belkin Cybersecurity

Be Ready For Today™

Belkin NIAP PP4.0 Secure
SKVM and SKM

Administrator Manual

Belkin Secure KVM and KM products adhere to the NIAP PP4.0 standard, and leave the factory configured to the strictest guidelines.
An Administrator Configuration Terminal is available in our SKVM/SKM products for system administrators allowing system auditing and customizations to suit your installation or user needs. Available options include:

- Viewing of system logs for auditing purposes
- Creation of additional administrator users
- Customization of allowed hardware
- Customization of channel colors

This document will guide you through the options available as a system administrator and provide tips for securing your SKVM/SKM systems.

Please see our How-To Guide located at **www.belkin.com/cybersecurity/resources** for how to use your 8-Port SKVM as an 8-Port SKM.

This guide applies to the following SKVM and SKM models:

Universal 2nd Gen Secure KVM	Modular Secure KVM	Modular Secure KM
F1DN102KVM-UN-4	F1DN102MOD-BA-4	F1DN002MOD-BA-4
F1DN104KVM-UN-4	F1DN104MOD-BA-4	F1DN004MOD-BA-4
F1DN108KVM-UN-4	F1DN108MOD-BA-4	F1DN108MOD-BA-4*
F1DN116KVM-UN-4	F1DN202MOD-BA-4	
F1DN202KVM-UN-4	F1DN204MOD-BA-4	
F1DN204KVM-UN-4	F1DN208MOD-BA-4	
F1DN208KVM-UN-4	F1DN102MOD-DD-4	
F1DN102KVM-UN4C	F1DN102MOD-HH-4	
F1DN102KVM-UNN4	F1DN102MOD-PP-4	
F1DN104KVM-UNN4	F1DN104MOD-DD-4	
F1DN104KVM-UN4C	F1DN104MOD-HH-4	
F1DN104KVMUNN4Z	F1DN104MOD-PP-4	
F1DN108KVM-UNN4	F1DN202MOD-DD-4	
F1DN116KVM-UNN4	F1DN202MOD-HH-4	
F1DN202KVM-UNN4	F1DN202MOD-PP-4	
F1DN202KVM-UN4C	F1DN204MOD-DD-4	
F1DN204KVM-UNN4	F1DN204MOD-HH-4	
F1DN204KVM-UN4C	F1DN204MOD-PP-4	
F1DN204KVMUNN4Z		

Table of Contents

Rev. C00, June 2024

Security Guidance and Precautions for Deployment

Although Belkin Secure KVM and KM products are designed and tested to meet the strictest guidelines, some precautions should be taken before deploying a system into a production environment.

Anti-Tamper Protections

Belkin SKVM and SKMs feature anti-tamper security protections. Depending upon the model, you may have Active or Passive anti-tamper indicators.

Anti-Tamper Security Tape

Applicable to:
Belkin Secure 2nd Generation Universal KVMs
Belkin Secure Modular KVMs
Belkin Secure Modular KMs

An anti-tamper security tape is placed on the SKVM/SKM unit. When disturbed, this tape displays a visible tamper message. If this tape is not present or displays the tamper warning message, discontinue using this SKVM/SKM.

Active Anti-Tamper Detection

Anti-Tamper Security Tape

Applicable to:
Belkin Secure 2nd Generation Universal SKVMs

Active anti-tamper is a physical and logical tamper system that detects if the SKVM was physically disturbed or opened. When the active anti-tamper detection is triggered, the SKVM will exhibit the following behaviors:

- No image will be shown on any connected display.
- Keyboard, Mouse and CAC functionality will be disabled.
- The SKVM will cycle through all channels while making a “click” sound.

Upon power-up, your SKVM performs a system self-check. If this check detects tampering, the SKVM will not function and will enter this state immediately. If you have an SKVM in this state, you can perform a troubleshooting test by disconnecting power from the SKVM and removing any items connected to it. After 10 seconds, reconnect power. If the SKVM continues to display this behavior, it indicates that the anti-tamper has been triggered and the unit is no longer usable.

Self-Test Versus Active Anti-Tamper

Anti-Tamper Security Tape

All Belkin SKVM and SKM models perform a self-test during power-up. If this test fails, the SKVM/SKM will display a self-test failure, causing the SKVM/SKM to stop functioning and cycle through the channels. Unlike an anti-tamper event, self-test failures can generally be recovered from. Self-test failure behavior appears very similar to the anti-tamper behavior except for the following:

- The SKVM/SKM will remain silent while cycling through channels.
- SKVM units may display an image from the computer connected to channel 1 of the SKVM.

Administrator Password Requirements

Your Belkin PP4.0 Secure KVM/KM product enables authorized administrators to access the Administrator Terminal to view and download event logs, audit the product operation, and change advanced settings. Each Belkin Secure KVM/KM leaves the factory with a default password assigned to the main admin user account. The product can be used normally without changing this password, but it is recommended for security purposes to change it before deploying your SKVM/SKM into a production environment.

IMPORTANT: The main admin user account and password cannot be reset or deleted. If the password is mistyped or misplaced, it cannot be recovered. If you misplace the password, your SKVM/SKM will continue to function with the last setting changes made to it.

Properly Exiting out of the Administrator Configuration Terminal

When using the Administrator Configuration Terminal, your SKVM/SKM intercepts all keystrokes before relaying them to the computer. The terminal has an option labeled “Exit Terminal,” which will stop intercepting keystrokes but will not log out of the terminal completely. This is for testing changes. The next time you try to enter the terminal, you will not be prompted for a password. This is regardless of restarting the computer or closing your text application.

It is important that once you are done making all changes and ready to exit the terminal completely, you power cycle the SKVM/SKM by unplugging it from power for 10 seconds and then plugging it back in. You will be prompted for a password next time you attempt to enter the terminal.

Blocking USB Ports with the Belkin F1DNUSB-BLK

The USB ports on your SKVM/SKM are always active. Although the ports have security features to limit what devices can connect to them, they cannot be disabled completely through software. Belkin offers the TAA USB Port Blocker, F1DNUSB-BLK, a secure plug for the USB-A ports on your SKVM. Once inserted, this device will remain locked in place, disabling that port from being connected to.

The USB-B ports on the SKVM are one-way, allowing data to flow only from the SKVM to the computer when active. Belkin does not offer a USB-B port blocker.

Installation Guidelines

Proper Device Connection and Power On

Belkin SKVM and SKM units perform device acquisition functions during power-up. This requires certain devices be connected and powered on in a specific order to function correctly, otherwise improper behavior will be seen.

NOTE: The following steps start out with nothing connected to the SKVM, including a power supply. The SKVM should be powered off before starting. Failure to follow the steps exactly as written can lead to improper function of the SKVM.

Proper Power On Sequence: :

1. For SKVMs, connect all monitors being used to the SKVM. Power on these displays and set them to the correct input being used.
2. Connect the keyboard and mouse to their designated ports on the SKVM/SKM. If using Belkin SKVM or USB extenders, connect the keyboard and mice to the extenders, and then connect the extenders to the SKVM. If the extenders are powered, power on the extenders at this time.
3. Connect your computers to the SKVM/SKM.
4. Power on the SKVM/SKM.

The SKVM/SKM should power on and default to channel 1. All status LEDs for the connected displays, keyboards and mice should be solid green if they were detected and are connected correctly. You can now power on the computers and begin using them.

Rejected Device Connections

Your SKVM/SKM features security protections designed to detect and reject devices that do not comply with NIAP PP4.0 regulations. When connected, these devices will either function improperly or not at all. If a device is rejected, your SKVM will show a red LED next to the device's port.

Keyboards

Keyboards must have a standard, basic keyboard design with no extra functionality. Non-approved keyboards will have functionality issues, including missed keystrokes or no keystrokes registered at all. Items that will cause this include:

- Keyboards with multimedia controls
- Keyboards with built-in CAC card readers
- Keyboards with built-in USB hubs

IMPORTANT: Some keyboards can trigger a rejected state even if they are qualified devices. This is due to the hardware in the keyboard deviating from standard devices. For these situations, Belkin can provide an HID device filter that will allow the keyboard's basic functionality to work.

Mice and Trackballs

NIAP regulations specify that mice must have a standard, basic mouse design with no extra functionality. Your SKVM/SKM is designed to work with pointing devices of this type and contains a basic mouse driver. If your mouse requires a driver outside the basic mouse driver provided by Windows, it may not function with the SKVM.

Monitors and Displays

Upon power-up, your SKVM searches for and attempts connection with all connected displays. The LED light next to the console monitor connector will flash green during connection. If a monitor cannot be properly communicated with, the LED will turn off, and you will not have any display from this monitor. Common causes of this are:

- Cable runs that are too long (15 feet or longer)
- Poor-quality cables
- Unsupported cable adapters
- Improperly installed cables

For proper display functionality, Belkin recommends the following:

- For longer cable runs, use a video extender rather than a cable.
- Use quality brand cables instead of generic no-name cables.
- Limit the use of adapters if possible. Belkin makes SKVMs that support the most common display types, helping reduce the need for adapters.
- If adapters are required, use an adapter marked as an "Active" adapter. Also, ensure that the connection goes in the correct direction.
- Use a cable designed to meet the exact specifications supported by your SKVM.
- Many displays try to use HDCP connections. NIAP regulations require HDCP signaling to be blocked due to the 2-way communication. Disabling HDCP on your displays and computers' graphics software can improve compatibility.

CAC and other Authentication Devices

When connecting a non-qualified CAC reader to the CAC port on your SKVM, the LED next to the port will flash green and then turn off. Your CAC reader will not pass data through.

If your CAC port shows a red LED next to the CAC port, your authentication device is detected but rejected. You can allow this device through the Administrator Terminal.

USB Hubs and USB Storage Devices

NIAP regulations do not allow for the use of USB hubs and USB storage devices with your SKVM/SKM. These devices are blocked by default with your SKVM/SKM and cannot be allowed through. Connecting one of these devices will show a red rejected light on the USB port it is connected to.

Cont'd

Installation Guidelines

Troubleshooting Keyboard, Mouse and Control Peripherals

Belkin Secure KVMs and KMs allow users to utilize a single set of control devices and peripherals across multiple computer systems. Devices connecting to the SKVM/SKM are not communicating directly with each other; rather, they interface with the SKVM/SKM, which then handles the communication between them. The secure nature of the SKVM/SKM does require certain functionality blocked on keyboards, mice and other control devices. Blocked functionality includes:

- Keyboards with built-in USB hubs
- Keyboards with built-in CAC readers
- Keyboards with multimedia controls
- Mice with multi-function buttons
- Keyboards and mice requiring special drivers

Some keyboard and mouse functionality is disabled due to the functional nature it requires. Devices with two-way communication, such as USB hubs, are fully blocked by the SKVM/SKM due to NIAP regulation requirements not allowing this functionality. Other items are required to be blocked by default for security reasons but can be enabled through the Administrator Configuration Terminal.

IMPORTANT: Before allowing any device to connect to your SKVM/SKM, it is recommended to check with your IT and security groups to ensure it does not violate any security policies. Belkin SKVM/SKMs are built and shipped following strict NIAP guidelines, with functionality turned off by default from the factory.

Enabling Keyboard Multimedia Controls

By default, multimedia key controls are blocked through the SKVM. These controls include items such as volume controls, media playback keys, and shortcut keys. Keyboards featuring these keys may function only with standard typing functionality or may not function at all. However, this functionality can be restored through the Administrator Configuration Terminal. These controls can be activated by typing Left Control | Right Control | k or by following the steps below:

Step 1:
Connect a working keyboard to the Keyboard port on the SKVM/SKM and log into the Administrator Configuration Terminal.

Step 2:
Choose Menu 7 – Configure Peripheral Devices.

Step 3:
Choose option 2 – Toggle Consumer (Keyboard) Support.

Step 4:
Once toggled on, back out and exit the Administrator terminal. Power down the SKVM/SKM and connect the keyboard you would like to use with the multimedia keys to the keyboard port on the SKVM/SKM.

Your keyboard's multimedia keys should now be functioning. If they still do not, please see Troubleshooting Blocked Control Peripherals.

Keyboard Status Lights

Belkin Secure KVMs and KMs block all two-way communication between peripherals and computer systems. This block in communication causes the Scroll Lock, Caps Lock and Number Lock keys on a keyboard to fail to illuminate when pressed. This is a security feature and not a functionality failure.

Belkin has included these lights on the SKVM unit itself. When activated, a light will illuminate on the SKVM next to that functionality to show it was activated. If you are using the Belkin Remote Control with Integrated Keyboard (F1DN008KBD) with your SKVM, this functionality is enabled for this keyboard.

The Scroll Lock, Caps Lock and Number Lock functionality is a per-channel function, meaning these keys can be activated or disabled independently of each other. The SKVM tracks the status when switching between channels and will return to the last known state for a channel when activating it. This status is reset to the default state (OFF) when the SKVM is power cycled.

Configuring Mouse Movement Speed

Your Belkin SKM intercepts all mouse traffic and relays it to the computer. Since the mouse is shared among multiple computers, you can end up with differing movement speeds when going through the SKM. This is extremely noticeable on laptops when using in a laptop mode rather than connected to the SKM.

The SKM Configuration menu has an option to adjust the Mouse Movement Speed directly on the SKM. This is a global setting and applies to the SKM rather than an individual computer. This means any channel you are on will use this movement speed as will any computer you connect to this SKM.

Using the Belkin HID Filter F1DN-FLTR-HID-4

Belkin Secure KVMs and KMs will work with standard keyboards and mice. Not all these devices are built the same, though, and contain additional hardware, representing themselves as non-standard input devices. As a result, the SKVM will block all functionality of these devices. If you come across a keyboard or mouse that does not function correctly or at all with the SKVM, the Belkin TAA USB-A HID Fixed Filter, F1DN-FLTR-HID-4, may be of use. This adapter filters out the unwanted signaling of these devices, allowing their basic functionality to work.

IMPORTANT: Earlier versions of this device offered an additional security feature that, when connected, locks itself to the port it is connected to and cannot be removed. If you are utilizing this device for testing, it is recommended that you connect the adapter to a short USB extension cable rather than directly to your SKVM.

Cont'd

Installation Guidelines

Software, Firmware and Driver Downloads

Belkin Secure KVMs and KMs are designed to be plug-and-play devices. These products follow strict NIAP guidelines and, due to their secure nature, reduce the need for drivers, software, and firmware updates where possible. Software and drivers are only required in the following scenarios:

- A driver is required when a computer used with an SKM has more than one monitor connected to it.
- When using an SKM, a custom monitor layout is needed. Belkin provides a software tool to create a custom layout, which is only needed to be installed on one computer to configure all SKMs.

Belkin Secure SKVM and SKM products do not have firmware updates available. NIAP regulations block updates to these units in the field. Belkin does not provide firmware updates for download on our support site, nor is a service to update the firmware offered.

Enabling CAC Port Freeze (CAC Port Equipped SKVMs)

Belkin SKVMs with CAC ports have a functionality called CAC Freeze. CAC Freeze is turned off by default, which allows the CAC port to switch between computers when the active channel is changed. Enabling CAC Freeze will set a static channel that the CAC will freeze to even if the channel is changed.

Step 1:
With the SKVM power off, connect a device to the CAC port on the SKVM.

Step 2:
Connect a USB-A to USB-B cable between the computer and the USB-B port labeled CAC on the channel for that computer.

Step 3:
Power on the SKVM and computer. Set the SKVM's active channel to the computer you wish to freeze the CAC to.

Step 4:
Quickly press and release the channel button for this computer three times to activate CAC Freeze for this channel. The CAC light on the front of the SKVM next to the channel button will illuminate to show the CAC is active on that channel.

Step 5:
Switch to another channel to ensure that CAC Freeze is active. The CAC device should not switch to any other channel.

Repeat steps 3 and 4 to disable CAC Freeze on that channel.

Enabling Audio Freeze (Audio Port Equipped SKVMs)

Belkin SKVMs with audio ports have a functionality called Audio Freeze. Audio Freeze is turned off by default, which allows both analog and digital audio to switch between computers when the active channel is changed. Enabling Audio Freeze will set a static channel that the audio will freeze to even if the channel is changed.

Step 1:
Set the SKVM's active channel to the computer you wish to freeze the audio to.

Step 2:
Press the channel button for this computer for three seconds to activate Audio Freeze for this channel. The Audio light on the front of the SKVM next to the channel button will illuminate to show the Audio Freeze is active on that channel.

Repeat steps 1 and 2 to disable Audio Freeze on that channel.

NOTE: For security purposes, analog and digital audio are segregated in the SKVM. Belkin SKVMs with 3.5mm analog audio cannot convert the analog signal to come out over a digital HDMI or DisplayPort connection or convert a digital audio signal to analog. Whichever input type you choose for audio will be the output type for that audio.

Using the Administration Configuration Terminal

Belkin Secure SKVM and SKM products adhere to the NIAP PP4.0 standard and leave the factory configured to the strictest guidelines. An Administrator Configuration Terminal is available in our SKVM/SKM products for system administrators, allowing system auditing and customizations to suit your installation or user needs. Available options include:

- Viewing of system logs for auditing purposes
- Creation of additional administrator users
- Customization of allowed hardware
- Customization of channel colors

How to Log into the Administrator Terminal

IMPORTANT: When logging into the Administrator Terminal, you communicate directly with the SKVM/SKM, with the text output sent to the computer. To access the Administrator Terminal, a keyboard must be connected directly to the Keyboard input port on the SKVM/SKM. You cannot use a keyboard connected to the computer or built into a laptop.

It is not necessary for a display to be connected to your SKVM to access the Administrator Terminal. As long as a display is connected to the computer you are accessing through the SKVM, you will be able to access the terminal.

1. Connect a keyboard and mouse directly to your SKVM/SKM. Connect one USB cable from the SKVM/SKM host port to your computer. Power on both the SKVM/SKM and your computer.

2. Select the SKVM channel for the computer you want to use. The SKVM defaults to channel 1 upon power-up, but any port can be used.

NOTE: Any port can be used to change the SKVM/SKM, but some settings are per-port. These settings will be outlined later in this document.

3. Open a text editor application on your computer. We recommend Microsoft Notepad for Windows-based computers, but any text editor will work. This will be used for the terminal output from your SKVM/SKM.

4. Using the keyboard connected to the SKVM/SKM, press and release the following keys in this order: Left CTRL, Right CTRL, T. This will cause the SKVM/SKM to enter Terminal Mode. During this time, the SKVM/SKM will intercept your keyboard key presses and output text into the text application.

NOTE: While in Terminal Mode, your SKVM/SKM will intercept your keystrokes and consider them terminal commands. If you leave the text editor screen and enter into another application, you will have reduced functionality until you exit Terminal Mode. To quickly exit Terminal Mode, disconnect power from the SKVM for 10 seconds and then power it back on.

5. Once Terminal Mode is activated, a message asking for a username will appear in your text editor application. Enter the administrator username you wish to use to log in.

NOTE: Your SKVM/SKM has a main administrator account and allows up to eight additional user accounts to be created. The default username for the SKVM/SKM is admin1234. This username ID cannot be changed or deleted.

IMPORTANT: The terminal does not allow the use of the keyboard number pad. When typing numbers, you must only use the top row of numbers above the letter keys; otherwise, the keystrokes will be missed.

6. Next, you will be prompted to enter a password for this administrator. The password will be obfuscated for security purposes, so do not worry if the keys displayed do not match what you entered. All passwords are case-sensitive.

IMPORTANT: If this is your first time logging into the Administrator Terminal, you must use the default password of 1234ABCDefg!@# . Once entered, you will be prompted to create a new password for this administrator account. Your new password is required to follow these guidelines:

a. Must be between 8 and 24 characters long
b. Must have at least 1 capital letter
c. Must have at least 1 lowercase letter
d. Must have at least 1 number
e. Must have at least 1 special character (symbol)

When changing the default password, you will be prompted to enter it again to confirm it matches. If it does not match, you will receive an error.

NOTE: Administrator account passwords can be changed anytime in the Administrator Terminal.

Troubleshooting Administrator Terminal Login Issues

If you are having difficulty connecting to or logging into the Administrator Terminal of your SKVM, there are some simple items that you can check:

1. **You only receive the letter “T” when trying to bring up the terminal.**
   The default keystrokes to activate the Administrator Terminal Mode are the Left and Right CTRL keys. However, through an option in the Administrator Terminal, the ALT keys can be used instead. Try pressing Left ALT, Right ALT, T instead.

2. **You press the correct key combination, but nothing registers on the screen.**
   Ensure you are not holding the keys down. Instead, press and release them as if you are typing.

3. **My username or password is not registering or not being accepted.** Try typing slower. The SKVM intercepts your keystrokes, and items like usernames and passwords are commonly typed quickly. Typing too fast can cause the SKVM to miss keystrokes and lead to login errors.
   Ensure you are using only the number keys in the row directly above the letters on the keyboard. The terminal does not accept inputs from number pads.
   Usernames and passwords are case-sensitive. Ensure you are using the correct capitalization and that the Caps Lock key is not engaged.

Cont'd

Using the Administration Configuration Terminal

4. **I don't have Notepad on my computer.**
   When entering the Administrator Terminal Mode, the SKVM outputs standard ASCII text. Any text application can display the terminal output. Notepad is recommended as the most commonly available text editor on Windows, but you can use your favorite text editor if Notepad is not available.

5. **Terminal text is missing or slow to display in my text application.**
   Try changing your text application to another one that is available on your system. You can use any standard text application for Terminal Mode display.

Failed Login Attempts

You are allowed up to four attempts to log in to the Administrator Terminal. Upon the fourth failed attempt, the SKVM/SKM will enter an anti-tamper mode. The SKVM will begin cycling and flashing the channel buttons on the SKVM while making a clicking sound. An image will still be displayed, but no mouse or keyboard functionality will be available. This failed login attempt will be logged into the SKVM system event log.

To exit anti-tamper mode, disconnect power from the SKVM for 10 seconds, and then power back on. The SKVM will function normally, allowing you to try logging in again.

Administration Configuration Terminal Menu Options

Once logged into the terminal, a numerical menu will be presented with different options available for viewing logs or customizing the functionality of your SKVM/SKM. The options are accessed using the top row of number keys above the letter keys on the keyboard. The terminal will not recognize keys pressed on number pads. Pressing a number will immediately enter that menu and display any sub options in the terminal.

Menu 0 - Asset Management

The Asset Management menu allows you to make bookkeeping changes to the SKVM, such as adding custom asset tags or names for the SKVM/SKM. This is useful when tracking your SKVMs to ensure the data is stored digitally alongside any asset tags placed on the product casing.

Option 1: Use standard descriptor as asset container
This applies the asset tag currently registered to the system to the iSerial of the device emulator.

Option 2: Use custom descriptor as asset container
This sends the asset tag over the device custom descriptor.

Option 3: Enter new asset tag
This assigns the asset tag to the system controller chip. Only alphanumeric characters are accepted.

Option 4: Show current asset tag
This shows the current asset tag tied in the system controller.

Option 5: Apply asset tag to de
This sends the asset tag created in option 3 to the device emulator chips.

Option 8: Back
Takes you back one level on the menu.

Option 9: Exit Terminal Mode
This option will back your SKVM/SKM out of Terminal Mode, allowing you to use it as normal. However, it does not log you out of the administrator account you are currently logged into. To fully log out of the administrator account, disconnect power from the SKVM for 10 seconds to reboot it.

Menu 1 - Firmware Versions

The Firmware Versions menu allows you to view information about the firmware of the different system boards in your SKVM/SKM. This information is helpful when working with Belkin Support.

NOTE: Belkin Secure SKVM and SKM firmware is not field upgradeable. NIAP regulations restrict data loading into the SKVM/SKM anywhere other than the factory, and Belkin does not offer firmware updates for its SKVM/SKM products.

Option 1: DE Version
This displays the firmware version of the device emulators. The device emulators consist of the system boards connecting to peripherals such as displays, the keyboard and the mouse. These capture input commands from your peripherals and emulate an output to a connected computer or display.

Option 2: SC Version
This displays the firmware version of the SKVM system controller board. The system controller board handles all the SKVM switching and management functions.

Option 3: VC Version
This displays the firmware version of the SKVM video controller board, which handles all the EDID traffic.

Option 4: DPP Version
This displays the firmware version of the DPP (Dedicated Peripheral Port) of the SKVM. This is labeled as the CAC port on the SKVM chassis and is available on SKVM models supporting CAC card readers.

Option 8: Back
Takes you back one level on the menu.

Option 9: Exit Terminal Mode
This option will back your SKVM/SKM out of Terminal Mode, allowing you to use it as normal. However, it does not log you out of the administrator account you are currently logged into. To fully log out of the administrator account, disconnect power from the SKVM for 10 seconds to reboot it.

Menu 2 - Configure DPP (Dedicated Peripheral Port)

The Configure DPP (Dedicated Peripheral Port) option is available on Belkin SKVM units with a CAC card reader port. This option allows you to configure what devices are allowed through the CAC port on your SKVM. The SKVM is pre-programmed to allow CAC card reader devices only through this port. If you are having difficulties with using your CAC card reader through this port, this feature can help.

IMPORTANT: NIAP regulations prohibit specific devices from being used with a Secure SKVM. Your SKVM will block any devices, such as USB hubs, cameras, and data storage devices, from being used with it, even if you attempt to allow them to be used. The CAC port is a slow-speed USB 1.1 port intended only for security authentication devices. The status LED next to the CAC port will illuminate green for approved devices and red for blocked devices.

Cont'd

Using the Administration Configuration Terminal

Option 1: Allow currently connected device on all channels
This will add the USB device currently connected to the SKVM's DPP (CAC) port to the allowed devices list. This is useful when troubleshooting authentication devices. This option will not allow you to add NIAP-blocked devices such as cameras, USB hubs, and storage devices. Even if you allow the device, the SKVM will still block it. The LED light next to the CAC port will light green to show a device is connected and working or red to show a device is connected but not allowed.

This is an SKVM-wide change and will impact all channels of this SKVM.

Option 2: Block currently connected device on all channels
This will add the USB device currently connected to the SKVM's DPP (CAC) port to the blocked devices list. By default, the SKVM blocks all devices except CAC card readers. You can use this option to block a device you previously allowed but no longer want to be accessible through the CAC port.

This is an SKVM-wide change and will impact all channels of this SKVM.

Option 3: Show currently connected device
This will show the device ID data for the USB device currently connected to the CAC port. This data is helpful for device auditing and troubleshooting. Belkin Support may ask for it when troubleshooting.

Option 4: Show currently approved devices
This will display a list of all devices currently approved to be connected to and used with the SKVM CAC port. By default, CAC card readers are approved but are not shown on this list. This list will only show individual devices that an administrator has connected to the SKVM and allowed to work with the CAC port. The approved device does not need to be connected to the SKVM at the time of accessing this list.

Option 5: Show currently blocked devices
This will display a list of all devices currently blocked from being used with the SKVM CAC port. By default, CAC card readers are approved but are not shown on this list. This list will only show individual devices an administrator has blocked on this SKVM CAC port.

Option 6: Reset DPP settings
This will reset any customizations made to the DPP (CAC) Port Blocked and Approved lists. It will also set the CAC port functionality back to the factory default, requiring you to manually add any devices other than CAC card readers that you wish to work with the CAC port.

This is not a factory restore and only impacts the DPP Blocked and Approved lists. Performing a factory restore will also reset all DPP settings.

Option 7: Upload DPP settings from the host
This option is under development and not functional at this time.

Option 8: Back
Takes you back one level on the menu.

Option 9: Exit Terminal Mode
Choosing this will back your SKVM/SKM out of the Terminal Mode, allowing you to use your SKVM as normal. However, this does not log you out of the administrator account you are currently logged into. To fully log out of the administrator account, disconnect power from the SKVM for 10 seconds to reboot it.

Menu 3 - Using the Configure SC (System Controller)

The Configure SC Menu allows for bulk customization options for your SKVM/SKM. Here, you can customize SKM functionality, including mouse cursor speeds, changing the Admin Terminal activation keys, switching between computers using only the mouse cursor, and customizing the RGB coloring of the Belkin Universal SKVMs and Belkin Remote Control with Integrated Keyboard (F1DN008KBD).

Option 1: Enter desktop configuration [0-40] [default = 0]
This option is under development and not functional at this time.

Option 2: Enter mouse speed [0-32] [Default = 5]
Changes the speed at which your mouse cursor moves across the screen. The SKVM/SKM intercepts all mouse movements, emulating them to the computers. If your mouse movement needs to be faster, it should be changed here instead of in Windows. Changing it in Windows may cause mouse movement issues when using a laptop computer, or it may not register due to the laptop's built-in touchpad.

Option 3: Upload configuration from the host
This option is under development and not functional at this time.

Option 4: Use CTRL key as shortcut prefix
Use to set what key activates Terminal Mode. By default, the left and right CTRL keys are used when activating Terminal Mode. This option will allow you to return it to the CTRL keys if you change it to the ALT keys.

Option 5: Use ALT key as the shortcut prefix
Use to set what key activates Terminal Mode. By default, the left and right CTRL keys are used when activating Terminal Mode. This option will allow you to change it to the left and right ALT keys instead.

Option 6: Guard Mode configuration
Guard Mode is used on SKMs to turn channel switching on or off when the cursor reaches the designated edge of a display, also known as Seamless Cursor Switching (SCS). By default, Guard Mode is enabled on all SKM units shipping from the factory. When enabled, you cannot automatically change channels with the mouse cursor unless the left CTRL key is held down when moving from one system to another. This can also be activated on some SKVM models.

IMPORTANT: The system administrator can turn off guard mode on an SKM, allowing users to change channels without holding down the left CTRL key. Before this is done, we recommend checking with your IT or security teams to ensure this is acceptable at your location, as it may violate NIAP regulations.

Option 7: RGB FP Configuration
Used for customizing the RGB color designations on the front panel of Belkin 2nd Generation Universal SKVMs and what is displayed using the Belkin Remote Control with Integrated Keyboard. If your SKVM/SKM supports color profiles, a sub-menu with additional options will appear when this option is chosen.

Cont'd

Using the Administration Configuration Terminal

Sub Option 1: Upload configuration from a host
This option is under development and not functional at this time.

Sub Option 2: Configure colors

Sub Option 3: Configure dimming
This option is under development and not functional at this time.

Select Option 2. A dialog prompt will display, allowing you to change the colors of each channel:

1. Select a Channel [1 – *]
   Choose a channel for which you wish to change the color designation.
   The number of channels shown will depend upon your SKVM and how many computers can be connected to it simultaneously. Use the top row of number keys to select the channel for which you wish to change the color. It does not have to be the channel you are currently using to access the Administrator Terminal.
   Pressing the escape (ESC) key on the keyboard will allow you to exit this dialog and return to the previous menu.
   Select a color
   The SKVM/SKM has 10 colors to choose from for any channel connected to it. Channels can share the same color. All channels must have a color chosen, even if it is the default white. Select the color you wish to apply to this channel using the top row of number keys.
   r – red
   o – orange
   y – yellow
   w – white
   m – mint
   g – green
   c – cyan
   b – blue
   p – purple
   t – magenta
2. After choosing your color, press 8 to return to the menu or 9 to exit the Terminal Mode.

NOTE: Choosing 9 will not log you out of the administrator account you are currently logged into. To fully log out of the administrator account, disconnect power from the SKVM for 10 seconds to reboot it.

Sub Option 8: Back
Takes you back one level on the menu.

Sub Option 9: Exit Terminal Mode
Choosing this will back your SKVM/SKM out of the Terminal Mode, allowing you to use your SKVM as normal. However, this does not log you out of the administrator account you are currently logged into. To fully log out of the administrator account, disconnect power from the SKVM for 10 seconds to reboot it.

Option 8: Back
Takes you back one level on the menu.

Option 9: Exit Terminal Mode
Choosing this will back your SKVM/SKM out of the terminal mode, allowing you to use your SKVM as normal. However, this does not log you out of the administrator account you are currently logged into. To fully log out of the administrator account, disconnect power from the SKVM for 10 seconds to reboot it.

Menu 4 - Account Management

The Account Management option allows configuring the administrator accounts on your SKVM/SKM. You can create, edit, and delete child administrator accounts or change passwords for all administrator accounts. This menu will not allow for password recovery if the password is misplaced. If the password for an account is lost, the account must be deleted and recreated.

IMPORTANT: The default administrator account cannot be deleted. However, you can change the password using this menu.

Option 1: Change Password
This allows for changing the password of any administrator accounts on the SKVM/SKM. The current password for that account must be known to change a password. If you have lost the current password for this account, you will not be able to change or recover it.

Passwords adhere to the following criteria:
- Must be between 8 and 24 characters long
- Must have at least 1 capital letter
- Must have at least 1 lowercase letter
- Must have at least 1 number
- Must have at least 1 special character (symbol)

Option 2: Create admin account
Up to eight additional child administrator accounts can be created for each SKVM/SKM. The additional administrator user accounts are separate from the main administrator account. These accounts can be erased through the Administrator Terminal Account Management menu or a factory restore.

Option 3: Delete all accounts
This option will delete all additional child administrators. Once the additional accounts are erased, you can add them back or create entirely new ones.

IMPORTANT: The default administrator account cannot be deleted and will remain on this SKVM/SKM even if after using this option.

Option 8: Back
Takes you back one level on the menu.

Option 9: Exit Terminal Mode
Choosing this will back your SKVM/SKM out of the Terminal Mode, allowing you to use your SKVM as normal. However, this does not log you out of the administrator account you are currently logged into. To fully log out of the administrator account, disconnect power from the SKVM for 10 seconds to reboot it.

Menu 5 - Reset to Factory Defaults

The Reset to Factory Defaults option will erase all customizations of your SKVM/SKM and non-critical system logs. A factory reset will not reset the default administrator password or erase critical system logs that contain information such as failed login attempts and tamper events.

IMPORTANT: A factory restore will remove all child administrator accounts, but no changes will be made to the default administrator account. It is highly recommended that you do not perform a factory restore if you have lost the password to the default administrator account, as you will lose all access to the Administrator Terminal once the child administrator accounts are erased.

Menu 6 - Logs and Events

The Logs and Events Menu allows viewing of all system and critical logs stored on your SKVM/SKM. Up to 100 log events per log are stored timestamped, with the oldest being overwritten as new events are logged. These logs are helpful for auditing, to see how your SKVM/SKM is functioning, or to view access attempts and system changes.

Option 1: Show OTP Log
The OTP (one-time programming) log stores records of the SKVM/SKM system's critical events. The information contained in this log is not deleted during a factory restore. The following events can be found in this log:

- Self-test failures
- Tampering events
- Peripheral device rejections
- Peripheral device changes through the DPP (CAC) port
- Admin password changes
- Factory restores

Option 2: Show RAM Log
The RAM log stores non-critical system operation events. The information in this log is not deleted during a factory restore. The following events can be found in this log:

- SKVM power-up
- Peripheral device acceptance
- Configuration changes
- Admin logins
- Addition/removal of admin accounts
- Password changes
- Login failures

Option 3: Show non-critical RAM log
The non-critical RAM log stores a rolling list of actions taken on the SKVM.

Option 8: Back
Takes you back one level on the menu.

Option 9: Exit Terminal Mode
Choosing this will back your SKVM/SKM out of the terminal mode, allowing you to use your SKVM as normal. However, this does not log you out of the administrator account you are currently logged into. To fully log out of the administrator account, disconnect power from the SKVM for 10 seconds to reboot it.

Menu 7 - Configure Peripheral Devices

The Configure Peripheral Devices Menu allows you to change how peripheral control devices such as keyboards, mice, and touchscreens function on your SKVM/SKM and activate certain SKM functionality on SKVMs.

Option 1: Toggle Touch Support – Add/remove touch device interface from DE
This will turn on/off support for touchscreen interfaces through the mouse/keyboard port on your SKVM. By default, this is disabled from the factory.

Option 2: Toggle Consumer (keyboard) support – Add/remove consumer device interface from DE
By default, your SKVM is set to block all functionality that is not a standard keyboard key. This includes items such as hotkeys and multimedia controls. This option will turn support for these functionalities on/off.

NOTE: This can be used when troubleshooting keyboard functionality, but it will not support keyboards with extended functionality, such as card readers, USB hubs, or non-standard keyboard hardware. Certain keyboards may require using the Belkin HID Filter (F1DN-FLTR-HID-4). Information on this can be found on the Belkin Cybersecurity website.

Option 3: Add/remove an ABS mouse interface to/from DE
This will toggle the Absolute Mouse functionality for this port on or off. When using your computer, the USB mouse is typically in Relative Mouse Mode. Relative Mouse enables the computer to move the pointer to where the operator moves the mouse based upon the location the pointer was at before.

On the other hand, Absolute Mouse Mode (ABS) sends an X and Y coordinate that may be based upon a virtual canvas. This functionality allows the operator to seamlessly control multiple Windows OS multi-display computers as if they were one larger system.

Option 5: Video Follow Mouse
This allows the user to operate the SKVM without a remote control by moving the mouse off the screen to switch to the next channel. The channel sequence follows the same sequence as the front panel of the SKVM (i.e., on a 4-port Universal SKVM, channels 1 through 4 start from left to right of the front panel).

Option 8: Back
Takes you back one level on the menu.

Option 9: Exit Terminal Mode
Choosing this will back your SKVM/SKM out of the Terminal Mode, allowing you to use your SKVM as normal. However, this does not log you out of the administrator account you are currently logged into. To fully log out of the administrator account, disconnect power from the SKVM for 10 seconds to reboot it.

CAC (DPP) Port Configuration and Troubleshooting

Certain models of Belkin Secure KVM feature a Dedicated Peripheral Port, labeled CAC on the SKVM. This is a one-way, slow-speed, USB 1.1 port designed for USB authentication devices. The CAC port, by default, is switchable and shared among all the computers connected to your SKVM or can be locked to a specific port. Belkin SKVMs leave the factory pre-programmed to accept the most common CAC reader devices, but additional devices can be added through the Administration Configuration Terminal.

IMPORTANT: Allowing or blocking devices requires the device to be connected to the SKVM when allowing or blocking.

Adding Additional Devices

The CAC port allows additional devices to connect through it. This is done through the Administration Configuration Terminal. When you add a new device, it is placed on an allow list, which can be viewed at any time through the Administration Terminal. Devices will remain on this list until added to the block list, a reset of DPP settings is performed, or a factory restore is initiated.

NOTE: Allowing a device through the CAC (DPP) port is an SKVM-wide change and will impact all channels of this SKVM.

Step 1: Log into the Administration Configuration Terminal.

Step 2: Use the top row of number keys to access Menu 2 – Configure DPP.

Step 3: Use the top row of number keys to choose option 1 – Allow currently connected device on all channels.

Step 4: Once added, back out and exit the Administrator terminal. Power down the SKVM/SKM and reconnect power.

Blocking Devices From Connecting Through the CAC Port

Blocking devices from connecting through the SKVM's CAC port can be used to add devices you had allowed but no longer want to allow, or to block specific devices that may be accessible in the location the SKVM is at. These devices are added to a block list stored on the SKVM. Devices will remain on this list until added to the block list, a reset of DPP settings is performed or a factory restore is initiated.

NOTE: Blocking a device through the CAC (DPP) port is a SKVM-wide change and will impact all channels of this SKVM.

Step 1: Log into the Administration Configuration Terminal.

Step 2: Use the top row of number keys to access Menu 2 – Configure DPP.

Step 3: Use the top row of number keys to choose option 2 – Block currently connected device on all channels.

Step 4: Once added, back out and exit the Administrator terminal. Power down the SKVM/SKM and reconnect power.

Viewing Approved and Blocked CAC Port Devices

Your SKVM keeps a list of devices that are allowed or blocked from connecting to the SKVM. This can be useful when troubleshooting or for auditing purposes and is done through the Administration Configuration Terminal.

Step 1: Log into the Administration Configuration Terminal.

Step 2: Use the top row of number keys to access Menu 2 – Configure DPP.

Step 3: Use the top row of number keys to view a list:
- Press 4 to show the Approved Devices list
- Press 5 to show the Blocked Devices list

Reset the CAC (DPP) Port Settings

If you have made changes to the CAC (DPP) port settings and want to return them back to factory defaults, you have two options available:

Reset DPP Settings Menu

Step 1: Log into the Administration Configuration Terminal.

Step 2: Use the top row of number keys to access Menu 6 – Reset DPP Settings.
This will erase all devices listed on the Approved and Blocked lists for the CAC (DPP) port. It does not change any other settings on the SKVM.

Factory Restore Your SKVM

Factory restoring your SKVM will erase all customizations on the SKVM, including your CAC (DPP) Port Approved and Blocked lists.

Using RS232 Serial Controllers

Applicable To: Belkin 2nd Generation Universal Secure SKVM Models

Belkin PP4.0 Universal SKVMs feature an RS232 port on the Console section that allows connecting to serial control devices to remotely control channel switching on the SKVM. A USB to RJ11 cable is needed to connect your SKVM to your external control devices and custom commands used.

RS232 Serial Commands

RS232 RC Jack

NOTE: The image above shows F1DN204KVM-UN-4 for illustration purposes only.

USB to RJ11 Serial Cable Pinout

For convenience, Belkin manufactures an RJ11 to USB-A cable (F1DN-RC-USB-CBL) for use with the SKVM. (Please see your sales representative for additional cable details.) Custom cables can be made using the following pin-out chart.

RJ11 Connector	USB Connector	Wire Color	Functionality Comment
PIN 1	PIN 1	Red	+5V Power
PIN 2	N/A	White	TTL From Remote to SKVM
PIN 3	N/A	Blue	TTL From SKVM to Remote
PIN 4	PIN 5	Black	RS232 From Remote to SKVM
PIN 5	PIN 4	Green	RS232 From SKVM to Remote
PIN 6	PIN 6	Exposed	Ground / Power Drain (Shield)

RS232 Serial Commands

Below are the communication settings as well as the channel-switching commands you can program into your control device.

Serial Communication Settings:
- Speed (baud): 115200
- Parity: None
- Flow Control: None

What are Keep-Alive Events?

Keep-Alive events are what the device uses to periodically communicate the status of its current configuration to the remote controller using the RS232 protocol.

All commands must be sent with a carriage return ending character and an implicit linefeed. For example, a Crestron controller may use \x0D. (Please refer to your controller's user manual for specific carriage return/linefeed instructions.)

Channel Control Commands:
To change the channels, you can program your controller or use a TTY terminal on your computer. If using a TTY program, type the command #AFP_ALIVE followed by the command for the channel you want to change to.

Example:
- **#AFP_ALIVE FD** will switch to channel 2.

Channel	Command	Channel	Command
1	FE	9	FF
2	FD	10	FDFF
3	FB	11	FBFF
4	F7	12	F7FF
5	EF	13	EFFF
6	DF	14	DFFF
7	BF	15	BFFF
8	7F	16	7FFF

For further information, please visit our Resources page and download our guide on using an RS232 serial connection to control your SKVM remotely.

SKVM and SKM Customizations

Configuring Channel Colors

Applicable to All PP4.0 SKVMs and SKMs

Belkin Secure SKVMs and SKMs can set a per-channel color for easier network identification. Both our 2nd Generation Universal SKVM models and Modular SKVM/SKM models support color configuration for the Belkin Remote Control with Integrated Keyboard (F1DN008KBD), and the 2nd Generation Universal SKVMs also support channel coloring via the front panel RGB lights.

NOTE: The Belkin Modular SKVM/SKM models can support colors on the Belkin Remote Control with Integrated Keyboard (F1DN008KBD) but do not feature RGB channel buttons. These models will only show white buttons on the SKVM/SKM themselves.

Configuring RGB Channel Color Designations

Step 1: Log into the Administration Configuration Terminal.

Step 2: Choose Menu 3 – Configure SC.

Step 3: Choose option 7 – RGB FP Configuration.

Step 4: Choose option 2 – Select Colors for Channels.

Step 5: A prompt will appear asking which channel you wish to change the color for. Press a number to choose a channel (left to right on SKVM/SKM).

Step 6: The SKVM/SKM has 10 colors to choose from for any channel on it. Channels can share the same color, but all channels must have a color chosen, even if it is the default white. Select the color you wish to apply to this channel using the top row of number keys.

r – red
o – orange
y – yellow
w – white
m – mint
g – green
c – cyan
b – blue
p – purple
t – magenta

Step 7: Repeat steps 5 and 6 for each channel you wish to set a color to.

Step 8: When finished, use the top row of number keys to choose option 9 to exit out of Terminal Mode.

Adding Channel Labels

Included with your SKVM is a set of labels that you can use to label each channel. The most common network labels are included along with a set of blank labels. Below each channel button is a convenient, designated area for you to place the label.

Modular SKVM/SKM Channel Labels (Black & Color Options)

Adding Asset Tags

All Belkin SKVMs and SKMs can store digital asset tags in the SKVM and add a physical sticker. This adds an additional layer of security and bookkeeping accountability. A convenient area has been marked on the casing of the SKVM/SKM for placing a physical asset tag.

Digital asset tags can be added through the Administrator Configuration Terminal.

Step 1: Log into the Administration Configuration Terminal.

Step 2: Choose Menu 0 – Asset Management.

Sub Option 1: Use standard descriptor as asset container

This applies the asset tag currently registered to the system to the iSerial of the device emulator.

Sub Option 2: Use custom descriptor as asset container
This sends the asset tag over the device custom descriptor

Sub Option 3: Enter new asset tag
This assigns an asset tag to the system controller chip. Only alphanumeric characters are accepted.

Sub Option 4: Show current asset tag
This shows the current asset tag associated with the system controller.

Sub Option 5: Apply asset tag to de
This sends the asset tag created in Option 3 to the Device Emulator chips.

Sub Option 8: Back
Takes you back one level on the menu.

Sub Option 9: Exit Terminal Mode

Enabling SKM Functionality in Belkin SKVMs

Belkin SKVMs are designed to share a keyboard, mouse, and one or two monitors between a set of connected computers. Belkin SKMs share only the keyboard and mouse, with each computer having access to its own displays. Belkin SKMs feature additional functionality that is disabled on Belkin SKVMs, but it is possible to enable this functionality using the Administrator Configuration Terminal.

How to Enable SKM Functionality for Your SKVM

Enabling SKM functionality will allow you to use Belkin SKVMs as SKMs for configurations we do not make SKMs in (such as 8-port SKMs) or to add items such as Seamless Cursor Switching (SCS) to a SKVM.

IMPORTANT: The steps below make configuration changes to settings on the system controller board of the SKVM. After making changes on one computer, you will need to log out of the terminal, switch to the next computer and follow the steps again for that computer.

Step 1: Log into the Administration Configuration Terminal.

Step 2: The mouse mode needs to be changed to Absolute. This is done by pressing and releasing the following keys in order: Left CTRL, Right CTRL, c.

Step 3: Use the top row of number keys to exit Terminal Mode by pressing 8 and power cycle the SKVM.

NOTE: If you see a letter C in the terminal, repeat step 2 but ensure you are pressing and releasing rather than holding the keys. If it continues, your SKVM may not support SKM functionality. While in Terminal Mode, use Menu 1 to document the firmware versions of your SKVM, and reach out to Belkin Support for further assistance.

How to Disable SKM Functionality on an SKVM

If you have enabled SKM functionality on your SKVM and now want to disable it, returning your SKVM into SKVM mode, a factory restore will need to be done. After this, your SKVM will function as a normal SKVM, and any customizations will need to be configured again.

Configuring a Display Layout for Your SKVM With SKM Functionality Enabled

With your SKM functionality enabled on your SKVM, we need to configure it with the layout of your monitors. This ensures your SKVM knows how many monitors are connected to each computer and in what orientation to switch channels when using Seamless Cursor Switching (SCS). It is essential for your SKVM configuration to match the layout of your monitors; otherwise, you will experience unwanted functionality of the mouse cursor.

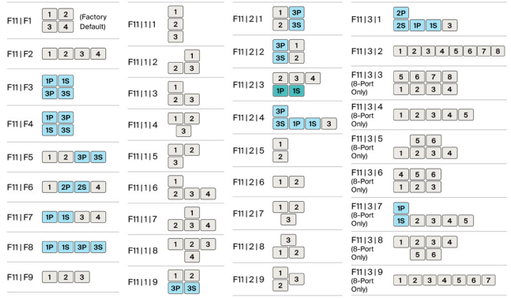
IMPORTANT: A single computer can connect to a maximum of four displays. The SKVM will not support more than four for any given computer.

Using a Pre-Defined Configuration

Your Belkin SKVM contains a list of pre-defined display layouts that match the most popular layouts. These configurations can be set in the SKVM by a key combination. To do so, press and release the following keys in order: Left CTRL, Left CTRL, F11, followed by two numbers that match that layout.

EXAMPLE: For example, for our 8-Port SKVMs, to select an 8-display configuration (one display per connected computer) in a row, you would want configuration 3,2. To enable this, you would press the keys as follows:
Left CTRL, Left CTRL, F11, 3, 2

After you choose your display layout, the SKVM needs to be power cycled. Disconnect the power from the SKVM and wait 10 seconds before reconnecting it. Once the SKVM boots up (10 seconds), it will be in the display configuration you chose. You can test out your new layout by moving the mouse.



Using a Custom Configuration

Although Belkin has programmed the most common display layouts into your SKVM, there are occasions when your layout will deviate from the pre-defined list and require a custom configuration.

Belkin has created a downloadable SKM Custom Configuration utility on our website. This utility allows you to create a display layout that matches your installation and provides a file that can be loaded into your SKVM through the Administration Configuration Terminal. For more information, please visit the Belkin website for this utility and the supporting documentation.

Enable and Disable Guard Mode on an SKVM With SKM Functionality Enabled

Belkin SKMs feature a mode called Guard Mode. Guard Mode is used for switching between connected computers by simply moving the mouse. When enabled, users are required to hold the Left CTRL key when moving between channels. Disabling Guard Mode removes this restriction, allowing users to switch by simply moving the mouse.

Step 1: Log into the Administration Configuration Terminal.

Step 2: Enable or disable Guard Mode by pressing and releasing the following key combinations:

- To enable: Left CTRL, Left CTRL, F11, C
- To disable: Left CTRL, Left CTRL, F11, B

Advanced SKM Configuration Options

Applicable to: Belkin Modular Secure KMs

Using Multiple Displays on a Single Computer

Belkin Secure KM products differ from SKVMs in that each connected computer can have its own dedicated display rather than sharing one or two between them. Belkin SKMs support up to four displays per connected computer.

When connecting more than one display to a computer, you will need to install the Multi-Display Driver found on the Belkin support site for your SKM. Without installing this, your computer will display on all monitors connected to it, but your mouse cursor will not move past the primary display of that computer.

Visit the Belkin Support site for your SKM and look for the Multi-Display Driver download page.

NOTE: This driver is only required for Windows computers.

Enable or Disable Guard Mode (Seamless Cursor Switching)

Guard Mode is a function enabled by default on Belkin NIAP PP4.0 SKMs. When active, Guard Mode restricts mouse movement to one computer at a time. This security feature helps prevent accidental channel switching by users. To switch between channels using the mouse cursor while Guard Mode is enabled, users will need to hold down the Left CTRL key while moving to the edge of the display.

Guard Mode can be disabled in the Administrator Configuration Terminal, which removes the need to hold down a key.

IMPORTANT: Guard Mode is enabled by default due to NIAP security regulations. It is recommended that you speak with your security group before disabling this feature.

Step 1: Log into the Administration Configuration Terminal.

Step 2: Choose Menu 3 – Configure SC.

Once finished, exit the terminal and power cycle the SKM to save the changes.

Using Custom Display Layouts

Since Belkin SKMs allow for up to four dedicated monitors connected to each computer, the SKM must be configured to know where these monitors are placed in relation to each other. Like configuring the display layout on your computer, it allows the SKM to know where the cursor can move between monitors or should move between computers.

Each SKM contains a default configuration of one display per connected computer laid out in a row. This can be changed by following the custom key commands in the user manual for that SKM model. If you are unable to find a display layout that matches yours, a custom layout can be created using the Belkin Custom Layout Configuration software available on the Belkin support site.

The software must be installed on a computer prior to use. It allows you to lay out the monitors to suit your needs and generates a file that can be uploaded to your SKM. The file is not locked to a single SKM unit, allowing it to be uploaded to multiple SKMs of the same model for easier administration.

Factory Restoring Your Belkin Secure KVM/KM

Belkin Secure KVMs and KMs contain a factory restore option that can be used when transferring an SKVM/SKM to a new facility, as well as for administrative or troubleshooting purposes. A factory restore will return your SKVM/SKM to the default settings from the factory as well as erase administrator users. There are some items that a factory restore will not erase:

Critical System Logs
Default Administrator Password

IMPORTANT: A factory restore will remove all child administrator accounts, but no changes will be made to the default administrator account. It is highly recommended that you do not perform a factory restore if you have lost the password to the default administrator account, as you will lose all access to the Administrator Terminal once the child administrator accounts are erased.

Step 1: Log into the Administration Configuration Terminal.

Step 2: Use the top row of number keys to access Menu 5 – Reset to Factory Defaults.

Your SKVM/SKM will perform a factory restore and then cycle off and back on. Once the SKVM powers on, it will be back in a factory-fresh state except for the items noted above that are not erasable.

Belkin International, Inc.
555 S Aviation Blvd, Suite 180
El Segundo, CA 90245-4852 USA
310-751-5569
belkin.com/cybersecurity

Support
Secure SKVM/SKM Support
800-282-2355

Sales
FederalBusinessDivision@belkin.com

Learn more: