alive and visible on its own display/s while mouse and keyboard are only active on one. The Belkin Advanced Secure 2-port Flip KM Switch keeps the two systems isolated and secure. Multi monitor function is supported and each computer system can be connected to up to 4 displays.

User can choose between 25 pre-defined monitor setups to reflect actual physical display positioning.



Flip KM

- Belkin® Secure 2-Port Flip **K**M Switch controls **K**eyboard and **M**ouse
- Displays are connected directly to the computers
- User operates computers using a single set of keyboard and mouse
- The user can simultaneously view both computers
- Switching control between computers can be done via:
 - SCS (Seamless Cursor Switching) – as mouse cursor moves from one display to the other
 - Switch control push-buttons



OVERVIEW

Equipment Requirements

Operating Systems

Product is compatible with devices running on the following operating systems:

- Microsoft® Windows®
- Red Hat®, Ubuntu® and other Linux® platforms
- Mac OS® X v10.3 and higher.

USB Keyboard console port

The product console USB keyboard port is compatible with Standard USB keyboards.

Notes:

- a. Console USB keyboard and mouse ports are switchable, i.e. you can connect keyboard to mouse port and vice versa. However, for optimal operation it is recommended to connect USB keyboard to console USB keyboard port and USB mouse to console USB mouse port.
- b. For security reasons products do not support wireless keyboards. In any case do not connect wireless keyboard to product.
- c. Non-standard keyboards, such as keyboards with integrated USB hubs and other USB-integrated devices, may not be fully supported due to security policy. If they are supported, only classical keyboard (HID) operation will be functional. It is recommended to use standard USB keyboards.

USB Mouse console port

The product console USB mouse port is compatible with standard USB mice.

Notes:

- a. Console USB keyboard and mouse ports are switchable, i.e. you can connect keyboard to mouse port and vice versa. However, for optimal operation it is recommended to connect USB keyboard to console USB keyboard port and USB mouse to console USB mouse port.
- b. Console USB mouse port supports Standard KVM Extender composite device having a keyboard/mouse functions.
- c. For security reasons products do not support wireless mice. In any case do not connect wireless mouse to product.

OVERVIEW

User Audio Devices

Product is compatible with the following types of user audio devices:

- Stereo headphones;
- Amplified stereo speakers.

Note: In any case do not connect a microphone to product audio output port including headsets.

Cables

No cables are required with the F1DN102K-3 as all cables are part of the product.

USB Mouse, keyboards and audio molded cables

The F1DN102K-3 includes two sets of USB and audio cables, one for each connected PC. The USB connectors on the client side of these computers are of type USB-A and audio 3.5mm jacks.

Reporting Belkin Product Security Vulnerability

If you are aware of potential security vulnerability with any Belkin Government product, we encourage you to contact us immediately at the following email address: gov_security@belkin.com or our technical support line at: **1-800-282-2355**

After your communication is received, Belkin Government personnel will contact you to follow up. To ensure confidentiality, Belkin encourages you to use PGP encryption key for secure communications.

The gov_security@belkin.com email address is not intended to reach technical support on Belkin Government products or services.

OVERVIEW

Safety Precautions

Please read the following safety precautions carefully before using the Belkin Secure KM:

- Before cleaning, disconnect the product from any electrical power supply.
- Do not expose the product to excessive humidity or moisture.
- Do not store or use for extensive period of time in extreme thermal conditions – it may shorten product lifetime.
- Install the product only on a clean secure surface.
- If the product is not used for a long period of time, disconnect it from electrical power.
- If any of the following situations occurs, have the product checked by a qualified service technician:
 - Liquid penetrates the product's case.
 - The product is exposed to excessive moisture, water or any other liquid.
 - The product is not working well even after carefully following the instructions in this user's manual.
 - The product has been dropped or is physically damaged.
 - The product shows obvious signs of breakage or loose internal parts.
 - In case of external power supply – If power supply overheats, is broken or damaged, or has a damaged cable.
- The product should be stored and used only in temperature and humidity controlled environments as defined in the product's environmental specifications.
- Never attempt to open the product enclosure. Any attempt to open the enclosure will permanently damage the product.
- The product contains a non-replaceable internal battery. Never attempt to replace the battery or open the enclosure.
- This product is equipped with an always-on active anti-tampering system. Any attempt to open the product enclosure will activate the anti-tamper triggers and render the unit inoperable and warranty void.

User Guidance & Precautions

Please read the following User Guidance & Precautions carefully before using the product:

1. As product powers-up it performs a self-test procedure. In case of self- test failure for any reason, including jammed buttons, the product will be Inoperable. Self-test failure will be indicated by the following abnormal LED behavior:
 - a. All channel-select LEDs will be turned ON and then OFF;
 - b. A specific, predefined LED combination will be turned ON;
 - c. The predefined LED combination will indicate the problem type (jammed buttons, firmware integrity).

Try to power cycle product. If problem persists please contact your system administrator or technical support.
2. By default, after product power-up, the active channel is #1.
3. The appropriate usage of peripherals (e.g. keyboard, mouse, display, authentication device) is described in detail in this User Manual's appropriate sections. Do not connect any authentication device with an external power source to product.
4. For security reasons products do not support wireless keyboards and mice. In any case do not connect wireless keyboard/mouse to product.
5. For security reasons products do not support microphone/line-in audio input. In any case do not connect a microphone to product audio output port, including headsets.
6. Product is equipped with an always-on active anti-tampering system. Any attempt to open product enclosure will activate the anti-tamper system indicated by all channel-select LEDs flashing continuously. In this case, product will be inoperable and warranty void. If product enclosure appears disrupted or if all channel- select LEDs flash continuously, please remove product from service immediately and contact technical support.
7. Connecting external USB devices to product CAC port:
 - a. When connecting a USB device that is not qualified or rejected for security reasons to product's CAC port, the CAC LED will flash green and USB device will be inoperable.
 - b. When connecting a USB device that is undetectable for any reason (e.g. failed device, non-standard device etc.) to product's CAC port, the CAC LED will not illuminate at all and device will be inoperable.
8. Do not connect product to computing devices:
 - a. That include telecommunication equipment;
 - b. That include frame grabber video cards;
 - c. That include special audio processing cards.

OVERVIEW

Table of Contents

SECTIONS

1

2

3

4

5

6

User Guidance & Precautions (Con.)

9. **Important!** Before re-allocating computers to channels, it is mandatory to power cycle product, keeping it powered OFF for more than 1 minute.
10. Product log access and administrator configuration options are described in product Administrator Guide.
11. If you are aware of any potential security vulnerability while installing or operating product, please remove product from service immediately and contact us in one of the ways listed in this manual.

Tamper Evident Labels

Belkin Secure Switch uses holographic tamper evident labels to provide visual indications in case of enclosure intrusion attempt.

If for any reason the tamper evident seal is missing, appears disrupted, or looks different than the example shown here, please avoid using product and call Belkin Technical Support at: **(800) 282-2355**.

Active Anti-Tampering System

Belkin Secure Switch is equipped with always-on active anti-tampering system. If mechanical intrusion is detected by this system, the Switch will be permanently disabled and LED will blink continuously.

If product indication tampered state (all LEDs blinking) - please call Technical Support and avoid using that product

Product Enclosure Warning Label

Belkin Secure Switch has the following warning printed next to the location of the product Asset Tag and Tamper Evident labels on product enclosure:

WARNING: This enclosure is tamper proof. The unit will self destruct if opened.

Tamper Evident Label
Do not use if disturbed.



OVERVIEW

Table of Contents

SECTIONS

1

2

3

4

5

6

Product Specifications

Part No.	F1DN102K-3
No. of Users Supported	1
No. of Computers Supported	2
Power Requirements	12V DC, 1A (maximum) power adapter with center-pin-positive polarity
AC Input Voltage	100 to 240VAC
Console Keyboard Input	USB Type A / PS/2. Bloomberg keyboard supported
Console Mouse Input	USB Type A
Console Audio output jack	1/8" (3.5mm) female
Computer Keyboard/Mouse wire	USB Type A
Computer wire length	6 ft [1.8 meters] – channel 1 6 ft [1.8 meters] – channel 2
Computer Audio Input Jack	1/8" (3.5mm) male
Port Selector illuminated push-buttons	2
User Channel Selection Methods	Push-buttons, SCS
Operating Temp	32° to 104° F (0° to 40° C)
Storage Temp	-4° to 140° F (-20° to 60° C)

Humidity	0-80% RH, non-condensing
Dimensions	4.3 (W) x 3 (D) x 1 (H) inch/ 110 (W) X 80 (D) X 25(H) mm
Weight	1.2 lbs. / 0.56 KG
OS	Windows, Linux, MAC OS
Made In	Designed in California. Assembled in US with US and Foreign components.
Product life-cycle	5 years
Warranty	3 Years
Enclosure	Impact Resistant ABS Plastic
Security Accreditation	Common Criteria Validated To NIAP Protection Profile PSS Ver. 3.0

OVERVIEW

Table of Contents

SECTIONS

1

2

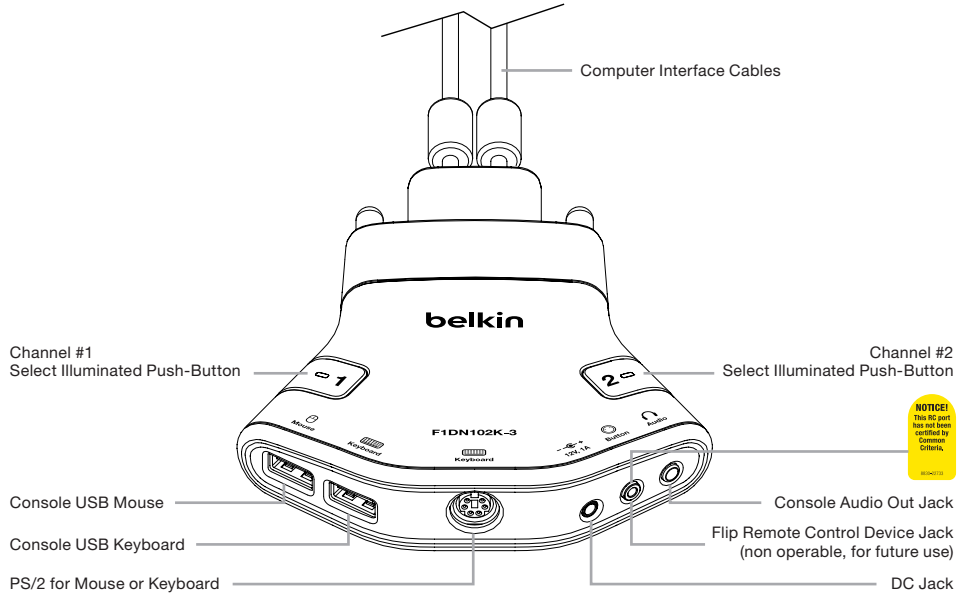
3

4

5

6

F1DN102K-3 Features



INSTALLATION

Before Installation

Unpacking the Product

Before opening the product packaging, inspect the packaging seal condition to assure that product was not accessed or tampered during delivery. If the packaging seal looks suspicious, contact Belkin Technical Support and do not use the product.

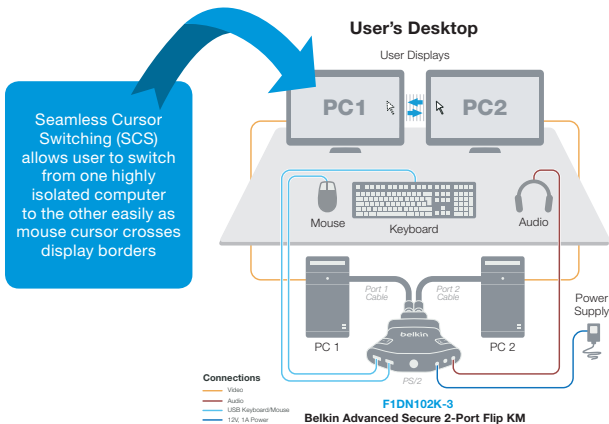
After removing the packaging seal, please inspect packaging content to verify that required components are included as listed in the Package Contents of this manual.

After the Secure KM Switch is removed from its packaging materials, inspect the tampering-evident label to assure that product is properly sealed. If one or more label is damaged or missing, contact Belkin Tech Support and do not use that product.

Consider the following when deciding where to place the Switch:

- Access to the front-panel push buttons
- The lengths of the cables attached to your keyboard and mouse
- The location of your computers in relation to your console

Warning: Avoid placing cables near fluorescent lights, air-conditioning equipment, or machines that create electrical noise (e.g., vacuum cleaners).



1. Monitors are connected directly to computers 1 & 2
2. Computers are connected to the Switch ports 1 & 2
3. Keyboard and Mouse are connected to the console section of the switch:
 - USB keyboard and mouse
 - Optionally PS/2 or Bloomberg keyboard
4. User headphones or amplified speakers are connected to audio-out port on the console section of the switch

Setup

Important:

1. If the unit's enclosure appears disrupted or if all channel-select LEDs flash continuously, please remove product from service immediately and contact Belkin Technical Support at **(800) 282-2355**.
2. Do not connect product to computing devices:
 - a. That include telecommunication equipment;
 - b. That include frame grabber video cards;
 - c. That include special audio processing cards.

Step 1 – Connecting Peripherals to the Secure KM Switch

Warning: Before attempting to connect anything to the Switch or computers, please ensure all devices are powered off.

- 1.1 Connect monitors directly to computers. For easier referencing, you can label each computer and monitor coupled together (e.g. PC1-Monitor1, etc.).
- 1.2 Connect the user keyboard to the Console section of the Switch.
Connect USB keyboards to the USB port marked "Keyboard."
Connect PS/2 and Bloomberg keyboards to the PS/2 port.
- 1.3 Connect the user mouse to the Console section of the Switch.
Connect USB mice to the USB port marked "Mouse".

Note: The Switch will not operate properly if the keyboard and mouse are not connected to their respective ports. The mouse USB console port supports both keyboard and mouse.

For security reasons, only standard keyboard functions are supported. Keyboards functions such as integrated USB hubs, card-readers, storage devices or multimedia extensions are not supported.

- 1.4 Connect user headphone or amplified speakers to the console audio output port marked "Audio".

Important: As the unit powers up it performs a self-test procedure. In case the self- test has failed for any reason the product LED behavior will be abnormal as described in User Guidance section. Try to power cycle the unit. If problem persists please contact your system administrator or Technical Support.

Caution: Do not connect a microphone to the audio output port. It is not supported for security reasons.

Step 2 – Connecting Computers to the Secure KM Switch

- 2.1 Connect the switch to two computers via product's molded wires. For USB, select any available functional USB port on the computer. For audio connect to available audio output jack (lime green color) or line output jack (blue color).

Step 3 – Powering Up

- 3.1 Power up the monitors.
- 3.2 Connect the product to the cable DC plug of the 12V 1A external AC/DC power supply.
- 3.3 Power up the two computers, and check display and peripheral functionality.

Notes: Your computers should recognize the Secure KM Switch and automatically install the HID USB driver if necessary.

Check that keyboard and mouse are working properly on each computer. If you encounter a problem, please check the cable connections to that computer and reboot. If problem persists, please refer to the Troubleshooting section in this Manual.

Configuration

Once the Secure KM Switch is connected and powered ON, you will need to configure the main settings of the product.

The first and most important setting is monitor positioning. For proper operation, it is essential to have compatibility between the Switch configuration and the actual positioning of the monitors. Setting monitor positioning is done by using one of the pre-defined presets available.

Selecting one of the predefined presets

To load one of the default settings available in the non-volatile memory of the Switch:

1. Select a default configuration type on the console keyboard by pressing "Control, Control, F11, Fx". Please refer to figure 1.
2. Power-cycle the Switch by disconnecting the power plug and reconnecting it to the Switch.
3. The Switch will boot with the new configuration.

Note: Additional settings can be accessed through pressing "Control, Control, F11, x, y". Please refer to figure 2.

The loaded configuration will include the following settings by default:

- All displays are 1920 x 1200 resolution, same size (26" diagonal)
- Mouse acceleration – set to 6
- Mouse speed – set to 5
- SCS – enabled
- Prevent transition while dragging feature – enabled

INSTALLATION

Examples for using predefined presets:

Note: See the complete list of preset options in figures 1 & 2.

F11, F1 is the default configuration. Two computers with single display each that are arranged as shown:



For example, the combination **Ctrl, Ctrl, F11, F5** will allow the following configuration:



In this setup, computer (1) has a single display while computer (2) has two displays.

Note: Only Windows computers support multiple displays with the KM.

The combination of **Ctrl, Ctrl, F11, F3** will apply the following:



In this setup, computer (1) has 2 displays and computer (2) has 2 displays.

Click F2 through F10 to select a preset configuration as listed in the table below.

Note: In the preset configurations, **Gray** indicates a single-display computer and **Blue** indicates a multi-display computer. **P** indicates primary display and **S** indicates secondary display in multi-display configurations.

F11, F1		F11, F6	
F11, F2		F11, F7	
F11, F3		F11, F8	
F11, F4		F11, F9	
F11, F5		F11, F10	

Figure 1 – (Pre-Defined Configuration List - Using CTRL, CTRL, F11, Fx)

INSTALLATION

Table of Contents

SECTIONS

1

2

3

4

5

6

Additional settings can be accessed through pressing the following keys on the console keyboard: **Ctrl + Ctrl + F11 + X + Y**.

After selecting a new configuration, disconnect and reconnect electrical power to apply this new configuration.

1, 1 is the default configuration. 2 computers, computer (1) with dual display and computer (2) with single display are arranged as shown below.



Click **1, 2** through **2, 4** to select a preset configuration as listed in the figure below.

Note: Only Windows computers support multiple displays with the KM.

For example, press **Ctrl, Ctrl, F11, 1, 0** to set the configuration below:



Computer (1) has two displays while Computer (2) has four displays.

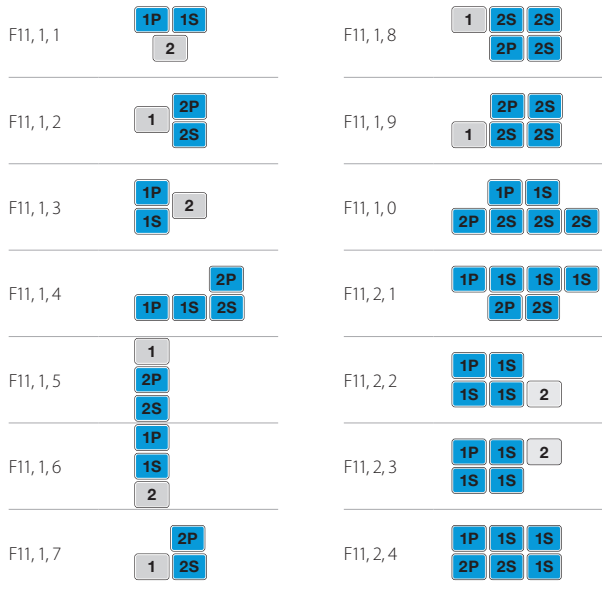


Figure 2 – (Pre-Defined Configuration List - Using CTRL, CTRL, F11, x, y)

INSTALLATION

Mouse Speed Setting

Constant mouse cursor speed is essential for system usability. Having several systems, each with a different cursor “ground speed”, causes usability problems.

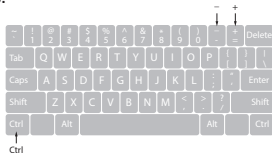
The Flip KM is designed to calculate and adjust cursor speed across different displays and computers by using geometry and display settings information entered by the administrator. The mouse speed setting can be further updated based on user inputs.

To increase mouse speed, press CTRL, CTRL, F11, +

To decrease mouse speed, press CTRL, CTRL, F11, -

Note:

- The “+” key referred to is the “=” key located next to the “backspace” on EN-US keyboards.
- The “-” key referred to is located next to the “0” key on EN-US keyboards.
- The CTRL key referred to in this manual is the **LEFT CTRL** key.



SCS Enabled / Disabled Setting

By choosing “SCS disabled” property one can disable mouse cursor Seamless Cursor Switching function. In this situation the Switch will enable channel selection only through:

- Switch push-buttons

Note: The SCS function is enabled by default.

Multiple-Head Display Driver Installation

For proper multi-display function of the KM, the Mouse Filter driver must be installed on the computer connected to multiple displays. This driver is available as an .exe file on Belkin website. In case Internet access is blocked in your organization, please contact Belkin to order the KM Switch programming CD Kit.

Keyboard Shortcuts

The following table describes the keyboard shortcuts available:

Key Sequence	Name	Description
CTRL, CTRL, F11, r	Reset to Factory defaults	Device will reset to Factory Default
CTRL, CTRL, F11, f	Freeze	Disable SCS. Switching between systems will not be possible via mouse movement.
CTRL, CTRL, F11, U	Unfreeze	Enable SCS. Switching between systems will be possible via mouse movement.
CTRL, CTRL, F11, +	Increase mouse speed	Mouse speed will be increased.
CTRL, CTRL, F11, -	Decrease mouse speed	Mouse speed will be decreased

OPERATION

Operating the Secure KM Switch

Self-Test Procedure

As product powers-up it performs a self-test procedure. In case of self- test failure for any reason, including jammed buttons, the product will be Inoperable. Self-test failure will be indicated by the following abnormal LED behavior:

- All channel-select LEDs will be turned ON and then OFF;
- A specific, predefined LED combination will be turned ON;
- The predefined LED combination will indicate the problem type (jammed buttons, firmware integrity).

Try to power cycle product. If problem persists please contact your system administrator or technical support.

Cursor Tracking (SCS Enabled)

Upon powering up, the cursor will be positioned at the center of the primary display of computer #1.

The keyboard and audio will be coupled to the same PC where the cursor is active.

Once the user moves the cursor to another display, the keyboard and audio will follow and move to that computer.

Illuminated Push Buttons

The default channel is #1 upon powering up.

The user can select the other channel by pressing the other push button. The mouse cursor will be positioned at the center of the selected computer display.

If computer has multiple heads, the cursor will be positioned at the center of the primary display.

The selected channel is indicated by the appropriate push button being illuminated.

The keyboard and audio will follow the selected channel once pressing the push button.

“Prevent transition while dragging” feature

The F1DN102K-3 offers a unique feature that further improves usability – “Prevent Transition while dragging”.

If the user drags an object on one display holding the left mouse key pressed, the cursor will remain in that display, even if the border of display is reached. That is – this function disables momentarily the SCS function.

This feature targets to prevent unintentional crossing of cursor to the other display when dragging an object and accidentally crossing display border.

OPERATION

Table of Contents

SECTIONS

1

2

3

4

5

6

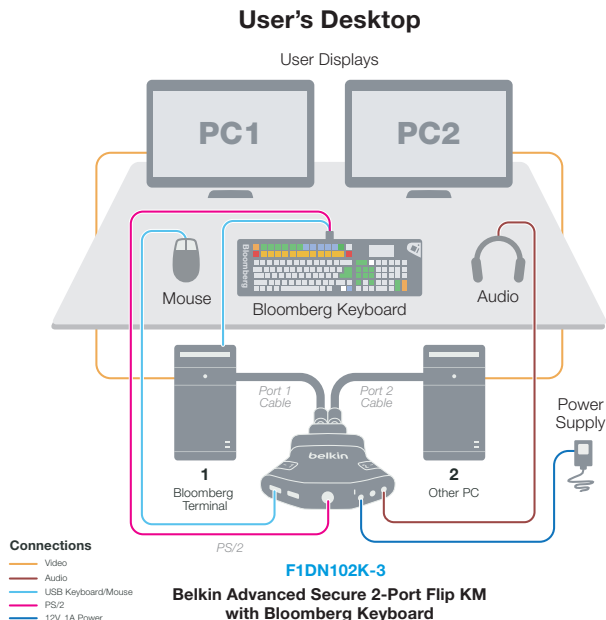
Cursor Acceleration and Speed

Cursor acceleration and speed combines a few factors, such as display size, resolution and static settings. If the current settings are not constant across the different displays or are not working properly, please ask your system administrator for assistance. Both cursor acceleration and speed can be set by the administrator to achieve optimal operation.

Working with the KM Switch connected to Bloomberg Keyboard

When using the Belkin Secure KM switch Connected to a Bloomberg Keyboard:

- Standard keyboard functions pass through Secure KM and are shared between the two computers.
- Dedicated functions and special keys, such as audio, BSAT (Bloomberg Secure Access Technology), LCD, etc. are operative only on the relevant Bloomberg computer.



TROUBLESHOOTING

General

As product powers-up all channel-select LEDs are turned ON and then OFF. After that a specific, predefined LED combination is turned ON. Product is inoperable.

- The product did not pass self-test procedure. Try to power cycle product. If problem persists please contact your system administrator or our technical support.

No power, and none of the channel selected buttons is illuminating

- Check that the power supply or power cable is properly connected to the mains socket
- Check that DC plug is fully inserted into the switch DC jack
- Check that the device is powered by using optical mouse with visible red light
- If power is not available, change the power supply

Channel select LEDs are blinking with audible repeating clicking sounds

- This occurs after the configuration is set. Power-cycle the unit (disconnect and re-plug the power adapter)
- If the blinking and clicking still persist after power cycling the unit, it is possible that the device anti-tampering system was triggered. Change the unit and call Belkin technical support

Keyboard/Mouse

Mouse not working (both channels)

- Check that the mouse is not plugged into keyboard port

The computer does not detect my keyboard, or my keyboard does not work when I switch computers or reboot

- Check that the keyboard you are using is connected properly to the KM Switch
- Check that the USB cable between the KM Switch and the computer is completely connected
- Try connecting to a different USB port on the computer
- Make sure the keyboard works when directly plugged into the computer, i.e the HID USB driver is installed on the computer. Rebooting may be necessary when trying this
- Make sure you are not using a keyboard with an integrated USB hub or other USB-integrated devices
- If the computer is coming out of standby mode, allow up to one minute to regain mouse function
- Try a different keyboard

The CAPS, NUM, and Scroll Lock lights on my keyboard do not function when I connect to the Switch

- This is normal operation. The lock-state information is fully functional. Due to the security of the Switch and known exploitation of lock-state information for leakages, the LED status is not supported. Please refer to the operating system for verification of the lock-state information for CAPS, NUM, and Scroll Lock

Certain keyboard functions are not working

- Some non-standard keyboard functions are disabled by the switch to prevent security risks. Contact Belkin Tech Support for latest compatibility list

Mouse

Mouse cursor does not leave primary display to secondary display in multiple-head computer

- Driver was not installed on that computer or not installed properly. Reinstall driver

The computer does not detect my mouse, or my mouse does not work when I switch computers or reboot

- Check that the mouse you are using is connected properly and to the correct port on the Switch
- Check that the USB cable between the Switch and the computer is completely connected

- Try connecting to a different USB port on the computer
- Make sure the mouse works when directly plugged into the computer, i.e. the HID USB driver is installed on the computer. Rebooting may be necessary when trying this
- Make sure you are not using a wireless mouse or a mouse with an integrated USB hub or other USB-integrated devices. These are not supported by the switch due to security policy
- If the computer is coming out of standby mode, allow up to one minute to regain mouse function
- Try a different mouse
- For extending USB, use only active USB extenders (over CAT5 cable)

Note: If the Belkin Secure Switch does not work properly, or the configuration procedure is unclear or does not work, contact Belkin support at **1-800-282-2355**.

INFORMATION

Safety Statement

INFORMATION TO USER

- USE INDOORS AND IN DRY LOCATION ONLY.
- This product may only be plugged in to socket outlets that are easily accessible.

FCC Statement

DECLARATION OF CONFORMITY WITH FCC RULES FOR ELECTROMAGNETIC COMPATIBILITY

We, Belkin International, Inc., of 12045 E. Waterfront Drive, Playa Vista, CA 90094, declare under our sole responsibility that the product, F1DN102K-3, to which this declaration relates, complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Federal Communications Commission Notice

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the distance between the equipment and the receiver.
- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

IMPORTANT NOTE:

Industry Canada Statement

This device complies with ICES-003 of the Industry Canada Rules. Operation is subject to the following two conditions:

1. This device may not cause interference, and
2. This device must accept any interference, including interference that may cause undesired operation of the device.

Ce dispositif est conforme à la norme CNR- standards d'Industrie Canada applicable aux appareils radio exempts de licence. Son fonctionnement est sujet aux deux conditions suivantes: (1) le dispositif ne doit pas produire de brouillage préjudiciable, et (2) ce dispositif doit accepter tout brouillage reçu, y compris un brouillage susceptible de provoquer un fonctionnement indésirable.

IC Statement:

This digital apparatus complies with CAN ICES-3(B)/NMB-3 (B).

CE Declaration of Conformity

We, Belkin International, Inc., declare under our sole responsibility that the product F1DN102K-3, to which this declaration relates, are in conformity with EMC Directive 2014/30/EU, Low Voltage Directive 2014/35/EU & 2009/125/EC RoHS Directive 2011/65/EU (Recast).

We further declare that the product meets the essential requirement of the above Directives. The limits contained in these articles are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates uses and can radiate

radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

A copy of the European Union CE marking "Declaration of Conformity" may be obtained at the website: www.belkin.com/doc.



For information on product disposal please refer to www.belkin.com/environmental.



Australia Declaration of Conformity

We, Belkin International, Inc., declare under our sole responsibility that the product F1DN102K-3, to which this declaration relates, are in conformity with the requirements of AS/NZS regulations for Class B Information Technology Equipment (ITE).

This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

Warranty

Belkin International, Inc., Limited 3-Year Product Warranty

What this warranty covers.

Belkin International, Inc. ("Belkin") warrants to the original purchaser of this Belkin product that the product shall be free of defects in design, assembly, material, or workmanship.

What the period of coverage is.

Belkin warrants the Belkin product for three years.

What will we do to correct problems?

Product Warranty.

Belkin will repair or replace, at its option, any defective product free of charge (except for shipping charges for the product). Belkin reserves the right to discontinue any of its products without notice, and disclaims any limited warranty to repair or replace any such discontinued products. In the event that Belkin is unable to repair or replace the product (for example, because it has been discontinued), Belkin will offer either a refund or a credit toward the purchase of another product from Belkin.com in an amount equal to the purchase price of the product as evidenced on the original purchase receipt as discounted by its natural use.

What is not covered by this warranty?

All above warranties are null and void if the Belkin product is not provided to Belkin for inspection upon Belkin's request at the sole expense of the purchaser, or if Belkin determines that the Belkin product has been improperly installed, altered in any way, or tampered with. The Belkin Product Warranty does not protect against acts of God such as flood, lightning, earthquake, war, vandalism, theft, normal-use wear and tear, erosion, depletion, obsolescence, abuse, damage due to low voltage disturbances (i.e. brownouts or sags), non-authorized program, or system equipment modification or alteration.

How to get service.

To get service for your Belkin product you must take the following steps:

1. Contact Belkin International, Inc., at 12045 E. Waterfront Drive, Playa Vista, CA 90094, Attn: Customer Service, or call **(800)-282-2355**, within 15 days of the Occurrence.
Be prepared to provide the following information:
 - a. The part number of the Belkin product.
 - b. Where you purchased the product.
 - c. When you purchased the product.
 - d. Copy of original receipt.
2. Your Belkin Customer Service Representative will then instruct you on how to forward your receipt and Belkin product and how to proceed with your claim.

Belkin reserves the right to review the damaged Belkin product. All costs of shipping the Belkin product to Belkin for inspection shall be borne solely by the purchaser.

If Belkin determines, in its sole discretion, that it is impractical to ship the damaged equipment to Belkin, Belkin may designate, in its sole discretion, an equipment repair facility to inspect and estimate the cost to repair such equipment. The cost, if any, of shipping the equipment to and from such repair facility and of such estimate shall be borne solely by the purchaser. Damaged equipment must remain available for inspection until the claim is finalized. Whenever claims are settled, Belkin reserves the right to be subrogated under any existing insurance policies the purchaser may have.

How state law relates to the warranty.

THIS WARRANTY CONTAINS THE SOLE WARRANTY OF BELKIN. THERE ARE NO OTHER WARRANTIES, EXPRESSED OR, EXCEPT AS REQUIRED BY LAW, IMPLIED, INCLUDING THE IMPLIED WARRANTY OR CONDITION OF QUALITY, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, AND SUCH IMPLIED WARRANTIES, IF ANY, ARE LIMITED IN DURATION TO THE TERM OF THIS WARRANTY.

Some states do not allow limitations on how long an implied warranty lasts, so the above limitations may not apply to you.

IN NO EVENT SHALL BELKIN BE LIABLE FOR INCIDENTAL, SPECIAL, DIRECT, INDIRECT, CONSEQUENTIAL OR MULTIPLE DAMAGES SUCH AS, BUT NOT LIMITED TO, LOST BUSINESS OR PROFITS ARISING OUT OF THE SALE OR USE OF ANY BELKIN PRODUCT, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

This warranty gives you specific legal rights, and you may also have other rights, which may vary from state to state. Some states do not allow the exclusion or limitation of incidental, consequential, or other damages, so the above limitations may not apply to you.

GS 5/15/2013

Reporting Belkin Product Security Vulnerability

If you are aware of potential security vulnerability with any Belkin Government product, we encourage you to contact us immediately at the following email address: **gov_security@belkin.com** or our technical support line at: **1-800-282-2355**

After your communication is received, Belkin Government personnel will contact you to follow up. To ensure confidentiality, Belkin encourages you to use PGP encryption key for secure communications.

The **gov_security@belkin.com** email address is not intended to reach technical support on Belkin Government products or services.

belkinbusiness.com

© 2016 Belkin International, Inc. All rights reserved. All trade names are registered trademarks of respective manufacturers listed. Windows and Windows Vista are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Mac OS is a trademark of Apple Inc., registered in the U.S. and other countries.

