

SECURE KVM SWITCHES

SOLUTIONS BROCHURE





Combat the variety of security threats that arise when sharing peripherals between computer networks with different security levels.

Why Secure KVM

Cyber threats are constantly evolving, becoming more frequent and sophisticated every day. Our reliance on technology, sharing of global resources and need for real-time collaboration have led to a growing web of data. While interconnectivity helps us work together more efficiently and effectively, it also leaves us increasingly vulnerable to devastating cyberattacks.

Major defense agencies and other organizations alike use advanced security measures to isolate networks and safeguard information from outside threats. However, there is one place where isolated networks and sensitive information come together: the user desktop.

Unsecure KVM switches are susceptible to cyberattacks and can allow cybercriminals to access classified data. If a cybercriminal wants to steal information off a classified server, they can attach a USB drive with malware on it into an unsecure KVM switch to access multiple servers instead of just one. Unsecure KVM switches are also susceptible to malicious use of LCD monitors (via EDID signal), microphones or CAC devices.

Through these methods, a wealth of classified information can get into the wrong hands and be used to harm government agencies.

Traditional KVM Switches

KVM switches allow access and management of multiple computers from a single workstation with a keyboard, mouse and video monitor. Users can easily access information and applications on completely separate systems by pushing a button or using keystrokes.

KVM technology provides monitoring solutions for automation, processes and workflow. It gives users improved operability and a quick return on investment due to better workplace ergonomics and productivity. KVM switches enable users to save space by reducing interface devices, save costs by eliminating redundant peripherals and react faster in critical situations.





Secure KVM Switches Keep Sensitive Data Classified

A secure KVM switch is a 2-, 4-, 8- or 16-port desktop switch that provides control and separation of PCs connected to networks of differing security classifications. Unlike traditional KVM switches, secure KVM switches can only be controlled using push button control. Hotkey commands are disabled, which ensures only the right users have access.

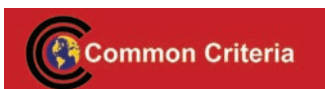
Secure KVM switches won't allow a USB drive that isn't recognized to access any information. It allows administrators to choose which USB devices are authorized or recognized. Secure KVM switches do much, much more to protect government agencies from today's most terrifying cyber threats.

NIAP Protection Profile for Secure KVM

Until recently, the National Information Assurance Partnership (NIAP) used Common Criteria Evaluation & Validation Scheme (CCEVS) to evaluate and approve KVM switches for security.

NIAP has implemented the Common Criteria Recognition Arrangement (CCRA) Management Committee Vision Statement for the application of the Common Criteria and no longer evaluates against Evaluation Assurance Levels (EAL). This strengthens evaluations by focusing on technology specific security requirements

As a result, they upgraded the Protection Profile (PP) for peripheral sharing switches to PPS 3.0 NIAP Protection Profile for Peripheral Sharing Switch Version 3.0, which are tests regarding the process of the design, testing, verification and shipping of security products. This protection profile is an international, standardized process for information technology security evaluation, validation and certification.



Rigid Security Features Inside Black Box Secure KVM Switches

- Mechanical, electrical and optical signal isolation to prevent hacking and data leakage → absolute isolation/no data leakage between secure ports and the outside world
- Protected firmware keeps intruders from reprogramming or reading firmware (non-reprogrammable ROM)
- Opto-isolated USB ports and keyboard/internal cache wiping keep USB data paths electrically isolated from each other to prevent USB data leakage between ports
- Secure EDID/video & AUX emulation restricts discovery of newly-connected displays during switching operations which prevents unwanted and unsecured data from getting transmitted between the computers and the display
- Chassis intrusion protection: equipped with active anti-tamper switches and external hologram, tamper-evident seals
- Optional configurable Common Access Card (CAC) support for smart cards, biometric readers and registration of external USB devices
- Unidirectional data flow to special peripherals like a projector, printer or audio system
- Certified to NIAP PP 3.0, the highest Common Criteria level (Protection Profile for Peripheral Sharing Switch Version 3.0)
- TAA compliant and made in U.S.

Tested and Certified to the Latest NIAP PP 3.0 Security Profile

Secure KVM switches from Black Box are designed for use in secure defense and intelligence applications where sensitive data must be protected. The secure KVM switches from Black Box are NIAP PP 3.0 certified and equipped with strongest security features that meet today's information assurance safe control standards. The switches contain unique hardware configurations that prevent data leakage between PCs and connected peripherals that eliminate any potential cyber threat.

Multi-Level Security for Strict Information Assurance

An absolute isolation of the mechanical, electrical and optical signals through air gapping prevents hacking and data leakage between the ports and the outside world. Each port of the secure KVM switch uses its own isolated data channels. By up-front switching on another target computer, the KVM switch erases the internal cache and keyboard data to ensure that no residual data remains in the channel. The fixed, secure firmware and ROM are non-reprogrammable and keeps intruders from reading or reprogramming via unwanted firmware upgrades.

Chassis Intrusion Protection

The secure KVM switches feature active anti-tamper switches; external hologram, tamper-evident seals; and a long-life, internal anti-tampering battery. If the cover is removed from the chassis, the KVM switch shuts down connection with all attached PCs and peripherals and disables any functionality to protect against any attempt of physical intrusion.

Keyboard & Mouse Emulation

The secure KVM switch emulates the presence of a keyboard and mouse for every attached computer through a USB cable. Both selected and non-selected computers maintain a constant connection with the switch's keyboard mouse emulation controllers, allowing for ultra-fast switching and restricting discovery of newly connected peripherals during switching operations. Emulation of keyboard and mouse also prevents direct connection between the peripherals and the connected computers, shielding systems from potential vulnerabilities.

Fully Configurable Common Access Card (CAC) Port for External USB Peripherals

Many secure KVM switches support CAC (Common Access Card) devices, such as smart-card and biometric readers that bolster security when using the device. However, BlackBox takes CAC security even further, allowing authenticated administrators to register and assign specific peripheral devices to the CAC port (optional). Users can then switch the connection between the assigned device along with the KVM switching of the connected computers.

Restricts New Monitor Connections During Switching

The secure KVM switches simulate a generic EDID as default, allowing them to operate most of the connected monitors. Selected and non-selected computers maintain constant connection with the switch's video and AUX emulation controllers, allowing for ultra-fast switching and restricting discovery of newly connected monitors during switching operations. This shields systems from potential vulnerabilities through unwanted and unsecure data transmittance through DDC lines.



Ideal for Multiple Industries



Government



Defense & Military

Control Rooms for
Traffic Management

Banking & Finance



Education

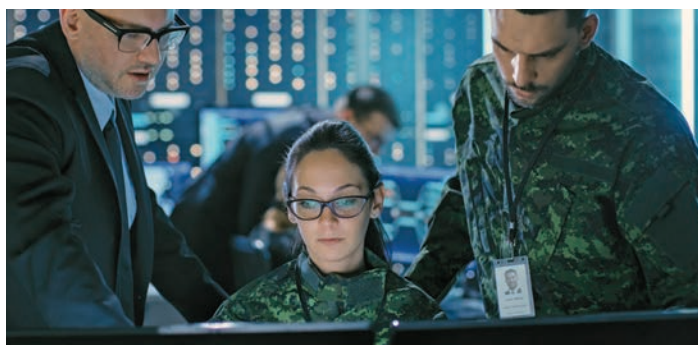


Healthcare



R&D Departments

Use Cases

**Defense Communications Center**

A defense customer came to Black Box with two pressing issues: inefficient network access and a cluttered workspace.

Their operators needed to access multiple computer networks in secure communications centers. It was a time-consuming process because each computer network required a separate keyboard, monitor and mouse which meant the operator had to move between the different systems to access sensitive data and intelligence networks. This also required a table for all six different monitors, six different keyboards and six different mice, which made for a cluttered and cramped workspace.

To overcome these challenges, they purchased an 8-Port Secure KVM Switch from Black Box that reduced their configuration to one monitor, one keyboard and one mouse, saving valuable time for operators having to switch between multiple networks and opening up a wealth of desk and office space. Now they operate more efficiently in a clean workspace while ensuring their vital data has no way of being compromised.

**Aerospace**

A company contacted Black Box when they required a high-end secure solution for an aerospace project. Project engineers needed to switch between an open (green) and a secure (red) network. Black Box suggested the 4-Port DVI USB Secure KVM Switch, which perfectly suits all their requirements. To date, more than 1,000 Black Box Secure KVM Switches have been installed at this company.

Enterprise

After a merger, a large enterprise was left with two separate networks. Operators at the enterprise needed quick, secure access to both networks to complete their jobs effectively. This prompted the enterprise to look into KM switching products.

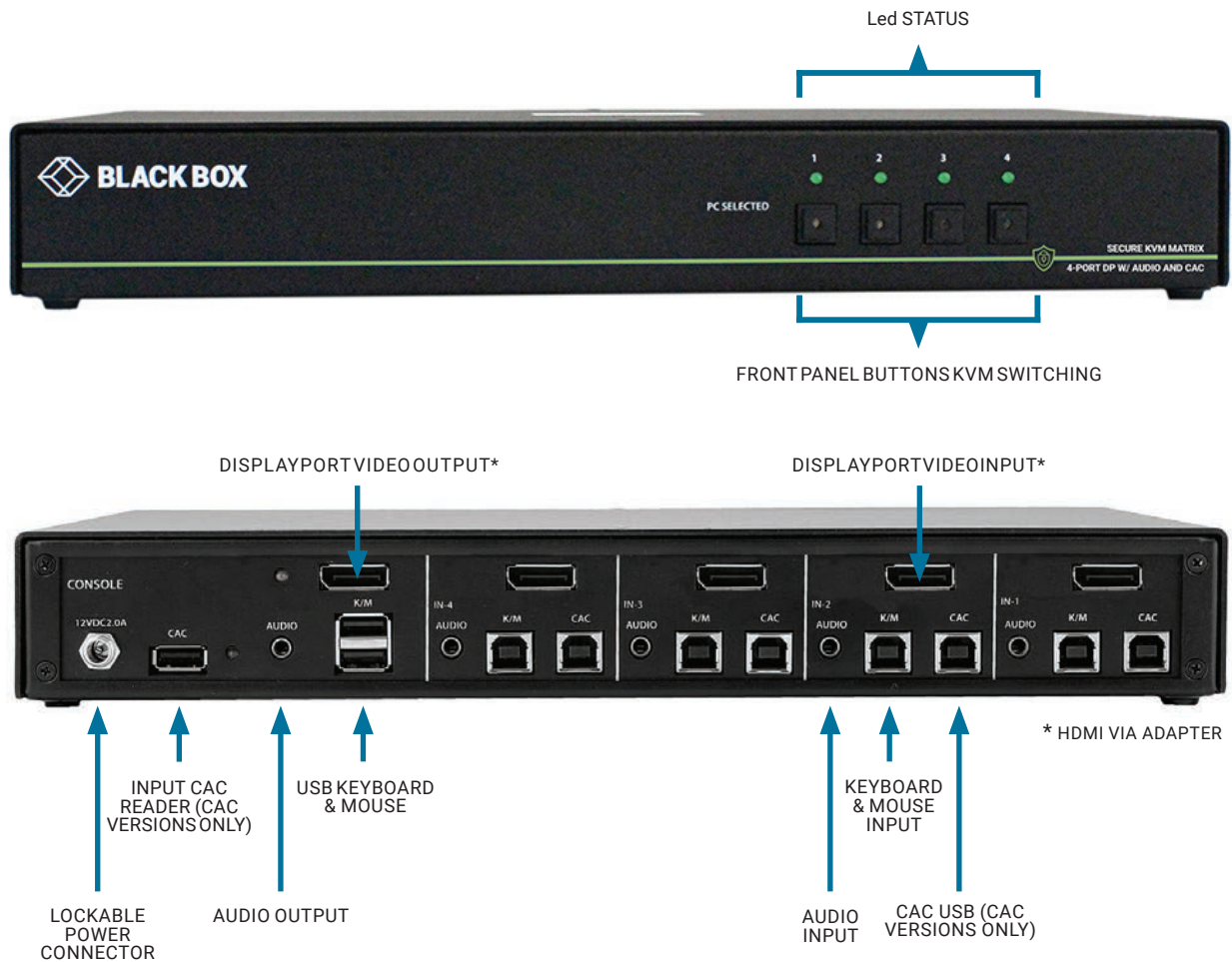
The enterprise requested Black Box Secure KM Switches. These switches let operators move freely between the two separate networks on a single desktop. They also saved desktop space and kept security separate on the two different networks.



Secure KVM Product Overview

Secure KVM Switch Design

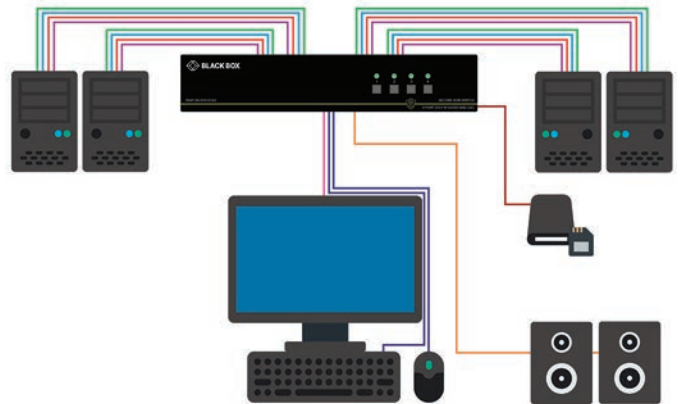
Example 4-Port Secure KVM Switch, Single User, Displayport, USB and CAC (SS4P-SH-DP-UCAC)



Secure Desktop KVM Switch Types

Secure Desktop KVM Switches, Single User

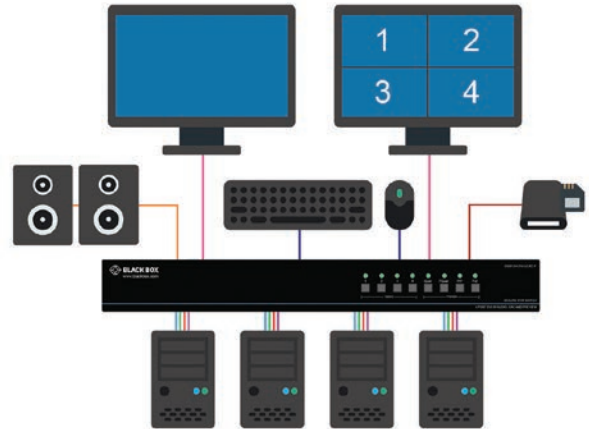
- Share a single user console between two, four, eight or 16 computers
- Available with DVI-I, DisplayPort or HDMI video
- High-quality DisplayPort 1.2/HDMI video with resolutions up to 4K Ultra-HD (3840 × 2160 @ 60Hz) and best DVI-I dual-link resolution up to 2560 x 1600 @ 60Hz
- Choose from models with single-, dual- or quad-monitor connections to the console
- USB keyboard/mouse plus stereo audio
- Available with or without CAC support
- NIAP 3.0 certified



Find the Right Product in the Selector on Pages 9 & 10.

DVI-I Secure KVM Switch, Single User With 4-IN-1 Window Display

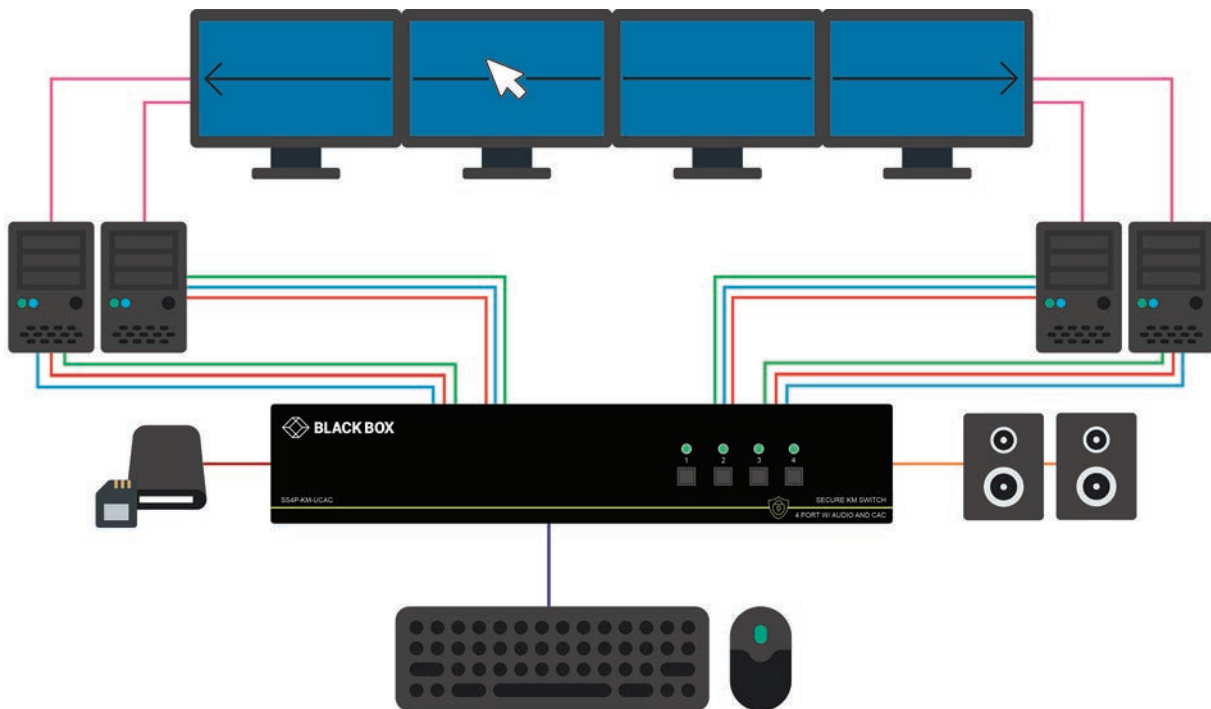
- Share a single user console between four computers, supports Quad, T-Quad, PIP, and Full Picture modes
- Monitor all sources concurrently on a 4-in-1 split screen while working with a second full-screen display on your active computer
- DVI-I video supporting single-link DVI, dual-link DVI and VGA
- Best dual-link resolution up to 2560 x 1600
- USB keyboard/mouse plus stereo audio
- CAC support for smart card readers and special peripheral assignment
- NIAP 3.0 doesn't have a testing profile for windowing displays.



Find the Right Product in the Selector on Page 10.

Secure Desktop KM Switches

- Switch by moving your mouse from monitor to monitor (Glide & Switch)
- View multiple sources concurrently through dedicated computer/monitor connections
- Stereo audio support
- Share a single user console with USB keyboard and mouse between four or eight computers
- Stereo audio support
- Available with or without CAC support
- NIAP 3.0 certified

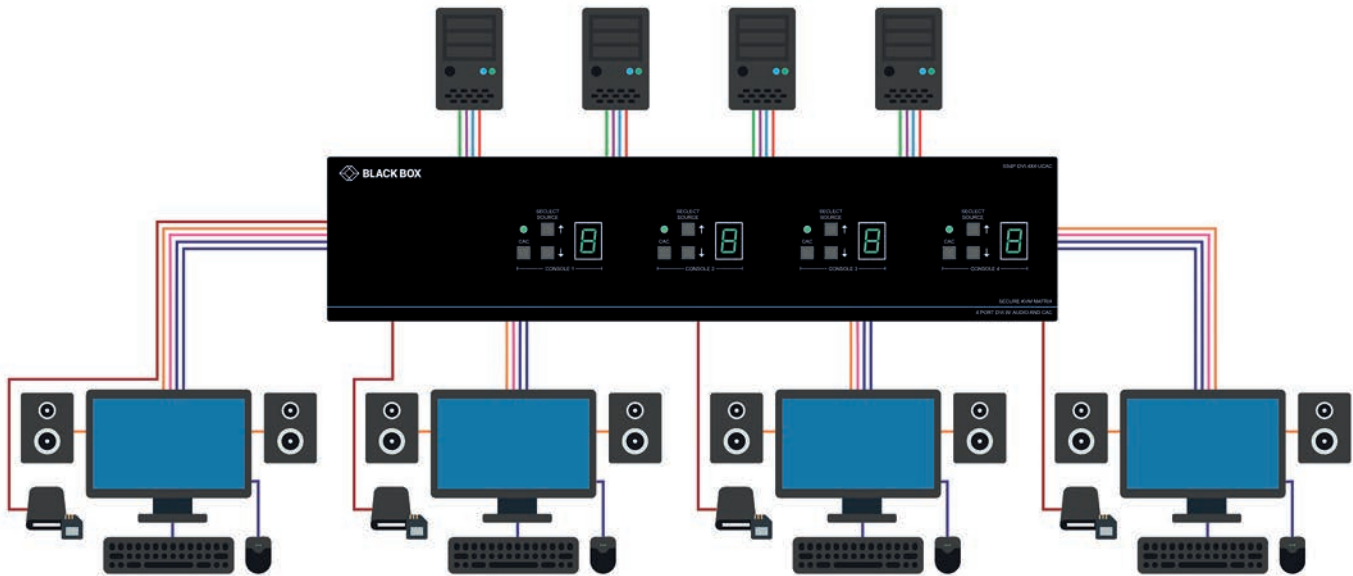


Find the Right Product in the Selector on Page 11.

Secure KVM Product Overview

DVI-I Secure KVM Matrix Switches, Multi-User

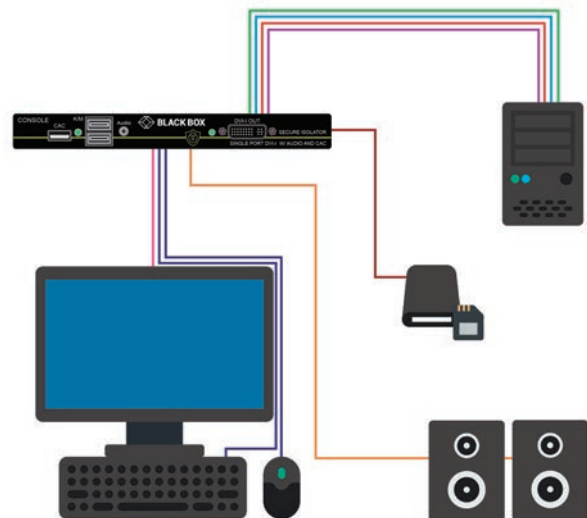
- Access for two or four users to four or eight computers
- DVI-I video supporting single-link DVI, dual-link DVI and VGA up to 2560 x 1600
- USB keyboard/mouse plus stereo audio
- CAC support for smart card readers and special peripheral assignment
- Support most monitors through Secure EDID Learning/Emulation
- Windows, Mac and Linux OS compatible
- NIAP 3.0 certified



Find the Right Product in the Selector on page 11.

Secure Peripheral Protector

- Blocks the direct connection between a host PC or laptop and a peripheral device exposed to security threats, such as a printer, projector, speaker or any other peripheral device that shares access with a classified computer or network
- Ensures unidirectional data flow of video, USB and audio from the computer to the peripheral
- Supports DVI-I video, USB and audio
- Supports most monitors through Secure EDID Learning/Emulation
- Stereo audio support
- Windows, Mac and Linux OS compatible
- CAC support
- NIAP 3.0 certified



Find the Right Product in the Selector on Page 10.



DisplayPort Secure KVM Switches NIAP 3.0 Certified						
						
Item #	SS2P-SH-DP-U/ SS2P-SH-DP-UCAC	SS4P-SH-DP-U/ SS4P-SH-DP-UCAC	SS8P-SH-DP-U/ SS8P-SH-DP-UCAC	SS2P-DH-DP-U/ SS2P-DH-DP-UCAC	SS4P-DH-DP-U/ SS4P-DH-DP-UCAC	SS4P-QH-DP-UCAC
Description	2-Port Secure KVM Switch, Single User, 4K DisplayPort Single Head	4-Port Secure KVM Switch, Single User, 4K DisplayPort Single Head	8-Port Secure KVM Switch, Single User, 4K DisplayPort Single Head	2-Port Secure KVM Switch, Single User, 4K DisplayPort Dual Head	4-Port Secure KVM Switch, Single User, 4K DisplayPort Dual Head	4-Port Secure KVM Switch, Single User, 4K DisplayPort Quad Head
# of Sources (Max.)	2	4	8	2	4	4
Computer Compatibility	Windows, Mac and Linux OS					
Max. Resolution	4K up to 3840 x 2160 @ 60 Hz					
Monitor Compatibility	Most monitors through Secure EDID Learning and Emulation					
Ports to User Console						
Monitor Connection(s)	1x DisplayPort 1.2			2x DisplayPort 1.2		4x DisplayPort 1.2
Keyboard Mouse Connections	2x USB 1.1 Type A, keyboard and mouse only					
Audio Output	1x 3.5mm audio jack with balanced speaker outputs and switching					
CAC Support (-UCAC Models Only)	1x USB Type A, fully configurable					
Ports to Computers						
Video Input(s)	1x DisplayPort 1.2 per source		2x DisplayPort 1.2 per source		4x DisplayPort 1.2 per source	
Keyboard Mouse Input	1x USB 1.1 Type B with USB emulation per source					
Audio Input	1x 3.5mm audio jack per source					
CAC Support (-UCAC Models Only)	1x USB Type B per source					

HDMI Secure KVM Switches, NIAP 3.0 Certified				
				
Item #	SS2P-SH-HDMI-U/ SS2P-SH-HDMI-UCAC	SS4P-SH-HDMI-U/ SS4P-SH-HDMI-UCAC	SS2P-DH-HDMI-U/ SS2P-DH-HDMI-UCAC	SS4P-DH-HDMI-U/ SS4P-DH-HDMI-UCAC
Description	2-Port Secure KVM Switch, Single User, 4K HDMI Single Head	4-Port Secure KVM Switch, Single User, 4K HDMI Single Head	2-Port Secure KVM Switch, Single User, 4K HDMI Dual Head	4-Port Secure KVM Switch, Single User, 4K HDMI Dual Head
# of Sources (Max.)	2	4	2	4
Computer Compatibility	Windows, Mac and Linux OS			
Max. Resolution	4K up to 3840 x 2160 @ 60 Hz			
Monitor Compatibility	Most monitors through Secure EDID Learning and Emulation			
Ports to User Console:				
Monitor Connection(s)	1x HDMI 1.4		2x HDMI 1.4	
Keyboard Mouse Connections	2x USB 1.1 Type A, keyboard and mouse only			
Audio Output	1x 3.5mm audio jack with balanced speaker outputs and switching			
CAC Support (-UCAC Models Only)	1x USB Type A, fully configurable			
Ports to Computers:				
Video Input(s)	1x HDMI 1.4 per source		2x HDMI 1.4 per source	
Keyboard Mouse Connections	1x USB 1.1 Type B with USB emulation per source			
Audio Input	1x 3.5mm audio jack per source			
CAC Support (-UCAC Models Only)	1x USB Type B per source			



DVI-I Secure KVM Switches (VGA via Adapter), NIAP 3.0 Certified								
								
Item #	SS2P-SH-DVI-U/ SS2P-SH-DVI-UCAC	SS4P-SH-DVI-U/ SS4P-SH-DVI-UCAC	SS8P-SH-DVI-U/ SS8P-SH-DVI-UCAC	SS16P-SH-DVI-UCAC	SS2P-DH-DVI-U/ SS2P-DH-DVI-UCAC	SS4P-DH-DVI-U/ SS4P-DH-DVI-UCAC	SS8P-DH-DVI-UCAC	SS4P-QH-DVI-UCAC
Description	2-Port Secure KVM Switch, Single User, DVI-I Single Head	4-Port Secure KVM Switch, Single User, DVI-I Single Head	8-Port Secure KVM Switch, Single User, DVI-I Single Head	16-Port Secure KVM Switch, Single User, DVI-I Single Head	2-Port Secure KVM Switch, Single User, DVI-I Dual Head	4-Port Secure KVM Switch, Single User, DVI-I Dual Head	8-Port Secure KVM Switch, Single User, DVI-I Dual Head	4-Port Secure KVM Switch, Single User, DVI-I Quad Head
# of Sources (Max.)	2	4	8	16	2	4	8	4
Computer Compatibility	Windows, Mac and Linux OS							
Max. Resolution	2560 x 1600 @ 60 Hz							
Monitor Compatibility	Most monitors through Secure EDID Learning and Emulation							
Ports to User Console:								
Monitor Connection(s)	1x DVI-I				2x DVI-I		4x DVI-I	
Keyboard Mouse Connections	2x USB 1.1 Type A, keyboard and mouse only							
Audio Output	1x 3.5mm audio jack with balanced speaker outputs and switching							
CAC Support (-UCAC ModelsOnly)	1x USB Type A, fully configurable							
Ports to Computers:								
Video Input(s)	1x DVI-I per source				2x DVI-I per source		4x DVI-I per source	
Keyboard Mouse	1x USB 1.1 Type B with USB emulation, 2x PS/2 miniDIN6 per source							
Audio Input	1x 3.5mm audio jacks with balanced speaker outputs and switching per source							
CAC Support (-UCAC Models Only)	1x USB Type B per source							

	Multi-Viewer NIAP, NIAP 3.0 Certified	Peripheral Protector NIAP 3.0
		
Item #	SS4P-SH-DVI-UCAC-P	SS1P-DVI-UCAC-P
Description	4-Port Secure KVM Switch, DVI-I with 4-in-1 Multi-View	1-Port Secure Peripheral Protector
# of Sources (Max.)	4	1 peripheral
Monitor Connections Per Console	2	N/A
Max. Resolution	2560 x 1600 @ 60 Hz	2560 x 1600 @ 60 Hz
Ports to User Console:		Peripheral Ports:
Monitor Connection(s)	2x DVI-I (1x full screen, 1x quad source view)	1x DVI-I
Keyboard Mouse Connections	2x USB 1.1 Type A	2x USB 1.1 Type A
Audio Output	1x 3.5mm audio jack	1x 3.5mm audio jack
CAC Support	1x config. USB Type A	1x 1 config. USB Type A
Ports to Computers:		
Video Input(s)	1x DVI-I per source	1x DVI-I
Keyboard Mouse Connections	1x USB 1.1 Type B emulated per source	1x USB 1.1 Type B emulated
Audio Input	1x 3.5mm audio jack per source	1x 3.5mm audio jack
CAC Support (-UCAC Models Only)	1x USB Type B per source	1x USB Type B



DVI-I KVM Matrix Switches NIAP 3.0 Certified					KM Switches, NIAP 3.0 No Switched Video Ports	
						
Item #	SS4P-DVI-4X2-UCAC	SS8P-DVI-8X2-UCAC	SS4P-DVI-4X4-UCAC	SS8P-DVI-8X4-UCAC	SS8P-DVI-8X4-UCAC	SS8P-KM-U/ SS8P-KM-U
Description	4x2 Secure KVM Matrix Switch, DVI-I	8x2 Secure KVM Matrix Switch, DVI-I	4x4 Secure KVM Matrix Switch, DVI-I	8x4 Secure KVM Matrix Switch, DVI-I	4-Port Secure KM Switch, Single User	8-Port Secure KM Switch, Single User
# of Sources (Max.)	4	8	4	8	4	8
Computer Compatibility	Windows, Mac and Linux OS				Windows, Mac and Linux OS	
# of Users	2	2	4	4	1	1
Monitor @ Console	1	1	1	1	N/A	
Max. Resolution	2560 x 1600 @ 60 Hz				N/A	
Monitor Compatibility	Most monitors through Secure EDID Learning and Emulation				N/A	
Ports to User Console:						
Monitor Connection	1x DVI-I per console				N/A, monitors keep direct computer connection	
Keyboard Mouse Connections	2x USB 1.1 Type A, keyboard mouse only per console				2x USB 1.1 Type A, keyboard and mouse only	
Audio Output	1x 3.5mm audio jack with balanced speaker outputs and switching per console				1x 3.5mm audio jack balanced output & switching	
CAC Support	1x USB Type A, fully configurable per console				1x USB Type A, fully configurable	
Ports to Computers:						
Video Inputs	1x DVI-I per source				N/A	
Keyboard Mouse Connections	1x USB 1.1 Type B with USB emulation per source				1x USB 1.1 Type B with USB emulation per source	
Audio Input	1x 3.5mm audio jacks with balanced speaker outputs and switching per source				1x 3.5mm audio jack per source	
CAC Support (-UCAC Models Only)	1x USB Type B per source				1x USB Type B per source	

Accessories	
Secure KVM Switch Cables	
SKVMCBL-DP-06	DisplayPort, USB, 3.5mm Audio; 1,8m
SKVMCBL-HDMI-06	HDMI, USB, 3.5mm Audio; 1,8m
SKVMCBL-DVI-06	DVI, USB, 3.5mm Audio; 1,8m

Contact Black Box

Not sure what you need? Contact our KVM experts.
Call 1.877.877.2269 or visit www.blackbox.com/securekvm



WHY BLACK BOX?

EXPERTISE

Black Box project engineers can assist with system assessment, design, deployment and training.

BREADTH

Black Box offers the most comprehensive suite of engineered KVM solutions in the industry.

SUPPORT

Reflecting our commitment to complete satisfaction, our dedicated team of highly trained support technicians is available by phone free of charge, 24 hours a day, every day of the year.

WARRANTIES

Multi-year warranties with multi-year extensions and replacement options are available.

EXPERIENCE

Providing leading technology solutions since 1976, Black Box helps more than 175,000 customers in 150 countries build, manage, optimize and secure IT infrastructures.

CENTER OF EXCELLENCE

Black Box offers a Center of Excellence featuring professional services and support agreements that help optimize customers' systems and maximize uptime.

SERVICE LEVEL AGREEMENTS

Our service level agreements give customers access to technical support, product training, dedicated application engineers and more.

