

# 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 defence agencies and other organisations 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 stick a USB drive with malware or a virus on it into a KVM switch to access multiple servers instead of just one. KVM switches are also susceptible to malicious use of LCD monitors (via EDID signal), microphones or inadequate CAC implementation.

Also, cybercriminals can pull hardware information through soundwaves from unsecure KVM switches. They can get programmable ROM sequences from soundwaves, which lets cybercriminals reconfigure or reprogram the server to make it unsecure. Through these methods, a wealth of classified information can get into the wrong hands and be used to harm the organisation.

### 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.





SS4P-DH-DP-UCAC



## 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 recognised to access any information. It allows administrators to choose which USB devices are authorised or recognised. It features non-reprogrammable ROM to block the pulling of hardware information from soundwaves. And that's just the tip of the iceberg. Secure KVM switches do much, much more to protect. Government agencies from today's most terrifying cyber threats.

Now, as desktop security becomes more critical than ever, Black Box is introducing a signature line of Secure KVM & KM switches. NIAP 3.0-certified secure KVM switches provide complete isolation between computer networks while sharing the same peripheral set. Each port uses its own isolated data channel to ensure absolutely no data leakage between ports with classified information and untrusted ports. A wide range of security features protects against cyber threats, while the tamper-proof hardware design prevents physical manipulation.

### 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, standardised 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 the highest 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 upfront 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, reprogramming via unwanted firmware upgrades or physically removing.

### 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, bolstering security when using the device. However, Black Box 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 &  
MILITARYCONTROL ROOMS FOR  
TRAFFIC MANAGEMENTBANKING AND  
FINANCE

EDUCATION



HEALTHCARE



R&amp;D DEPARTMENTS

## USE CASES



## DEFENSE COMMUNICATIONS CENTRE

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 centres. 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 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. More than 1.000 secure KVM switches have already been installed.

## ENTERPRISE

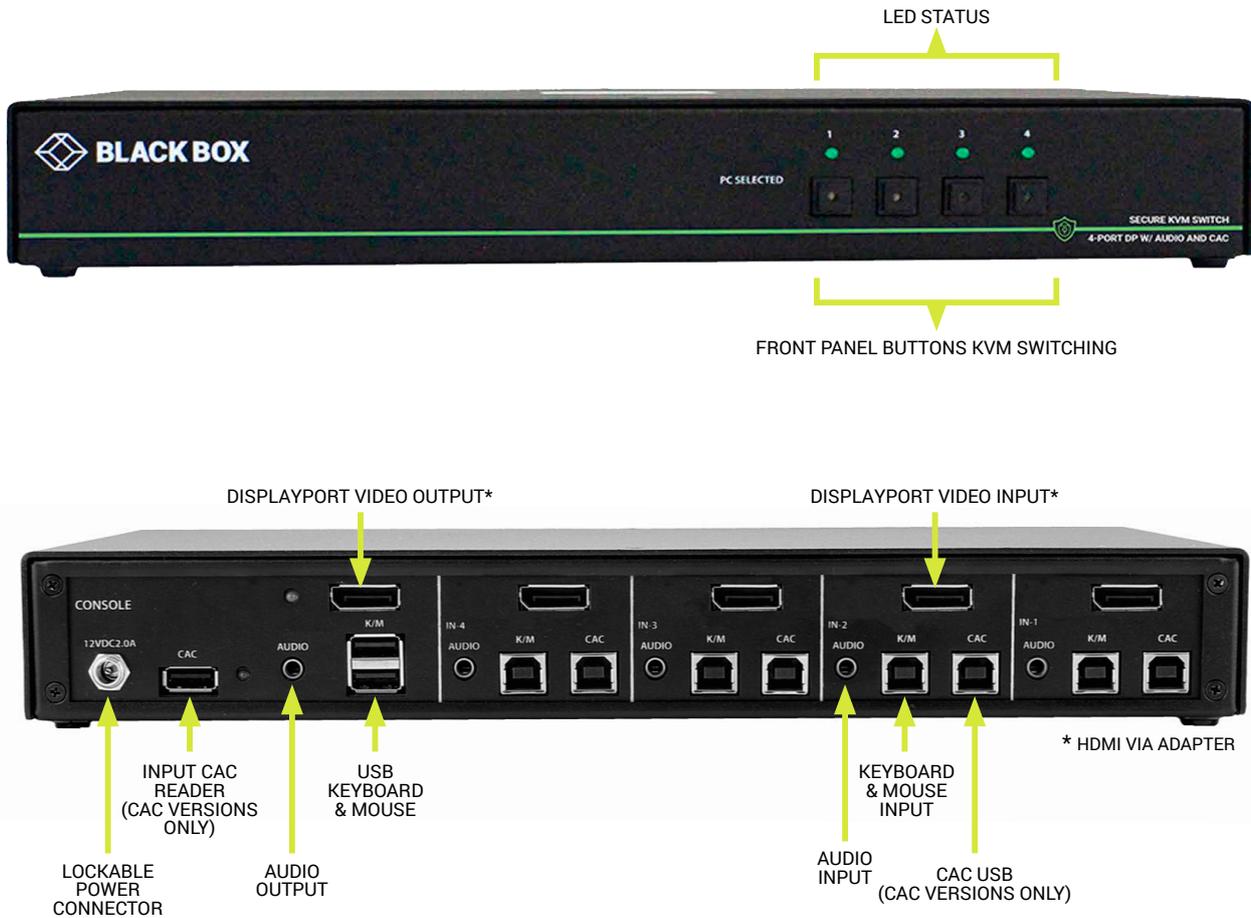
Sharing of global resources, and need for real time collaboration have led to a growing web of data. While interconnectivity helps organisations work together more efficiently and effectively, it also leaves them increasingly vulnerable to devastating cyberattacks. Ultimately systems that access the Internet need to be kept away from other systems which are used for sensitive corporate or personal data. To maintain their information assurance, many organisations are replacing standard with secure KVM switches.



# SECURE KVM PRODUCT OVERVIEW

## SECURE KVM SWITCH DESIGN

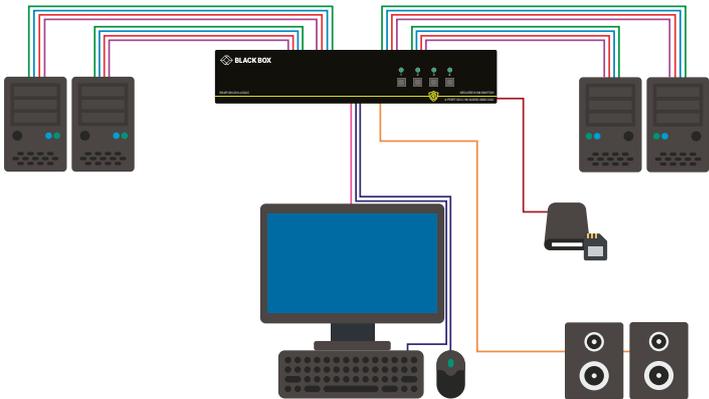
Example 4-Port Secure KVM Switch, single user, Displayport, USB and CAC (SS4P-SH-DP-UCAC)



## 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 (3840x2160 @ 30Hz) and best DVI-I dual-link resolution up to 2560 x1600 @ 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

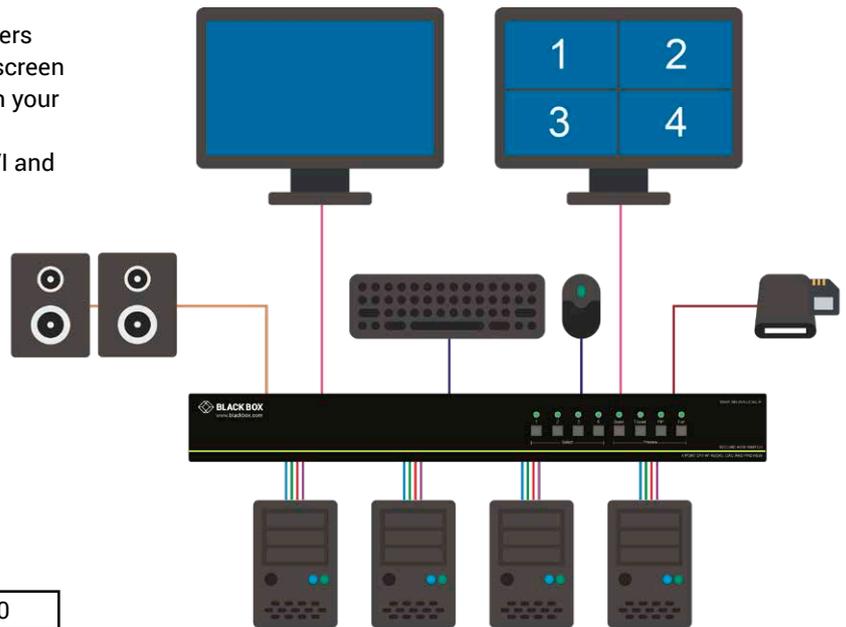


**i** Find the right product in the selector on pages 9 & 10



## DVI-I SECURE KVM SWITCH, SINGLE USER WITH 4-IN-1 WINDOW DISPLAY

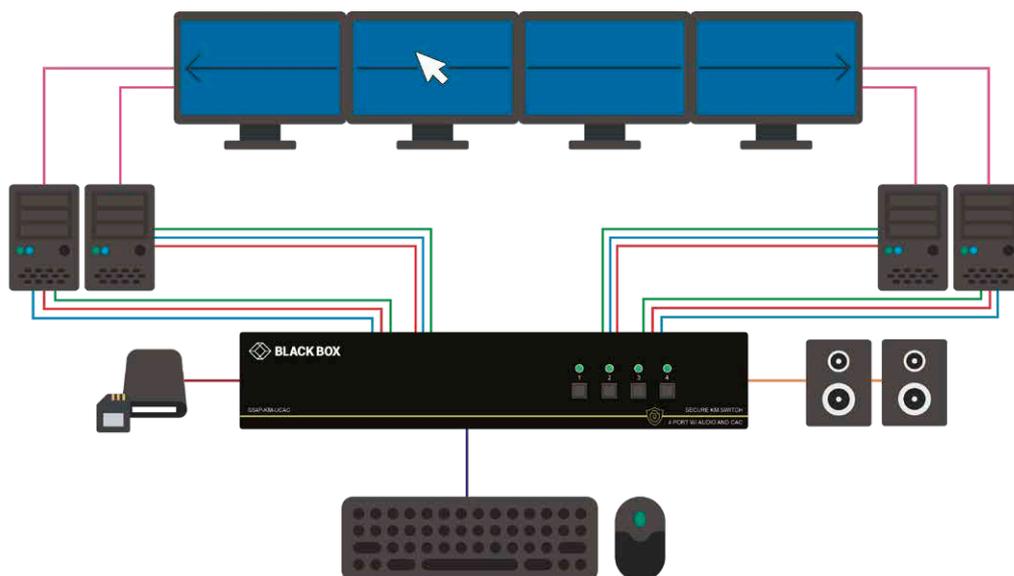
- Share a single user console between four computers
- Monitor all sources concurrently on a 4-in-1 split screen while working with a second full-screen display on your active computer
- DVI-I video supporting single-link DVI, dual-link DVI and VGA
- Best dual-link resolution up to 2560 x1600
- USB keyboard/mouse 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.



**i** 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

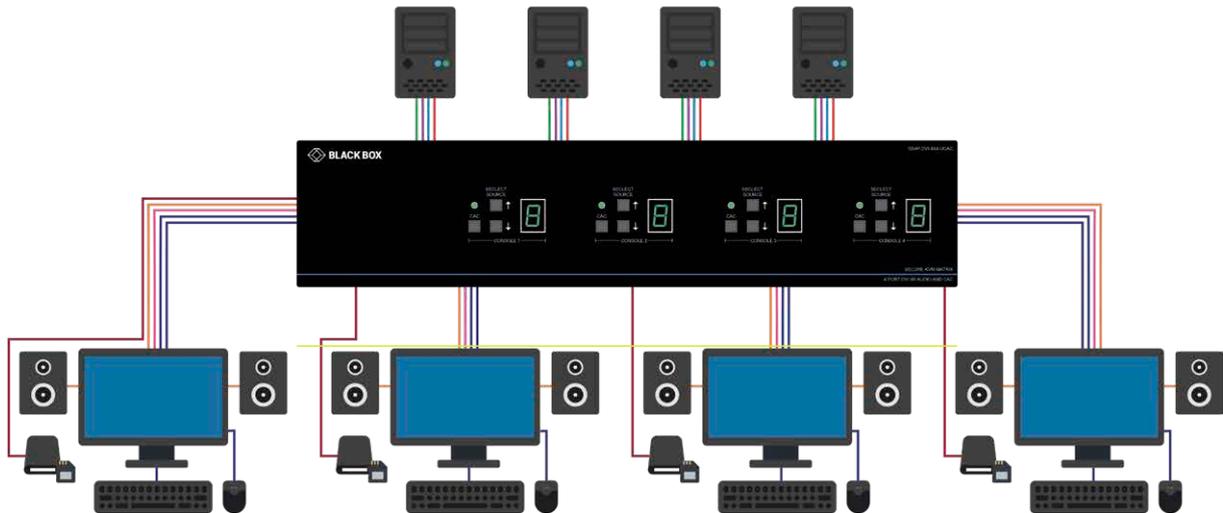


**i** Find the right product in the selector on page 11

# SECURE KVM PRODUCT OVERVIEW

## DVI-I SECURE KVM MATRIX SWITCHES, MULTI-USER

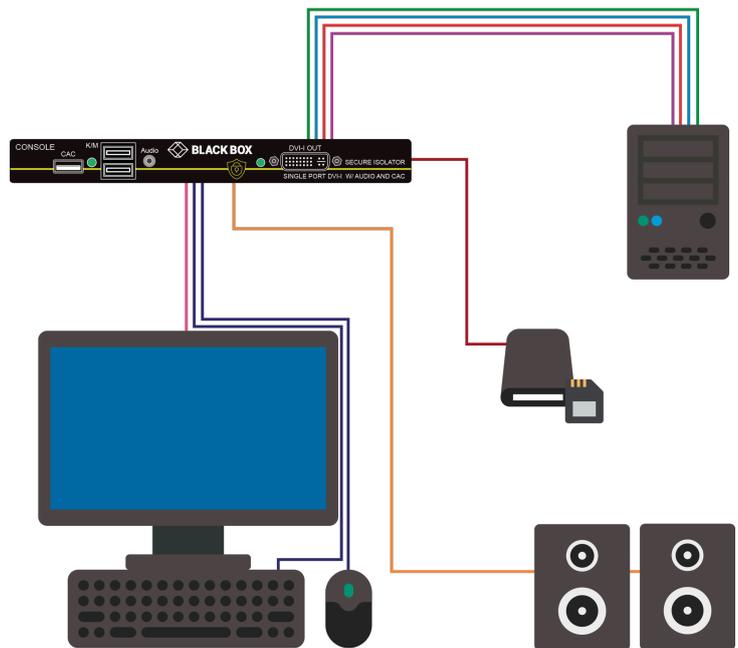
- Access for two or four users to four or eight computers
- DVI-I video supporting single-link DVI, dual-link DVI and VGA up to 2560 x1600
- USB keyboard/mouse plus stereo audio
- CAC support for smart card readers and special peripheral assignment
- Support most monitors through Secure EDID Learning/Emulation
- Windows, Mac and Linux OS compatible
- NIAP 3.0 certified



**i** 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
- Ensure unidirectional data flow of video, USB and audio from the computer to the peripheral
- Supports DVI-I video, USB and audio
- Support most monitors through Secure EDID Learning/Emulation
- Stereo audio support
- Windows, Mac and Linux OS compatible
- CAC support
- NIAP 3.0 certified



**i** 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 @ 30 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 @ 30 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							
<b>PORTS TO USER CONSOLE:</b>								
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 models only)	1x USB Type A, fully configurable							
<b>PORTS TO COMPUTERS:</b>								
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							

	<b>MULTIVIEWER NIAP, NIAP 3.0 CERTIFIED</b>	<b>PERIPHERAL PROTECTOR NIAP 3.0</b>
		
ITEM #	SS4P-SH-DVI-UCAC-P	SS1P-DVI-UCAC-P
Description	4-Port Secure KVM Switch, DVI-I with 4-in-1 multiview	1-Port Secure Peripheral Protector
# of sources (max.)	4	1 peripherhal
Monitor Connections per console	2	N/A
Max. Resolution	2560 x 1600 @ 60 Hz	2560 x 1600 @ 60 Hz
<b>PORTS TO USER CONSOLE:</b>		<b>PERIPHERAL PORTS:</b>
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	x 3.5mm audio jack
CAC Support	1x config. USB Type A	1x config. USB Type A
<b>PORTS TO COMPUTERS:</b>		
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	SS4P-KM-U/ SS4P-KM-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	Computers with Windows, Mac and Linux OS				Windows, Mac and Linux OS	
No 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 00800-2255 2269 or  
visit [WWW.BLACK-BOX.EU/TSC](http://WWW.BLACK-BOX.EU/TSC).



## 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, every day of the year.

### WARRANTIES

Secure KVM Switches come with a 3-Year warranty and extension options are available.

### FINANCIAL STRENGTH

Nearly \$1 billion in annual revenue; publically traded (BBOX).

### EXPERIENCE

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

### CENTRE OF EXCELLENCE

Black Box offers a Centre of Excellence featuring professional services and support agreements that help optimise customers' systems and maximise uptime.

### SERVICE LEVEL AGREEMENTS

Our Service Level Agreements give customers access to technical support, product training, dedicated application engineers and more.