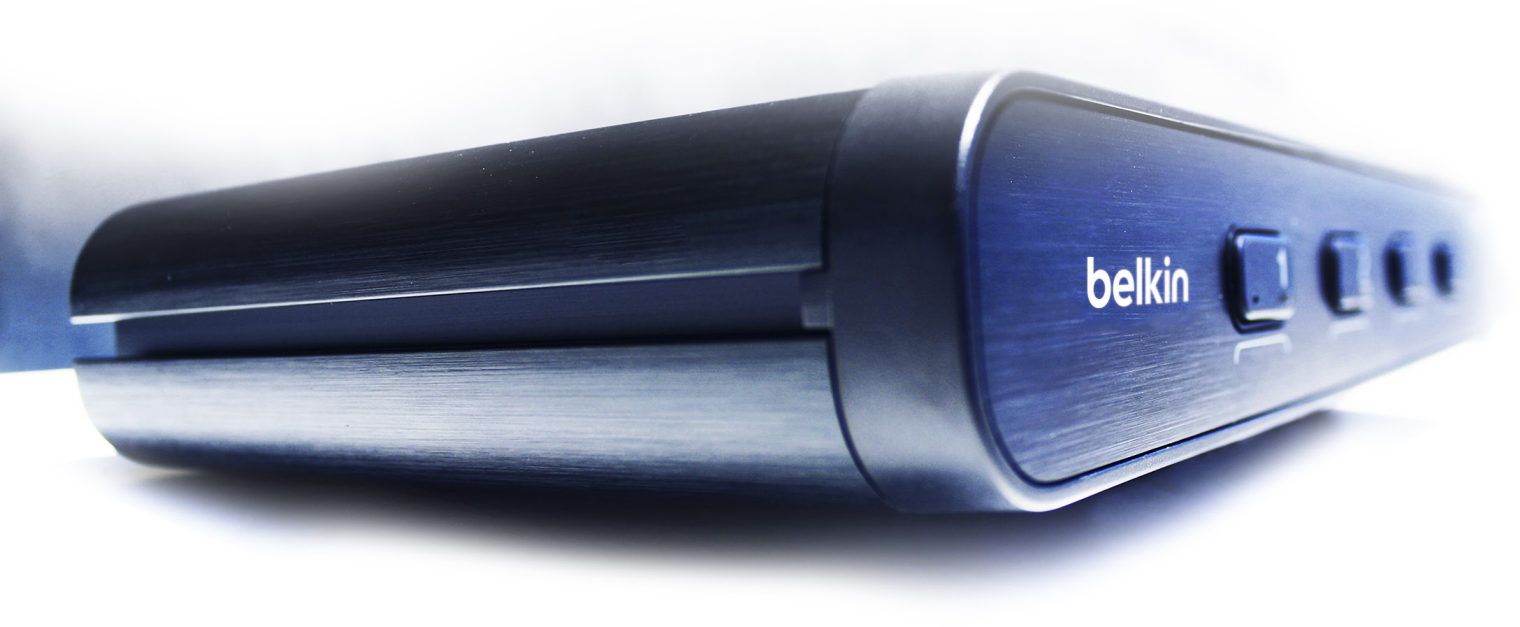
belkin • Your Essential Connection



Belkin Secure Products

Frequently Asked Questions

belkin

TABLE OF CONTENTS

BELKIN SECURE KVM

SECURITY FEATURES

What are the potential security risks when using an unsecure KVM?

There are many cases where one user needs to work simultaneously with a few computers, operating at various security levels. Users rely on the KVM used to protect the networks from system breaches and data leakages. If the KVM that is used is not secure, it may be easily exploited by a remote attacker to leak confidential information to non-secure networks, or even to the Internet.

Where are Belkin Secure KVMs manufactured?

Belkin Secure KVMs are designed in California and assembled in the USA., in an authorized factory meeting all the security requirements defined by the Common Criteria Protection Profiles. Belkin security products are also TAA-compliant and therefore meet the requirements of the U.S. Government's Trade Agreements Act (TAA). The product development and production life cycles are similar to MIL-STD high-security products.

What measures are taken to make sure that the Belkin Secure KVM is not physically tampered or interfered with throughout the product life cycle?

1. The Belkin Secure KVM is equipped with battery-backed, always-on, electronic sensors that render the KVM inoperable if the chassis is tampered with.
2. Secure, unique, and authenticated packaging is used to pack the Belkin Secure KVM when the KVM is ready for delivery. The packaging can only be opened via a tamper-evident label and ripstop banding that needs to be completely torn to gain access to the product. This packaging cannot be resealed once opened.
3. Serialized, traceable, holographic FIPS-compliant labels can be found on the Belkin Secure KVM, providing a visual indication of an external tampering attempt.
4. The reinforced, metal chassis is designed to reduce entry points and electromagnetic emissions.
5. All microcontrollers in the product are locked and firmware is encrypted to prevent possible firmware tampering.

What are optical data diodes and what are they used for in Belkin Secure KVMs?

At Belkin, we trust in physics, as software can be hacked or modified! Optical data diodes prevent peripherals from being used to breach systems. The optical data diodes convert digital data streams into light and back to digital to assure unidirectional data flow between the peripherals and the connected computers. The optical data diodes make it impossible for a computer to load information to a connected peripheral even if the driver is breached.

Why are emulators used in Belkin Secure KVMs and why are the emulators isolated?

An emulator is a special circuitry that duplicates the functions of one computer system into another computer system, so that the emulated behavior closely resembles the behavior of the real system. In the Belkin Secure KVM, the emulators are used as a firewall between the peripheral device and the computer, making sure that only "legal" information is passed. The Belkin secure KVM has a separate emulator for every computer port to assure that no information is shared between the computers, preventing data from being shared between two computers.

BELKIN SECURE KVM

SECURITY FEATURES

Why are the LEDS of the Num Lock and Caps Lock keys disabled?

Belkin Secure KVM blocks all data sent from the computer to the keyboard in order avoid attacks that use keyboard inherent security vulnerabilities (one example is the keyboard mailbox attack). Hardware - controlled unidirectional data flow allows the keyboard to communicate in only one direction, preventing the keyboard from receiving data from the computer. Keyboard strokes are sent from the keyboard to the connected computer, any commands sent from the computer to the keyboard will be blocked e.g. Num Lock and Caps Lock keys LEDs.

How does the Belkin Secure KVM reduce the risk of user errors?

1. Color coded chips can be used to associate the port with the network, and port button illumination indicates which computer the console is controlling
2. Audible indication when switching channels

Are Belkin Secure KVMs Failsafe / High Assurance products?

Yes, all Belkin Secure KVMs are designed and tested for failure modes to assure that even in the most severe failure modes; data would not leak through the product. Belkin Secure KVM products rely on physics (conversion of data to light) to assure that even if microcontrollers fail, data would not leak between computers. This level of assurance is critical when connected networks are of varying security levels (secret, top secret, etc.). Belkin Secure KVM products are designed to prevent a single point of failure. Data streams are fully isolated, and secure, even in the remote event of severe hardware failure.

How does the Belkin Secure KVM prevent unauthorized USB peripheral usage?

The Belkin Secure KVM is equipped with specific ports for Keyboard and Mouse only. Peripherals connected to USB hubs are not supported to prevent potential hacking or social attack. The Belkin Secure KVM product features a dedicated processor per computer port to emulate peripheral devices. This keeps each computer running on different security levels physically separated and secure at all times, and prevents any unintended data leakage between computers. Optical diodes are used to enforce unidirectional data flow from the peripheral devices to computers preventing potential leakage paths between computers; even in the event that one of the connected computers becomes compromised.

What is the Belkin Secure KVM active anti tampering system?

The Belkin Secure KVM active anti tampering system consists of unique electronic sensors that render the KVM permanently inoperable when the chassis is opened. The active anti tampering mechanism is battery-backed, and always-on, with a life span of over 15 years; making the Belkin Secure KVM one of the most reliable KVM switches in the industry.

Front-view F1DN104F-3

DETECTION OF KVM ATTACKS

Can an intrusion detection system (IDS) or an anti-virus software detect an attack on KVMs?

No. The attacks on KVMs are targeted and very particular, the code used in such attacks is written by professionals with specific intentions, taking advantage of KVM and or peripheral device vulnerabilities. In the case of a targeted attack(s) that use Zero Day Vulnerabilities, IDSs and anti-virus software are not efficient to protect the network.

What are the signs that your KVM has been tampered with?

1. The KVM did not arrive in its original secure packaging. If you are not sure how the packaging of the KVM is supposed to look, please contact Belkin support and request an image.
2. The holographic labels show signs of an external tampering attempt.
3. The screws show signs that they have been opened or replaced.
4. The LEDs of the KVM flash continuously indicating that the KVM has been physically tampered with.

What should you do if you think that the Belkin Secure KVM that you purchased, has been tampered with?

1. Stop using the Belkin Secure KVM immediately.
2. Contact your Information Security Officer.
3. Contact Belkin Support as soon as possible.

Please note that Belkin Secure KVM cannot be upgraded, serviced, or fixed.

What should I do if I discover a security vulnerability in the Belkin Secure KVM?

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 and let us know. Alternatively you can call our technical support toll-free number at (800) 282-2355. Belkin maintains proper system and procedures to handle such cases as required by worldwide security agencies.

What are the risks when having a microphone input switched by a KVM?

Eavesdropping and data leakage can be a result of having a microphone input switched by a KVM; as computer sound cards can be reprogrammed by malicious code to detect weak audio signals. For this reason, KVMs should not switch an analog microphone input signal to protect from this inherent vulnerability of analog audio leakages.

Is it possible to attack a secure KVM remotely?

Yes, it is possible to attack the KVM remotely, through the computers connected to the KVM, or through one of the peripherals connected to the KVM. This is especially applicable to secure KVMs connected between the Internet and classified networks.

DETECTION OF KVM ATTACKS

What is the risk of a shared display or projector with a secure KVM?

A shared display or projector can store information loaded on it from connected computers in multiple ways. A display may be used as a mail-box to leak data across connected computers through EDID, MCCS, firmware upgrade, asset tags etc. A typical display has up to 10 megabytes (MB) of storage which may be utilized by the attacker to load information through the KVM. When switched between networks the shared display is used as a shared storage device that is switched between the two networks.

What are the mounting options available for the Belkin Secure KVM?

Belkin Secure KVMs with up to four ports can be placed on the user's desktop, or an optional mounting bracket can be used to allow for under-the-desk, or side-wall mounting.

Brackets can be ordered directly from Belkin:

Belkin Part Numbers:

F1D006 – Secure KVM Single Head Mounting Bracket

F1D008 – Secure KVM Dual Head Mounting Bracket

What types of keyboards are supported by the Belkin Secure KVM?

All standard USB keyboards are supported by the Belkin Secure KVM. In some cases when using nonstandard keyboards that have extra function keys, the standard keys will work, while the nonstandard keys will be disabled. Some models also support legacy PS/2 keyboards.

Please note:
Keyboards which include built-in USB hubs are not supported to prevent hacking and social-based attacks.

Can VGA and DVI be connected at the same time to the Belkin Secure KVM?

The Belkin Secure KVM supports the DVI-I signals which means it can support both VGA (Analog) and DVI-D (Digital) video formats. However, the Belkin Secure KVM like all other KVMs cannot convert one signal to another, meaning that you either connect DVI-D or VGA sources to the KVM; depending on the display(s) connected to that KVM. In order to connect VGA and DVI at the same time, use the Belkin VGA to DVI Smart Cable to convert DVI to VGA (if the display is VGA) or to convert VGA to DVI (if the display is DVI). When using multiple head products (dual monitor) it is possible to have VGA and DVI console displays connected at the same time to each port. The video source needs to match the console display source. Contact Belkin for more information if you have any questions or concerns about connecting various video sources to the KVM, or need help determining the appropriate cables required for your setup.

What operating systems are supported by the Belkin Secure KVM?

Windows, Linux, Sun, and Mac OS are all supported with no need for any software installation.

Please note that Belkin Secure KVM products cannot be upgraded, serviced or fixed.

FUNCTIONAL FEATURES

Is it possible to hot-swap monitors when using the Belkin Secure KVM?

The Belkin Secure KVM reads the monitor information only once when the Belkin Secure KVM is powered up for security reasons. If monitors are swapped while the KVM is operating, the Belkin Secure KVM will use the settings of the previous monitor. When swapping monitors, it is recommended to power off the KVM, swap your monitors, and then reapply power to the KVM.

Do I need to install software with the Belkin Secure KVM?

No, there is no need to install any software.

Can I/Should I turn off the Belkin Secure KVM?

No, there is no need to turn off the KVM. Most Secure KVM products do not have a power switch. The Belkin Secure KVM Product consumes very little power when not used.

Does the Belkin Secure KVM support display EDID (Extended Display Identification Data) plug and play?

Yes, with new operating systems display EDID is a must. Without proper EDID communications, the connected display(s) may not work at all, or will not display properly. Because the EDID information can be used to attack connected computing devices and peripherals, the Belkin Secure KVM has a unique hardware based protection mechanism to ensure security when using EDID.

Does the Belkin Secure KVM affect video quality?

No, the video quality is not affected as long as proper cables are used.

Does the Belkin Secure KVM support VGA displays?

Yes, the Belkin Secure KVM supports DVI-I that enables VGA support with a simple cable or adapter.

Does the Belkin Secure KVM support VGA computers?

Yes, with the use of Belkin Secure Cables. Note that if a VGA computer is connected, then all other inputs must be VGA as well, including the display.

Can I use both USB and PS/2 peripherals at the same time?

Yes, USB and PS/2 peripherals can be used at the same time.

Can I use another power supply with the Belkin Secure KVM?

No, the power supply supplied with the Belkin Secure KVM is part of the unit and must be used.

Is PS/2 more secure in comparison to a USB device?

No, both devices can leak data.

USB is considered to be more protected against electrical leakage compared to PS/2, as it uses a differential signals, as opposed to a single-ended signal.

BELKIN SECURE KVM

FUNCTIONAL FEATURES

Does the Belkin Secure KVM support composite devices?

Yes the Belkin Secure KVM does support composite devices as long as the composite device is connected to the KVM mouse port.

Can I update the firmware in the Belkin Secure KVM?

No, for security reasons Belkin Secure KVMs are One-Time Programmable (OTP) protected, to prevent the possibility of any changes being made.

Can I prevent the CAC from being switched to specific computers?

Yes, on Belkin Secure KVMs that support CAC, each channel CAC port is controlled by a CAC switch next to each channel button on the KVM. Sliding the CAC switch to the left will disable the CAC port from being mapped on that specific channel.

In dual-head Secure KVM models, is it possible to have one "row" switching VGA while the other row switches "DVI"?

Yes, this is possible. Remember that the row switching VGA must have a VGA compatible display. Example: The bottom row of the dual head SKVM has all DVI computers and a DVI monitor connected, and the top row has all VGA computers and a VGA monitor connected. Please note that VGA and DVI cannot be mixed on the same row.

Can I use a CAC port to switch biometric readers?

Yes, most USB authentication devices can be used when using the Belkin CAC ports.

Can a wireless keyboard or mouse be used with a Belkin Secure KVM?

No. According to NIAP PP PSS Ver. 3.0 wireless peripherals should not be used for security reasons.

How do I know if the KVM will be compatible with my new equipment?

Belkin prides itself on 20 years of experience designing desktop KVMs. We perform rigorous compatibility testing on equipment used by Secure KVM customers. In the rare event of a compatibility issue, Belkin's dedicated Secure KVM support team can be contacted to provide quick assistance by phone or in person, even at secure locations.

I have new systems next to legacy systems. Do you have a product to support both?

Yes. Belkin has developed specialized cables with built-in electronics that convert DVI-D to HDMI and VGA, VGA to DVI-D, and USB to PS/2. These cables do not require external power supplies, and integrate easily with the Belkin Secure KVMs.

BELKIN SECURE KM

GENERAL INFORMATION

What is the difference between a KM and a KVM?

KVM's are designed to switch displays, allowing the user to only see and manage one target device at a time. When using a KM switch, users can see all the connected computers, securely, at the same time. A KM switch is a device that switches a single keyboard and mouse between multiple computers. A KM switch is essentially a KVM switch without the video switching; all displays are continuously connected to their respective computers, so that all connected device can be managed seamlessly, in real time. To navigate from one computer to the next, simply move your mouse cursor from one monitor to the next.

Can a Secure KVM be used as a KM?

No, Secure KVMs are designed to switch video as well as mouse and keyboard at the push of a button. On a KM, the switching channel is done by just moving the mouse cursor from monitor to monitor.

When should a Belkin Secure KM Switch be used?

A KM switch should be used when one user needs to work simultaneously with multiple displays attached to multiple computers using a single keyboard and mouse. Multiple displays can be connected to each computer that is connected to the Belkin Secure KM. The Belkin Secure KM is designed to have multiple computers connected and working simultaneously in any possible monitor setup.

SECURITY FEATURES

Are Belkin KM Switches as secure as Belkin KVM Switches?

The Belkin Secure KM Switch is a derivative of the award winning Belkin Secure KVM product line, and is equipped with the same high security features: Active Always-On Anti-Tampering, Heavy-Duty Tamper-Resistant Enclosure, Tamper Evident Label, Unidirectional Data Paths, Dedicated Processors for Emulation, USB Port Protection, Non- Reprogrammable Firmware, Tamper-Proof Hardware, and more.

Front-view F1DN104K-3

Rear-view F1DN104K-3

FUNCTIONAL FEATURES

Do I need to install software drivers with the Belkin Secure KM?

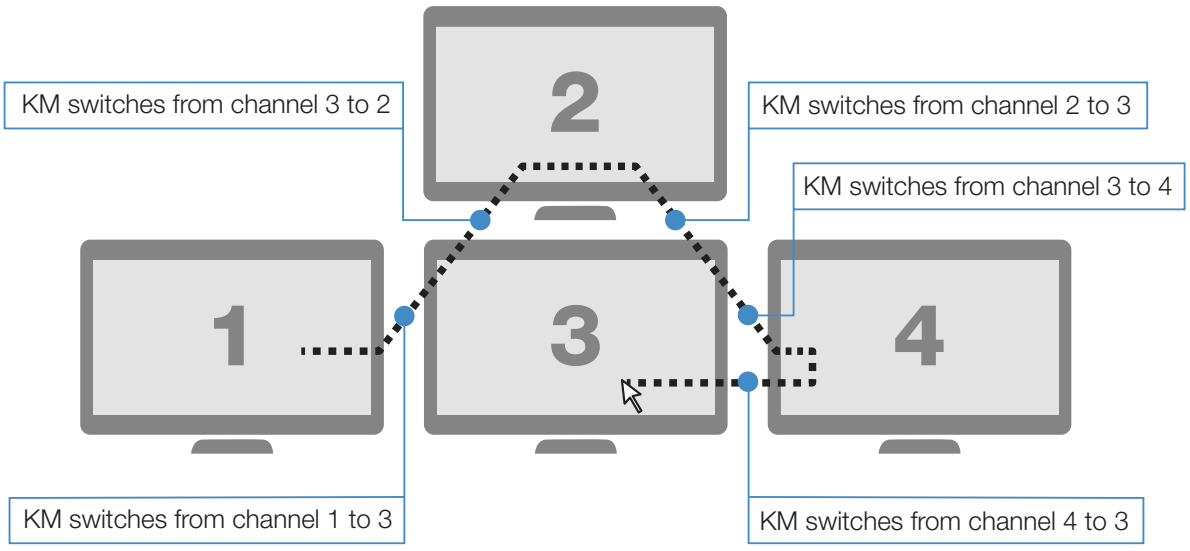
The Belkin Secure KM can be easily configured to support dual, triple, or quad head computers through a signed software driver. Single head installations, one monitor per computer, do not require any software installation. Customization of the KM monitor layout is to be done at the administrator level only, prior to a deployment to the end-users that will operate the device.

Can I use a KM with multiple-display computers?

Yes, The Belkin Secure KM can be easily configured to support dual, triple, or quad head monitors on up to eight computers. This allows the 4-Port Secure KM to support up to 16 monitors, and the 8-Port Secure KM to support up to 32 monitors.

What operating systems are supported by the Belkin Secure KM switch?

The Belkin Secure KM supports Windows, Linux and Mac operating systems. For configuring multiple-display computers and the KM monitor layout, only Windows is supported.



Seamless Cursor Switching (SCS)

BELKIN SECURE WINDOWING KVM

GENERAL INFORMATION

What is the difference between a KVM and a Windowing KVM?

KVM's are designed to switch displays, allowing the user to only see and manage one target device at a time. When using a Windowing KVM, the user can work simultaneously across computers at different security levels, without exposing the organization to the risks of information leakage through the KVM. The Belkin Secure Windowing KVM device uses advanced video processing technology to draw a high resolution dynamic "mosaic" of images generated by different computer sources.

SECURITY FEATURES

Is the Belkin Secure Windowing KVM as secure as the Belkin Secure KVM switches?

Yes. The Belkin Secure Windowing KVM Switch is a derivative of the award winning Belkin Secure KVM product line, and is equipped with the same high security features as the Belkin Secure KVM; Active Always-On Anti-Tampering, Heavy-Duty Tamper-Resistant Enclosure, Tamper Evident Label, Unidirectional Data Paths, Dedicated Processors for Emulation, USB Port Protection, Non- Reprogrammable Firmware, Tamper-Proof Hardware, and more.

Front-view F1DN204M-3

Rear-view F1DN204M-3

BELKIN SECURE WINDOWING KVM

FUNCTIONAL FEATURES

Can the Belkin Secure Windowing KVM use analog (VGA) computer output?

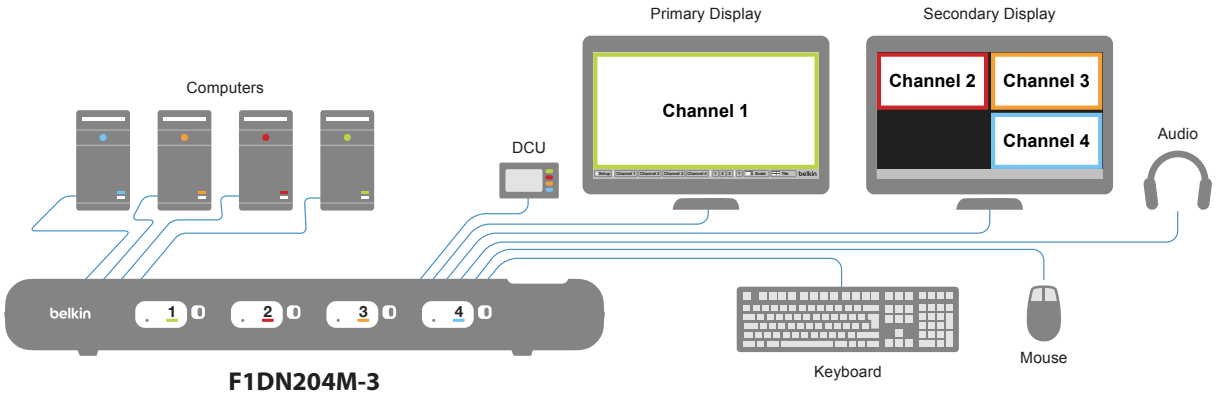
No. Only DVI is supported.

Can the Belkin Secure Windowing KVM scale video input?

Yes, The Belkin Secure Windowing KVM has an advanced scaling function allowing the user to scale the video source to ensure proper viewing and superb work experience. A user can fit four full HD sources on a single or dual HD displays by scaling each source, all in real time with no data loss.

It is possible to use a mouse other than the mouse supplied with the Belkin Secure Windowing KVM?

It is recommended to use the mouse supplied with the Belkin Secure Windowing KVM but if another type of mouse is used, it must be a five-button mouse, with a recommended mouse DPI of 5400 for best performance.



Belkin Secure Windowing KVM F1DN204M-3 System Diagram
Scale mode in Dual Display Extend Mode view

NIAP RELATED INFORMATION

If cables manufactured by another company are used together with the Belkin Secure KVM, does this affect the CC (Common Criteria)?

Yes, it is highly recommended to use the Belkin Cables together with the Belkin Secure KVM, in order to meet the security requirements defined by the Common Criteria Protection Profiles. All products are compliant with NIAP latest PP PSS ver. 3.0 standard.

Is the "Belkin Secure KVM" Common Criteria (CC) certified?

All of Belkin's Secure KVMs undergo a formal evaluation process to validate that the products meet the security requirements defined by the Common Criteria Protection Profiles.

Are Secure KVMs validated to the same levels equally as secure?

No. Although two Secure KVMs are listed as validated to the same Common Criteria level, they may not be equal. Manufacturers of Secure KVMs can add other features that may not be covered by current Protection Profile requirements. Refer to your Belkin Sales representative or visit www.belkinbusiness.com for additional details.

Are Belkin's Secure KVMs TAA-compliant and GSA-listed?

Yes. Belkin's Secure KVMs are manufactured in the United States in California, and are GSA-listed under contract #GS-35F-0085U.

What is NIAP?

(Derived from www.niap-ccevs.org)

The National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) have established a program under the National Information Assurance Partnership (NIAP) to evaluate IT product conformance to international standards. The program, officially known as the NIAP Common Criteria Evaluation and Validation Scheme for IT Security (CCEVS) is a partnership between the public and private sectors. This program is being implemented to help consumers and government agencies select commercial off-the-shelf information technology (IT) products that meet their security requirements and to help manufacturers of those products gain acceptance in the global marketplace.

What are EAL and Common Criteria?

(Derived from www.niap-ccevs.org)

The Common Criteria for Information Technology Security Evaluation (CC), ISO/IEC 15408 Standard, defines general concepts and principles of IT security evaluation and presents a general model of evaluation. It presents constructs for expressing IT security objectives, for selecting and defining IT security requirements, and for writing high-level specifications for products and systems. It specifies information security functional requirements and predefined assurance packages, known as Evaluated Assurance Levels (EALs), against which products' functions were tested and evaluated. EALs provided vendor and user flexibility to define functional and assurance requirements that are unique to operating environments obtaining an evaluated product best suited to those needs. The new NIAP PP PSS Ver. 3.0 standard no longer uses EALs for its products.

BELKIN SECURE PRODUCTS

NIAP RELATED INFORMATION

What is the Protection Profile?

(Derived from www.niap-ccevs.org)

A Protection Profile is the specification document used by a consumer, consumer group, vendor, or any consortium to specify what functional requirements they would like to have in commercial information assurance (IA) products, and to document to what assurance level(s) they would like to have the product tested. Protection Profiles serve two purposes:

- Provide customers with the ability to specify security requirements for their given environment (levels of concern/ robustness); and
- Serve to identify, for vendors, known markets for products that meet specified customer requirements.

What is CCEVS? What is its purpose?

(Derived from www.niap-ccevs.org)

The Common Criteria Evaluation and Validation Scheme (CCEVS) is a program under the NIAP to meet the security evaluation needs of both IT/IA product producers and users. Its purpose is to evaluate COTS IA and IA-enabled products (e.g., a firewall or an operating system) in accordance with the International Common Criteria for Information Technology Security Evaluation (generally referred to as the “Common Criteria”). It accomplishes this through the use of U.S.-government-accredited Common Criteria testing laboratories.

belkin • Your Essential Connection

belkinbusiness.com