



User Manual

Models:

F1DN001R – 4 Buttons DCU for 2-4 ports

F1DN002R – 4 Buttons DCU for 2-4 ports with LCD

F1DN003R – 3 Buttons DCU for 2-16 ports with LCD

8820-00778 Rev. A00

Contents

Section 1 - Introduction	2	Option 5 – Load Configuration	23
Package Contents	2	Option 6 – Save Configuration.....	24
Section 2 - Overview	3	Option 7 – Language.....	25
Security Features	3	Option 8 – Reset to Factory Defaults.....	27
Operational Features.....	4	Section 4 - Operation	28
Equipment Requirements.....	5	Section 5 - Troubleshooting Guide.....	35
Safety Precautions	6	Section 6 - Information	38
Front Panel Features – F1DN001R.....	7	Section 7 - Warranty	39
Front Panel Features – F1DN002R.....	8		
Front Panel Features – F1DN003R.....	9		
Rear Panel Features - F1DN001R.....	10		
Rear Panel Features – F1DN002/3R	11		
Tamper Evident Label	12		
Active Anti-Tampering System	12		
Product Specifications	13		
Section 3 - Installation	14		
Before Installation	14		
Installation	15		
Typical system installation diagram with the Belkin Secure DCU	16		
Step 3 – Administrator Configuration (F1DN002/3R Only)	17		
Option 1 - System Information	18		
Option 2 – Customize Channels.....	18		
Option 3 – Channels Visibility	21		
Option 4 – Display backlight	22		

Introduction

Table of Contents	SECTIONS	1	2	3	4	5	6	7
-------------------	----------	---	---	---	---	---	---	---

Section 1 - Introduction

Thank you for purchasing this Belkin Secure Desktop Controller Unit product (DCU). The Belkin Secure DCU is a major enhancement to Belkin's Secure KVM products. This product provides an easy and intuitive user interface to control complex Secure KVM systems. This product enables textual browsing of the available networks / resources through a color display. This product significantly improves user's situational awareness and therefore enhances security and productivity for users that operate continuously in multiple domain, secure environments.

This User Manual provides all the details you'll need to install and operate your new DCU, in addition to troubleshooting guidance—in the unlikely event of a problem.

Package Contents

- Belkin Secure DCU
- RJ14, 6 ft, DCU Cable
- USB programming cable (F1DN002R and F1DN003R only)
- This User Manual

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: 1-800-419-5546

After your communication is received, Belkin Government personnel will contact you to follow up. To ensure confidentiality, Belkin encourages you to use our [PGP encryption key](#).

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

Important: This Switch is equipped with 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 (800) 282-2355.

Section 2 - Overview

Security Features

Belkin's Secure KVM Switch is the most advanced and secure commercially available KVM Switch available today. The Belkin Secure DCU is an accessory which is designed to improve the usability of Belkin's Secure KVMs and therefore must provide a similar set of advanced security features.

Below is a summary of some of the key security features incorporated into the Belkin Secure DCU.

Improved User Situational Awareness

The Belkin Secure DCU provides clear indications of selected channel through number as well as programmable text and color (for F1DN002R and F1DN003R models only).

Non-Reprogrammable Firmware

The Belkin Secure DCU features custom firmware that is not reprogrammable, preventing the ability to remotely attack the DCU control logic.

Active Always-On Anti-Tamper

The Belkin Secure DCU active enclosure anti-tamper system prevents the DCU electronic circuitry from being accessed and tampered with by permanently disabling the product once tampering is detected.

Holographic Tamper-Evident Label

A serially numbered holographic security tamper-evident label is placed on the Belkin Secure DCU enclosure surface to provide a visual indication if the product enclosure has been opened or compromised.

Secure Packaging

"Tear away" packaging ensures secure delivery of the product as it is routed to the end user.

Common Criteria EAL-4 Listing

The Belkin Secure KVM Switch and the Belkin Secure DCU are listed by the Common Criteria organization. Belkin's DCU is Common Criteria validated to EAL 4+ (Evaluation Assurance Level 4) to assure the highest level of protection.

Operational Features

The Belkin Secure DCU was designed to enhance the usability and ease of use of the Belkin secure KVM systems. Below is a summary of some key operational features incorporated into the Product.

Textual Display of network / resource name

The F1DN002/3R color LCD presents available network numbers along with administrator programmable network / resource name in clear text. Up to 16 channels may be displayed and controlled through the F1DN003R.

Custom network / resource color

The F1DN002/3R LCD enables network / resource name coloring customization by the system administrator to enable easy user recognition.

Clear textual DCU and KVM error messages

The F1DN002/3R is designed to provide clear error messages resulted from abnormal KVM or the DCU operation.

Easy configuration using microSD card

F1DN002/3R enables easy deployment of multiple systems using Save and Load functions and microSD storage card.

Clear indication of CAC status

The Belkin Secure DCU color LCD provides clear and intuitive indications of the CAC status.

Manual and automatic display backlight adjustment

The Belkin Secure DCU color LCD designed to operate in wide range of lighting conditions. High dimming ratio is available through manual brightness control or through ambient light sensor automatic control.

Multilanguage support

The F1DN002/3R models support network/resource name customization in English, German, French, Spanish, and Russian.

Administrator Lock / Unlock

Advanced DCU settings are locked to prevent access by unauthorized users. Administrator may access these settings through the use of special unlock microSD card.

Equipment Requirements

Cables

Belkin Secure DCU requires one RJ14 custom cable available from Belkin.

Cable supplied with the unit is 6ft long. You can use other cables with a maximum length of approximately 50ft.

DCU Cables:

- F1D9026-06 (CABLE, RJ14, 6P6C, 26AWG, UNSHIELDED, DCU CABLE, 6')
- F1D9026-50 (CABLE, RJ14, 6P6C, 26AWG, UNSHIELDED, DCU CABLE, 50')

Important: Do not connect to PoE, LAN switches or LAN ports or you may damage connected equipment or DCU.

Secure KVM

You can connect the DCU only to Belkin's Secure KVM units that support DCU. For the latest information on product support see the Belkin website <http://belkinbusiness.com/>

Note that F1DN0001R model is only intended for use with Belkin 2 or 4-port KM/KVM/Windowing KVM.

Administrator Setup Equipment

The F1DN0002/3R enables administrators to interface other standard equipment to support an easy setup of one or multiple systems. The following parts are included in Belkin's DCU Programming Kit that may be ordered from Belkin:

- Mini-USB plug to USB Type-A receptacle adapter cable
- microSD card with custom file format, sample configurations and DCU setup unlock function.

In addition to the above kit, the administrator may need a standard USB keyboard to enable manual text and color programming.

Safety Precautions

Please read the following safety precautions carefully before using the product:

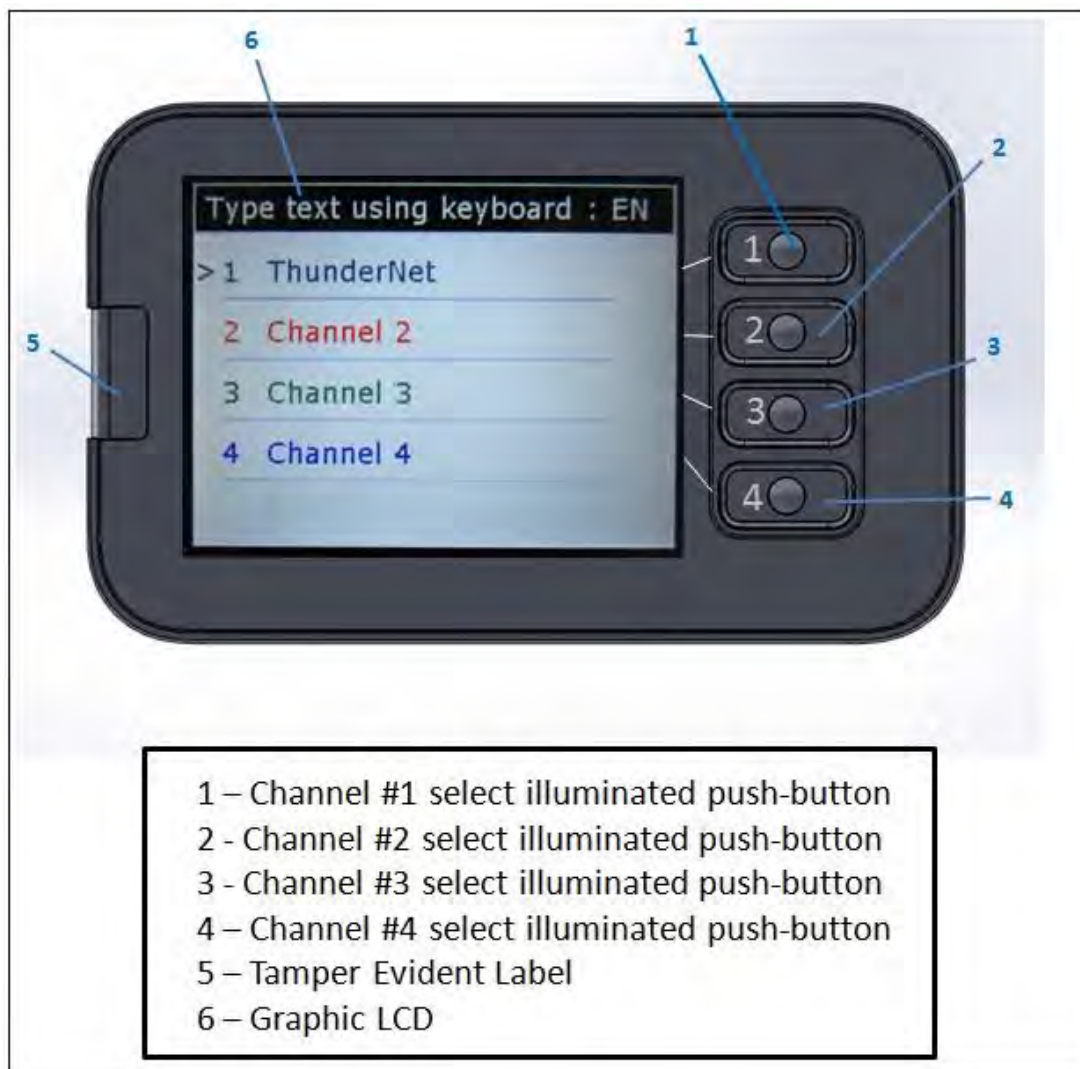
- Before cleaning, disconnect the product from the attached secure KVM unit.
- Be sure not to expose the product to excessive humidity.
- Do not store or use for extensive period of time in extreme thermal conditions - it may shorten product life time.
- Be sure to install the product on a clean secure surface.
- Do not place the DCU cable in a path of foot traffic.
- If the product is not used for a long period of time, remove the KVM's wall-mount power supply from the mains jack.
- If one of the following situations occurs, get the product checked by a qualified service technician:
 - Liquid penetrates the product's case.
 - The product is exposed to excessive moisture or water.
 - 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 has obvious signs of breakage or loose internal parts.
 - Power supply overheated, broken, 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.

- Product contains internal battery. Battery is non-replaceable. Never attempt to replace battery as any attempt to open product enclosure would permanently damage the product.

Front Panel Features – F1DN001R



Front Panel Features – F1DN002R



Overview

Table of Contents

SECTIONS

1

2

3

4

5

6

7

Front Panel Features – F1DN003R



- 1 – Graphic display
- 2 – Up illuminated push-button
- 3 – Select illuminated push-button
- 4 – Down illuminated push-button

Overview

Table of Contents

SECTIONS

1

2

3

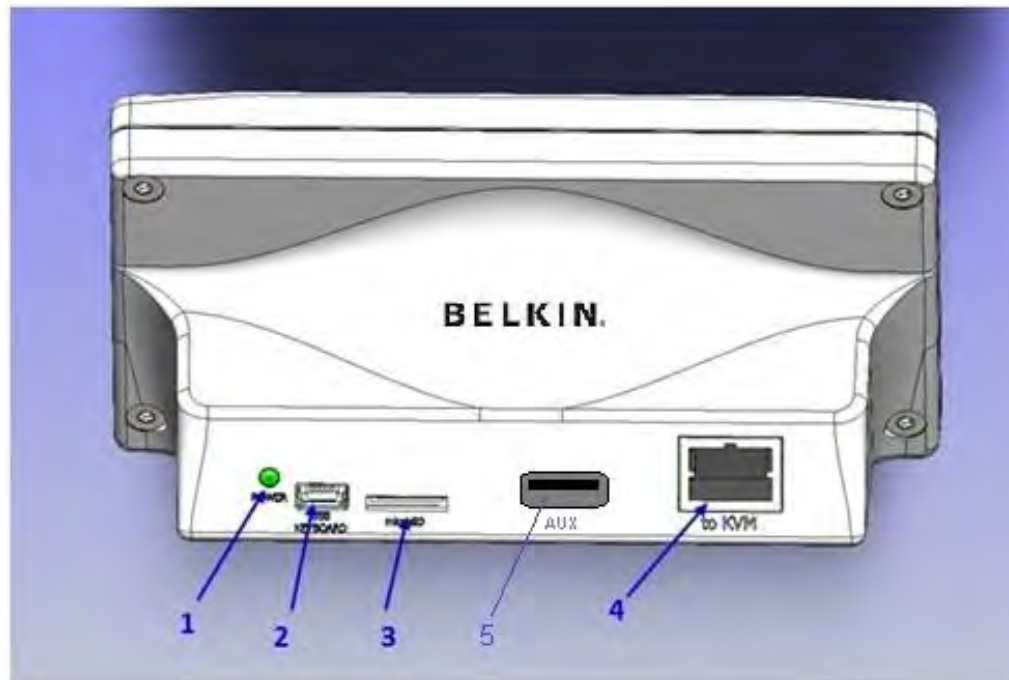
4

5

6

7

Rear Panel Features - F1DN001R



- 1 – Power LED (not assembled in 001R model)
- 2 - Mini-USB Programming Connector
- 3 – microSD card slot (not assembled in 001R model)
- 4 – DCU cable RJ-14 jack
- 5 – AUX port (not assembled in 001R model)

Overview

Table of Contents

SECTIONS

1

2

3

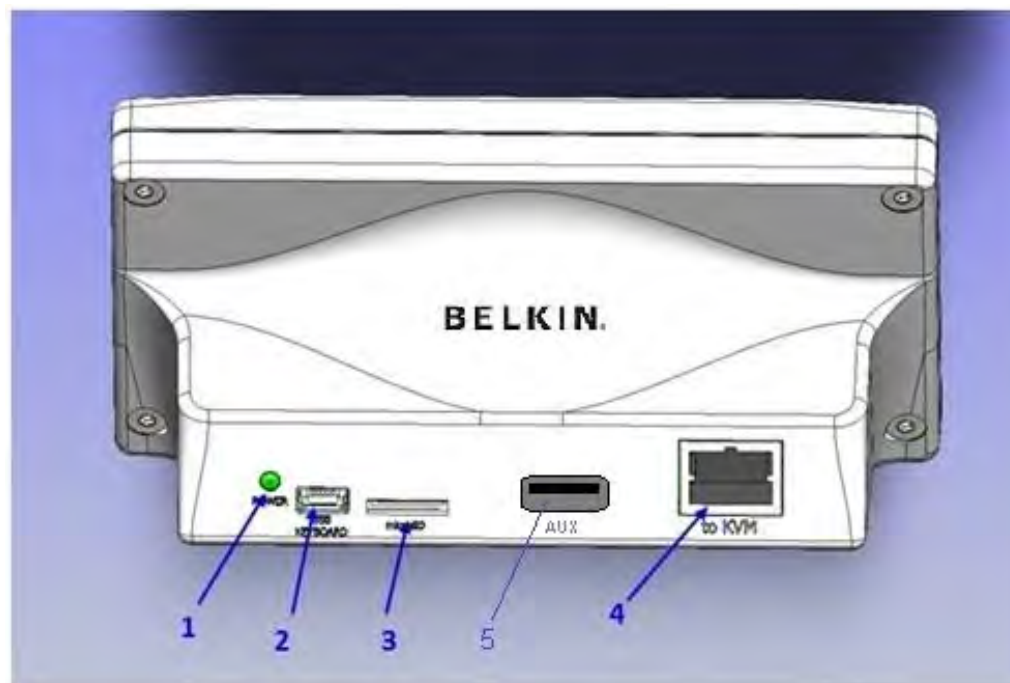
4

5

6

7

Rear Panel Features – F1DN002/3R



- 1 – Power LED (not assembled in 002R and 003R models)
- 2 - Mini-USB Programming Connector
- 3 – microSD card slot
- 4 – DCU cable RJ-14 jack
- 5 – AUX port

Overview

Table of Contents	SECTIONS	1	2	3	4	5	6	7
-------------------	----------	---	---	---	---	---	---	---

Tamper Evident Label

The Belkin Secure DCU uses a holographic tamper evident label to provide visual indications in case of an enclosure intrusion attempt. This label indicates white dots or the text “VOID” once removed. When opening product packaging inspect the tamper evident label.

IMPORTANT NOTICE:

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



Belkin Holographic Tampering Evident Label

Active Anti-Tampering System

The Belkin Secure DCU is equipped with an always-on active anti-tampering system. If mechanical intrusion is detected by this system, the DCU will display a message stating the product that has been tampered with.

If the product indicates a tampered state- please call Belkin Technical Support and avoid using the product

Product Specifications

Part No.	F1DN001R F1DN002R F1DN003R
Enclosure	Impact Resistance ABS Plastic
Power Requirements	5V DC, 1A (maximum) from connected Secure KVM unit
No. of Channels supported	16 maximum [4 maximum in F1DN001/2R model]
No. of Users Supported	1
Displays Size	3.5 inch diagonal [F1DN002/3R]
Display Resolution	240 (RGB) x 400 [F1DN002/3R]
Display Color Depth	65K [F1DN002/3R]
Display Technology	a-Si with white LEDs for backlight
KVM Interface	RJ-14 jack for Belkin Secure DCU bus. This interface uses special Belkin Secure DCU cable supplied with the product.
Other Interfaces	<ul style="list-style-type: none"> - Mini-USB Type A female connector for administrator keyboard connection (adapter cable must be ordered separately). - microSD card slot. - AUX control and monitoring port [available in F1DN002/3R only]

User interface

- Four illuminated channel select push-buttons [available in F1DN001/2R only]
- One toggle switch with up/down/select actions [F1DN003R model]

Sensors

Ambient light sensor

Languages Supported

English, French, Spanish, German, Russian

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

140 (W) x 90 (D) x 110 (H) mm / 5.51 (W) x 3.54 (D) x 4.34 (H) inches

Weight

0.25 Kg. (0.55 lbs.)

Security Accreditation

Common Criteria EAL 4+

Made in

U.S.A

Product design life-cycle

10 years per MIL-HDBK-217E

Section 3 - Installation

Before Installation

Unpacking the Product

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

After seal removal inspect packaging content to verify that required components included. See packaging content list in page 2 above.

After the Belkin Secure DCU removed from its packaging materials inspect the tampering-evident label to assure that product is properly sealed. If the label is damaged or missing contact Belkin support and do not use that product.

Where to locate the Belkin Secure DCU?

The Belkin Secure DCU is designed for desktop placement near the user's display. As access to the Secure KVM channel selection and continuous status monitoring is required from security standpoint, the Belkin Secure DCU must be located in the user's primary field of view while working with the display. Typical location is on the user's at the lower right side of the display (for right-handed users) or at the lower left (for left-handed users).

Product may be fixed to a rack or table using Velcro pads if necessary.

Avoid direct sunlight or strong light sources reflections on the Belkin Secure DCU display to prevent user's eyes fatigue.

Product must be located in a secure and well protected environment to prevent potential attacker access.

Consider the following when deciding where to place the Belkin Secure DCU:

- User access to the Belkin Secure DCU push-buttons is required.
- DCU to KVM cables length. Cables typically may be extended to a distance of 8 meters.
- The Belkin Secure DCU must be in the user's primary field of view.

Installation

Step 1 - Connecting the Belkin Secure DCU to the Belkin Secure KVM Switch

See figure in page 17 for typical system installation.

- Complete all Secure KVM installation steps as defined in the applicable product User Manual.
- Verify that the Secure KVM device is unpowered.
- Using supplied DCU cable DCU RJ-14 jack to the Secure KVM DCU jack.

Note: Connection must be direct – no switching or connections to other devices allowed.

Step 2 - Power up

- Power up user display.
- Power up the Secure KVM.
- Verify that KVM front panel LEDs indicating that channel #1 (default channel) is selected.
- Models F1DN002/3R Check that the Belkin Secure DCU display is illuminated and check that it is indicating that channel #1 is selected and no messages appeared.
- If using F1DN001R Check that the Belkin Secure DCU push buttons are illuminated and are indicating channel 1.

Note: Green LED at the back of the Belkin Secure DCU indicating that the product is properly powered. If LED is not illuminated refer to Section 5 below for troubleshooting guidance.

Note: When Belkin Secure DCU is connected to a Secure KVM, the Secure KVM front panel push-buttons become disabled.

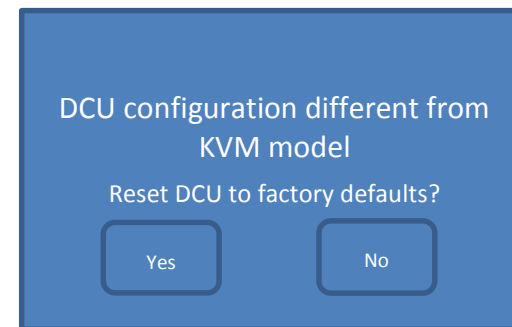
Note: If using the F1DN001R the installation is now complete. You can skip the rest of this section.

Note: If the Belkin Secure DCU is connected after Secure KVM power up or if DCU was momentarily disconnected and reconnected, then the Belkin Secure DCU will be inoperative (Secure KVM will continue to work without

and interaction with the connected Belkin Secure DCU). To use the Belkin Secure DCU again, restart KVM when the product is connected.

First Power Up after Belkin Secure DCU changed from another system (models F1DN002/3R)

- If Belkin Secure DCU was moved from a system having different configuration (for example different number of ports), the following error message will appear at first power up:

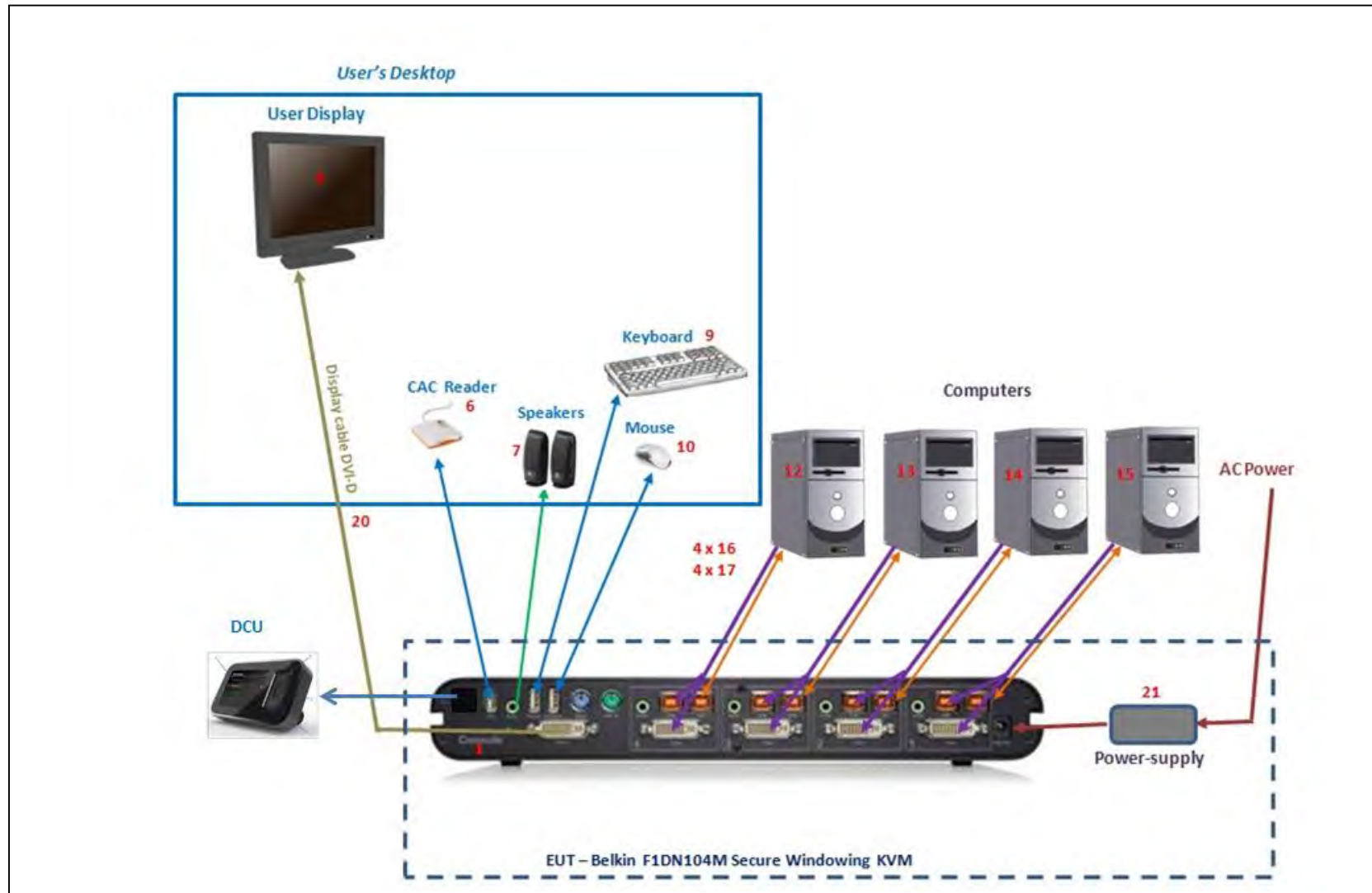


- Click on the Yes option to restore the Belkin Secure DCU to factory defaults. The product will restart with proper system configuration. All previous system settings will be deleted.

Installation

Table of Contents	SECTIONS	1	2	3	4	5	6	7
-------------------	----------	---	---	---	---	---	---	---

Typical system installation diagram with the Belkin Secure DCU



Step 3 – Administrator Configuration (F1DN002/3R Only)

How to enter setup mode:

F1DN002R:

- Press both 2 and 3 push buttons at the same time
- Use the 1 or 4 push buttons as up/down and select setup
- Press 2 or 3 to select

F1DN003R:

- Press double click central push button
- Use the up/down push buttons and select setup
- Press central push button to select

Notice: Users are not allowed to access the Setup menu and should not modify device settings.

By default, only the following Setup options are accessible to the user:

1. System Information
3. Channels visibility
4. Display backlight

Special microSD card with unlock function is needed to access all DCU Setup options (should be ordered separately).

Note: During Setup menu access the Secure KVM functions are disabled (no display, keyboard, mouse or audio output).

Note: When DCU is connected to a Secure KVM, the Secure KVM front panel push-buttons become disabled.

- Move the arrow to the Setup key using up/down buttons (for F1DB003R).



- Press center push buttons (F1DN003R) to enter the Belkin Secure DCU Setup menu. In the Belkin Secure DCU Setup menu – move arrow with the up\down arrow keys to the desired option and press the center key to select. To exit move arrow to Exit key at the bottom and select.

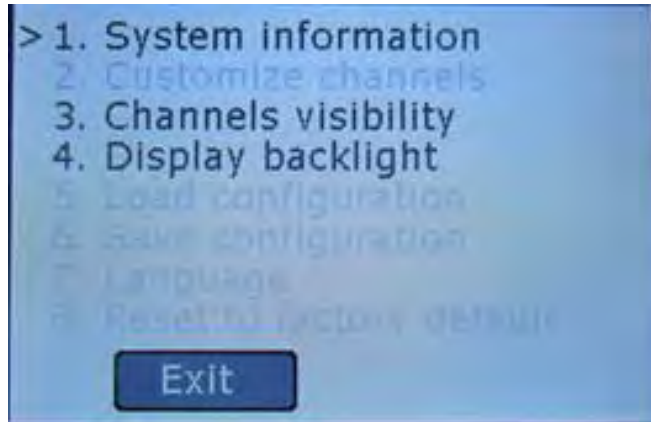
Note: If the Belkin Secure DCU is connected after Secure KVM power up or if the Belkin Secure DCU was momentarily disconnected and reconnected, then product will be inoperative (Secure KVM will continue to work without and interaction with the connected Belkin Secure DCU).

Installation

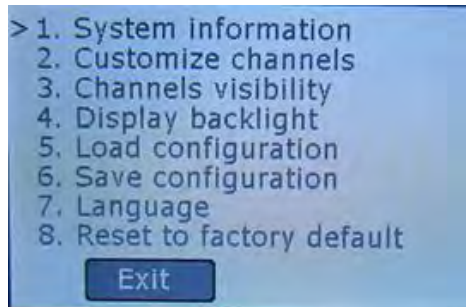
Table of Contents	SECTIONS	1	2	3	4	5	6	7
-------------------	----------	---	---	---	---	---	---	---

DCU Setup Lock / Unlock (F1DN002R/3R Only)

Note: if unlock microSD card is not inserted into the Belkin Secure DCU, only 3 Setup options are accessible. All other 5 options are grayed out and inaccessible.



- When the unlock microSD card is inserted into the microSD slot, the full Belkin Secure DCU Setup menu becomes accessible (all 8 options are in black color).



Note: Don't forget to remove the unlock card from the Belkin Secure DCU after setup is completed.

Option 1 - System Information

The System Information screen provides some basic information about the Belkin Secure DCU and about the connected Secure KVM. This information may be essential before contacting Belkin support.

Note: Some fields in the System information screen may be blank or zero if function not supported by the current system setup.

Option 2 – Customize Channels

You can enter customized text and fonts color for each one of the channels using Customize channel option (2). Note that text language may be changed using option 7 in the Setup menu as will be shown below.

Installation

Table of Contents

SECTIONS

1

2

3

4

5

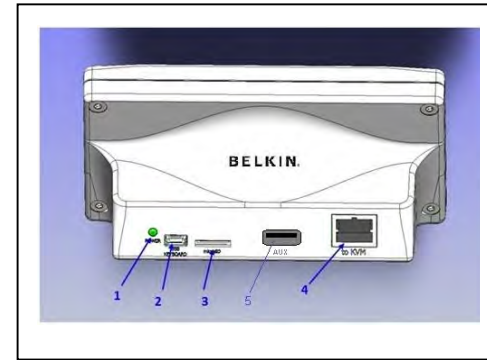
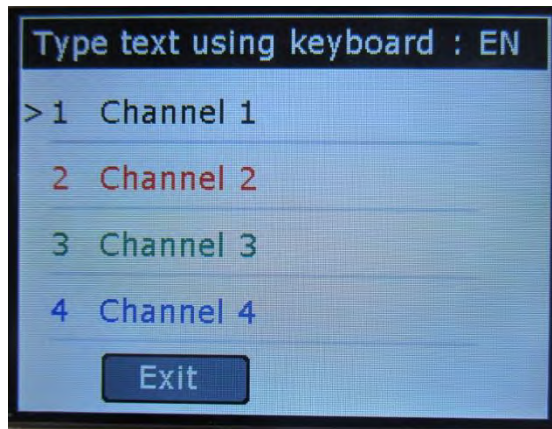
6

7

Important Note:

During channel customization or as long as the USB keyboard is connected to the Belkin Secure DCU, communication with the KVM is disabled and KVM will show similar behavior as a tampered product to prevent normal use. After customization is completed – recycle the power to the system to resume normal operation.

- After selection of Customize channels – the following display is shown. You can click on channel 1 to enter desired text or move the cursor to any other channel as needed.



Note: At any time that the USB keyboard is connected to the Belkin Secure DCU, KVM may not be used and KVM behavior is similar to tampered device. KVM Combiner will show fast automatic sequencing of channels.

- Selecting channel 1 will enable free text writing. Typing language appears at the top of the screen (English in this example).

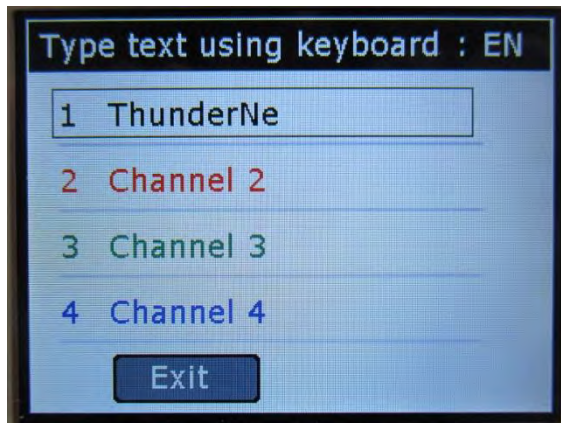
- Text may be entered manually using a standard USB keyboard that is connected to the Belkin Secure DCU Mini-USB Programming connector (2 in the below diagram) located at the unit's rear panel. Mini-USB to USB Type-A jack adapter can be ordered separately.

Installation

Table of Contents	SECTIONS	1	2	3	4	5	6	7
-------------------	----------	---	---	---	---	---	---	---



- You can use the right / left arrows to move and the delete key to delete typed text. Also you can use: Home, End, Insert, Shift and Caps lock as necessary.



- When text typing is completed press the keyboard "enter" key or the select key (for F1DN003R). The product will prompt to enter text color.



- Use up/down buttons or keyboard arrows to move up and down in the color palette. To select a color – press keyboard enter or select button (center key).

Installation

Table of Contents	SECTIONS	1	2	3	4	5	6	7
-------------------	----------	---	---	---	---	---	---	---

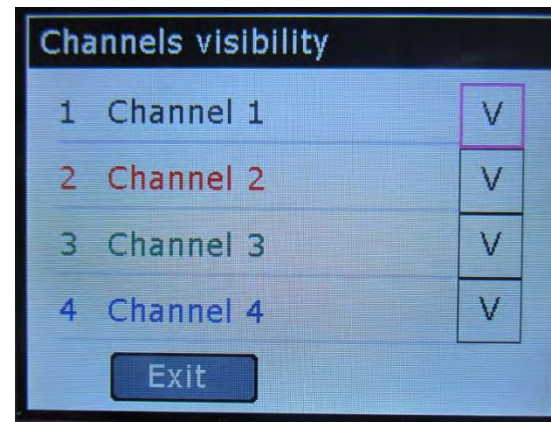
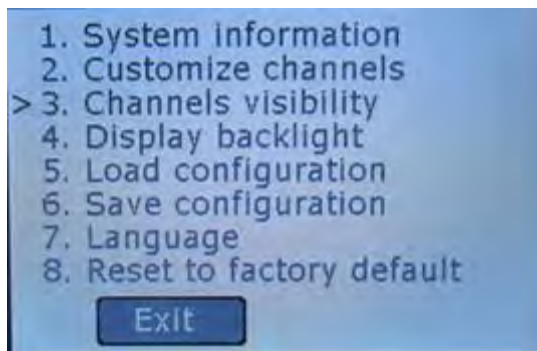
- You can then move to the next channel or exit this Setup option by pointing to the Exit key. Exit key will return back to Setup menu.

Note: After channel customization changes were applied recycle power to the KVM. Power must be recycled before resuming normal system operation.

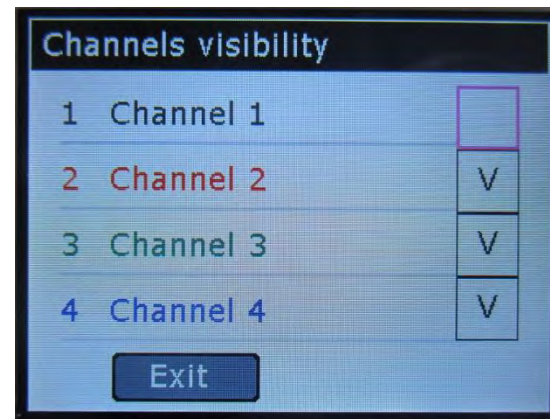
Option 3 – Channels Visibility

The channels visibility setup allows the user or administrator to Enable / Disable the Belkin Secure DCU access to specific channels. This function may be useful if only some channels are alive at specific point in time. Note that you may leave the KVM cables connected to disabled computers even if Belkin Secure DCU channel is disabled.

- From the setup menu navigate to the third menu option – Channels visibility.



- When channel is disabled – its line text will be gray in the Belkin Secure DCU Main menu screen. Still due to security considerations disabled lines are still accessible to the user.



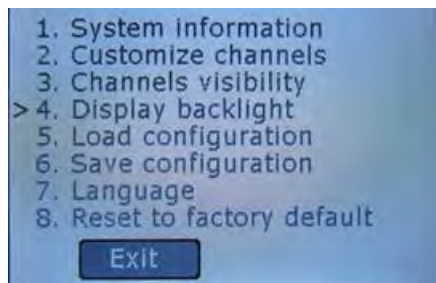
- Scroll to the specific channel and press the select button to disable or enable that channel.

Option 4 – Display backlight

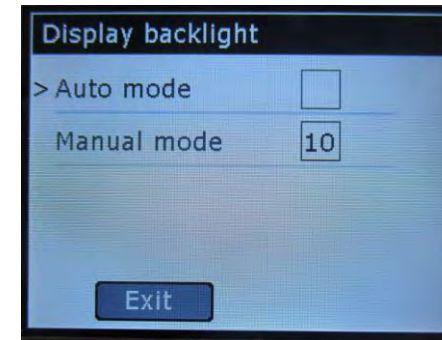
This Belkin Secure DCU setup options allows the user or the administrator to adjust the LCD backlight intensity.

Two modes of backlight intensity control are supported:

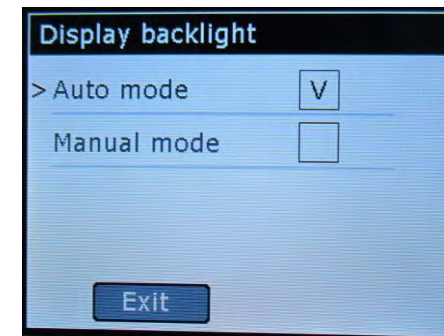
1. Auto mode – in this mode the backlight intensity is adjusted automatically by the system through ambient light sensing.
 2. Manual mode – in this mode the user manually selecting comfortable intensity by entering numbers from 1 (dim) to 10 (maximum brightness).
- To access this setup option – from the setup menu enter the fourth line – Display backlight.



- You can select Auto for ambient light sensor corrections or manual to enter brightness value manually.



- In manual mode – use the up/down buttons to increase or decrease the indicated value and the select button to select a value.



- For Auto mode – use the up/down buttons to check the Auto mode checkbox. Brightness will adjust based on ambient light sensor readings with 5 seconds average and delay to prevent flickering.

Option 5 – Load Configuration

The Belkin Secure DCU enables complete save and load of product configuration on a special microSD memory card (same card that used to unlock the Belkin Secure DCU). This function may save time when system administrator wants to deploy a small or large number of systems with similar settings.

Note: Only microSD card supplied by Belkin will work with Belkin Secure DCU. Special binary formatting required to properly operation in the Belkin Secure DCU.

Note: Belkin MicroSD card is not included with this product and has to be order separately.

Note: Do not use PC or devices other than Belkin Secure DCU to change the files stored on this microSD or files / card may become unusable!

Note: During configuration loading from microSD card the KVM may not be used. KVM behavior during configuration loading is similar to a tampered device. Windowing KVM will show fast automatic sequencing of channels.

Make sure that the microSD card is properly inserted at the Belkin Secure DCU

microSD card slot before attempting to load a configuration file.

- To access this setup option – select the fifth line from setup menu to enter the Load configuration menu.



- Once in the Load configuration screen, you can scroll up and down to select the proper configuration file from the list.

Note that configuration file must match the current system that the Belkin Secure DCU is connected to at the time of loading.

Configuration file format is DCU followed by *System Configuration* character and the 3 digits of sequential numbers.

System Configuration can be:

2 = 2-port KVM

4 = 4-port KVM

8 = 8-port KVM

F = 16-port KVM

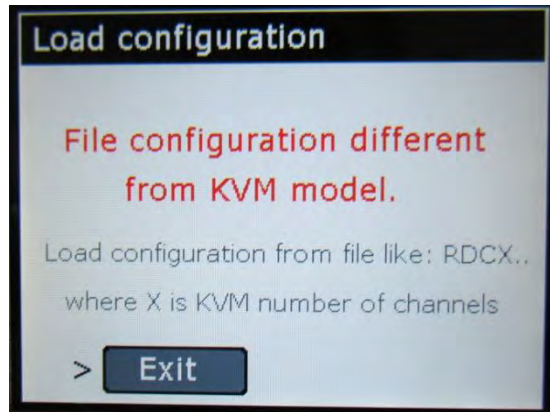
Before you load a configuration – verify that this character matches your current system configuration or loading process will fail.

microSD cards supplied by Belkin includes one sample configuration file for each of the above system configurations. You can use these files if you didn't save your configuration on the card before.

Installation

Table of Contents	SECTIONS	1	2	3	4	5	6	7
-------------------	----------	---	---	---	---	---	---	---

- Once file was loaded successfully – the message in the picture above will be shown.
- If loaded file is different from the current system configuration, the following error message will appear:



- In case that the loaded file is corrupted – the following message will appear: "File DCUXC000 is corrupt. Try to load another file."
- After configuration file was loaded – recycle the power to the system to resume normal operation.
- It is recommended that after configuration loading the administrator will test each channel and option in the configured Belkin Secure DCU to verify that configuration process completed according to the required setting.

Option 6 – Save Configuration

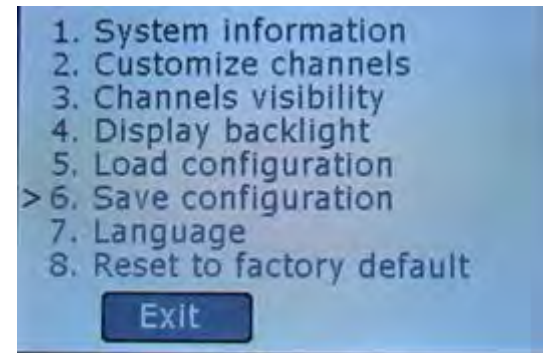
This setup option allows system administrator to save the current Belkin Secure DCU configuration on the microSD card.

Note: Only microSD card supplied by Belkin will work with Belkin Secure DCU. Special binary formatting required for proper operation with the product.

Note: Belkin MicroSD card is not included with this product and has to be order separately.

Note: Do not use PC or devices other than Belkin Secure DCU to change the files stored on this microSD or files / card may become unusable!

- Make sure that the microSD card is properly inserted at the Belkin Secure DCU microSD card slot before attempting to save a configuration.
- To access the Save configuration option – select the sixth line from the setup menu and enter the Save configuration menu.



Installation

Table of Contents	SECTIONS	1	2	3	4	5	6	7
-------------------	----------	---	---	---	---	---	---	---

- Press the select buttons to save the current configuration into the card.



- If file save process was successful – message will appear with the saved file name. File name is defined automatically by the Belkin Secure DCU based on the following rules:
 - DCU
 - Followed by System Configuration character (see above in Load Configuration).
 - Followed by 3 digits of sequential number (one more than last file saved on that card).

Note that saved configuration can be loaded only on systems with same configuration.

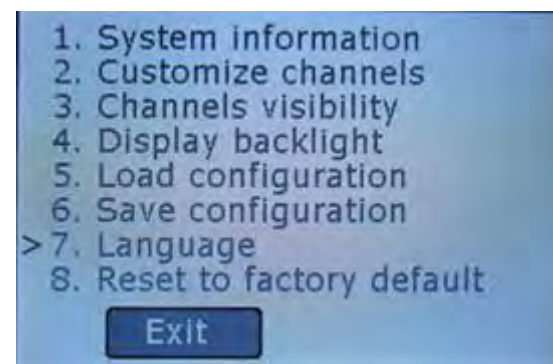
Note that the microSD card supplied by Belkin may store up to 1,000 different configuration files.

Option 7 – Language

This option allows system administrator to set the channel name text language.

Selected language will accept USB keyboard in that language and enables customized channel text to appear on the LCD.

- To access the Setup Language option – select the seventh line from the setup menu and enter the language selection menu.



Installation

Table of Contents	SECTIONS	1	2	3	4	5	6	7
-------------------	----------	---	---	---	---	---	---	---

- The language selection menu enables selection of: English (default), Spanish, French, German and Russian.



- Selected language appears at the top right corner of the screen when channel text is entered.

Spanish Keyboard Layout



French Keyboard Layout



German Keyboard Layout



Russian Keyboard Layout

Installation

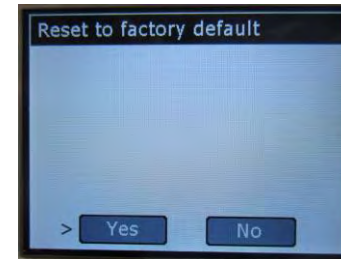
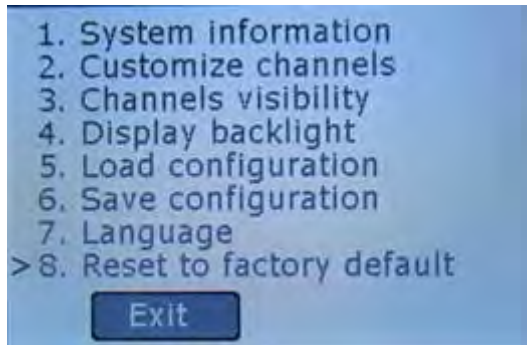
Table of Contents	SECTIONS	1	2	3	4	5	6	7
-------------------	----------	---	---	---	---	---	---	---

Option 8 – Reset to Factory Defaults

This function allows the system administrator to erase all Belkin Secure DCU configurations and reset the product back to production state.

This function may be used before moving the product from one environment to another or to troubleshoot installation and configuration issues.

- To access the Setup Reset to factory defaults option – select the eighth line from the Setup menu and enter the Reset to Factory Defaults menu.



- The Belkin Secure DCU will prompt for reset approval. If “Yes” option is selected, the product will reset and return back to factory settings.

Section 4 - Operation

When the Secure KVM and the Belkin Secure DCU are properly installed and configured, the system is ready for use. Default channel after power up is channel #1 (all KVMs except for Windowing KVMs) as indicated by channel select LED #1 illumination at the Secure KVM front panel and on the Belkin Secure DCU display.

In the following example we will use a four-port Secure KVM to demonstrate the Belkin Secure DCU operation.

Note: Operation of F1DN002R model is similar to F1DN003R described here but instead of the up/down and select push buttons use the 4 illuminated push-buttons to control the cursor location and state.

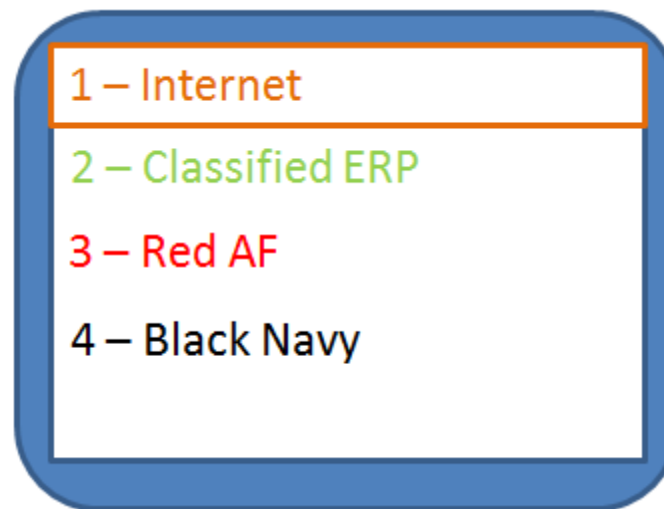
Operation of F1DN001/2R is simply done by pressing the illuminated buttons on the Belkin Secure DCU. The illuminated push buttons are actually an extension of front panel push buttons of the KVM and behave exactly the same.

Note: once connecting the Belkin Secure DCU to the switch the front panel push buttons of the KVM are disabled.

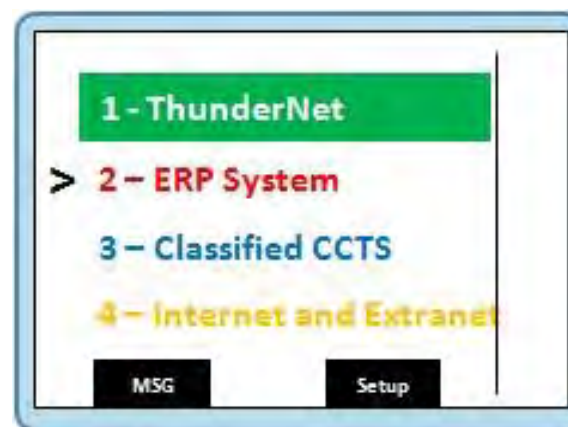
1. Channel selection on F1DN003R

You can select which computer you wish to control using the Belkin Secure DCU through the following actions:

- Default display after Belkin Secure DCU and KVM power up indicating channel #1. KVM channel selected is #1. Arrow is pointing to the default channel #1.



- The user uses up/down push buttons to move the arrow to channel #2. KVM is still switched to channel #1.



Operation

Table of Contents

SECTIONS

1

2

3

4

5

6

7

- The user presses the select button to select the channel where the arrow is (channel #2). Channel #2 selected as indicated by the red cursor.



- The user may use keyboard shortcuts to switch to another channel. In this example – if the user types Control-Control-4 the KVM switches to channel #4 as indicated in the Belkin Secure DCU display.

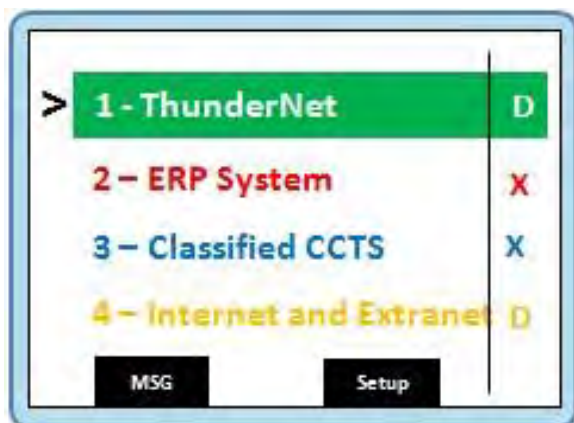


2. Normal operation with CAC

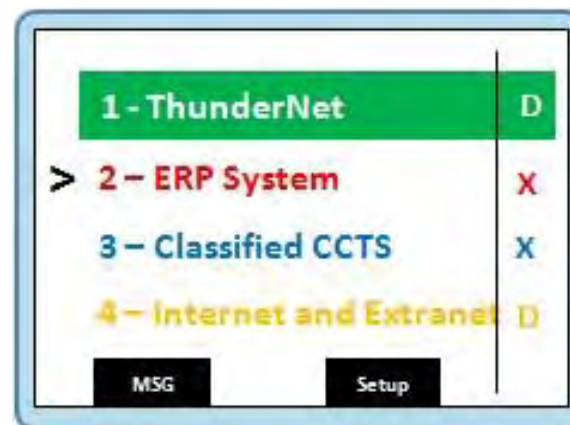
CAC status is presented at the right side of the display area (to the right of the vertical divider line). This area is empty if no device connected to the Secure KVM CAC Port.

In the following example we will use F1DN104G 4-Port Secure KVM with CAC enabled for computers #1 and #4 only.

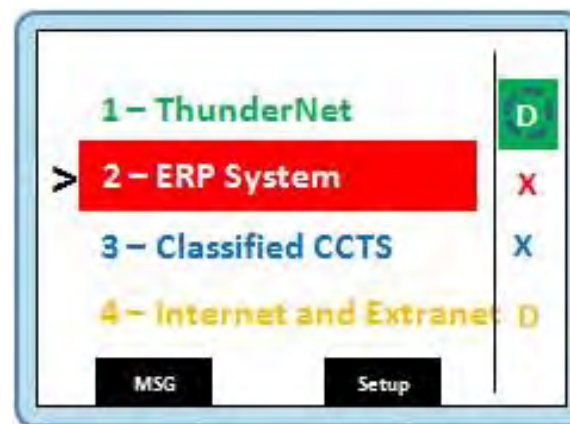
- Default display after Belkin Secure DCU and KVM power up. KVM channel selected is #1. CAC port channel selected is #1. Channels 2 and 3 have an unpowered / unconnected CAC interface as indicated by the X.



- The user uses the up/down buttons to move the arrow to channel #2.



- The user presses the “select” push button to select channel #2. Channel #2 is now selected as indicated by the red cursor. CAC port automatically enters freeze mode as indicated by blinking D in line #1.



Operation

Table of Contents

SECTIONS

1

2

3

4

5

6

7

- The user selects select channel #4. The arrow is now pointing to line #4 with CAC port on the same line.



3. Operation with 8/16 ports

This section covers the differences in Belkin Secure DCU operation when connected to Secure KVMs having 8 or 16 ports.

In general Belkin Secure DCU operation is similar to 4-ports operation demonstrated above with two exceptions:

1. List of channels in Belkin Secure DCU Main screen is longer than one screen.
2. Selected channel always shown. Either on top or bottom of the list.

The following example will use F1DN108F 8-ports secure KVM to highlight the operational differences.

- In Belkin Secure DCU Main screen you can scroll down to channel 8. Still selected channel (1 in this case) is fixed to the top of the list. Note that CAC port selected channel is 1 and the number 1 appears on top of the CAC column.



- If channel 8 is now selected, it will be marked and fixed to the bottom of the list.



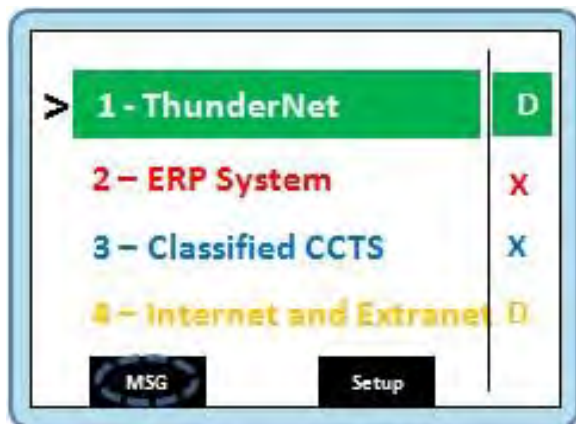
- Note that in this case, as channel 8 does not have CAC (X), CAC will automatically enter freeze mode and will remain on channel 1.

4. Abnormal Operation

This section provides additional information about Belkin Secure DCU abnormal operation.

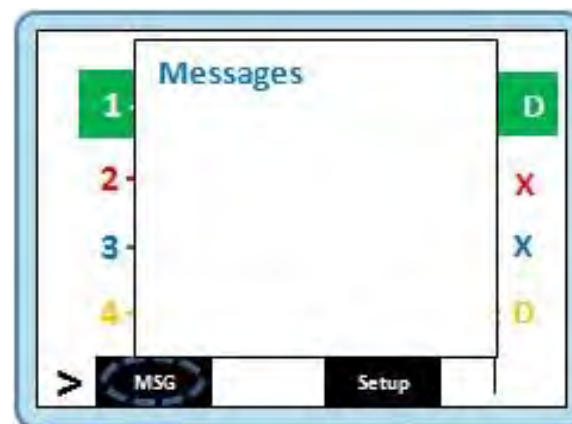
- If keyboard or mouse devices are not qualified, the MSG key will blink.

Note: Whenever there is a new message that was not yet accessed by the user before – the MSG key will blink.



- Once a message was accessed it will remain in the messages screen until the problem is fixed.
- If keyboard or mouse devices are not qualified, the MSG key will blink to indicate that there is a new message. Other KVM functions are still functional.
- To view all messages the user should double click the select key (F1DN003R) or push both 2 and 3 buttons (F1DN002R). navigate to the message box and press select.

- When problem is fixed (bad mouse device removed for example) message will disappear.



- Press select again to close message dialog.

Operation

Table of Contents

SECTIONS

1

2

3

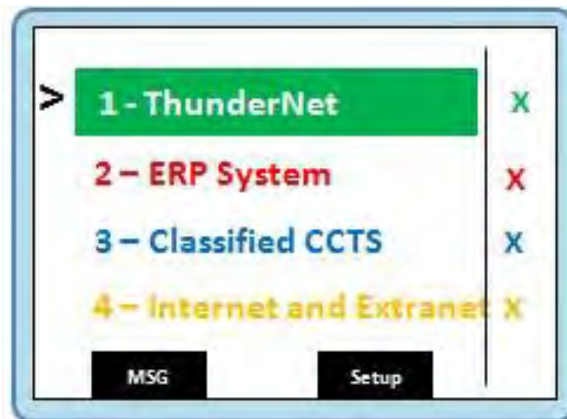
4

5

6

7

- If the device connected to CAC is qualified but all four channels are disabled as indicated by the four X in the CAC area.



- When device connected to CAC is not qualified, the MSG key will blink and the following icon will appear in the CAC area.



- To resolve problem – connect another (qualified) device.

- If the KVM anti-tampering system was triggered, the following message will appear in the Belkin Secure DCU display. Belkin Secure DCU can still be used with another Secure KVM.



- If the Belkin Secure DCU anti-tampering system was triggered, the following message will appear in the Belkin Secure DCU display. Belkin Secure DCU is permanently disabled (cannot be used). Secure KVM may still be used without the tampered Belkin Secure DCU.



Section 5 - Troubleshooting Guide

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

General

Problem: Belkin Secure DCU display backlight is not illuminated – Belkin Secure DCU is unpowered.

Solutions:

- Check that the Secure KVM is powered through front panel LEDs. Check the green power LED at the back of the DCU unit. If not illuminated – change cable and try again.
- Power down the system by disconnecting the Secure KVM DC power and reconnect after 10 seconds.
- Check that the Belkin Secure DCU cable connecting the product and the Secure KVM is securely connected and fully inserted at both sides.
- Check that cable is the supplied Belkin RJ14 custom cable – change cable for testing.
- Check that the Secure KVM used supports DCU (as indicated in the KVM User Manual).

Problem: The cursor does not follow the arrow once the push buttons are pressed.

Solutions: Commands from Belkin Secure DCU are not passed to the Secure KVM.

- Check the Belkin Secure DCU cable (see above).

- Power down the system by disconnecting the Secure KVM DC power and reconnect after 10 seconds.

Problem: The Belkin Secure DCU does not work – The following error message appears:

“DCU- KVM Communication Problem”

Solutions: Commands from Belkin Secure DCU are not passed to the Secure KVM.

- Check the Belkin Secure DCU cable (see above).
- Check that USB keyboard is not connected to the Belkin Secure DCU. If yes – disconnect it.
- Power down the system by disconnecting the Secure KVM DC power and reconnect after 10 seconds.

Troubleshooting

Table of Contents	SECTIONS	1	2	3	4	5	6	7
-------------------	----------	---	---	---	---	---	---	---

Problem: Belkin Secure DCU display is very dim.

Solutions:

- Go to Setup and change mode to manual. Adjust display brightness to maximum (10).
- Check Belkin Secure DCU cable length. Must be less than 8 meters. Change to a short cable for testing.

Problem: Belkin Secure DCU failed to save current configuration on inserted microSD card.

Solutions:

- Change microSD card device (use card supplied by Belkin as part of the Belkin Secure DCU Programming Kit).

Problem: Belkin Secure DCU failed to load (read) configuration file from connected microSD card.

Solutions:

- Change microSD card (use card supplied by Belkin as part of the DCU Programming Kit).

Video

Problem: No video image in user display (all channels/specific channel)

Solutions: Refer to the applicable Secure KVM troubleshooting guide in User Manual. Problem is not related to Belkin Secure DCU.

Keyboard

Problem: Keyboard rejected by KVM – see message below.



Solutions:

Problem is not related to Belkin Secure DCU.

- Change user keyboard device.
- Follow Secure KVM User Manual guidance.

Mouse

Problem: Mouse rejected by KVM – (see message below).



Solutions:

Problem is not related to Belkin Secure DCU.

- Change user mouse device.
- Follow Secure KVM User Manual guidance.

Problem: CAC is not working (one channel only). Indicated as X on Belkin Secure DCU display.

Solutions:

- Make sure that connected PC is powered and loaded the OS.
- Check that device is working properly when connected directly to the PC.
- Check that there is a CAC USB cable connected between that PC and the required CAC port in the switch.
- Follow Secure KVM User Manual guidance.

Section 6 - Information

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 products: F1DN001R ,F1DN002R ,F1DN003R to which this declaration relates:

Comply 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.

CE Declaration of Conformity

We, Belkin International, Inc., declare under our sole responsibility that the F1DN001R ,F1DN002R ,F1DN003R to which this declaration relates, are in conformity with Emissions Standard EN55022 and with Immunity Standard EN55024, LVP EN61000-3-2, and EN61000-3-3.

ICES

This Class B digital apparatus complies with Canadian ICES-003. Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

Section 7 - 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)-223-5546, 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: 1-800-419-5546

After your communication is received, Belkin Government personnel will contact you to follow up. To ensure confidentiality, Belkin encourages you to use our [PGP encryption key](#).

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

belkin.com

© 2013 Belkin International, Inc. All rights reserved.

All trade names are registered trademarks of respective manufacturers listed. Windows, Windows Vista, Microsoft, and IntelliMouse are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Mac OS and Mac are trademarks of Apple Inc., registered in the U.S. and other countries.