Adder AVSC1104-US 4 Port VGA/USB Secure KVM Switch with Card Reader

This listing is for AVSC1104 (4 Port) Switch only. Use description below as a general reference.

The ADDERView® Analogue Enhanced SecureSwitch allows a keyboard, monitor and mouse to be shared between high and low security systems, “red and black networks” together with secure smartcard reader sharing. The high density, highly robust, small form factor unit ensures maximized security to prevent the compromise of critical data.

- **Secured Channel Switching**: device can only be directly controlled, not via peripherals
- **Security of Data**: unidirectional flow of data and controlled memory limits access to information
- **Tamper Proof Design**: physical casing and circuitry minimize risk of unauthorized access
- **Industry Recognized**: designed to meet Common Criteria; EAL4+ certified
- **Secure Smartcard reader sharing**: between the connected systems

Features

- **TEMPEST qualified and EAL4+ certified:** Tempest certified design (USA NSTISSAM Level I and NATO SDIP-27 Level A), EAL4+ Common Criteria Evaluation Assurance Level 4 (augmented by ALC_ FLR.2 and ATE_DPT.2)
- **Physical port identification:** Channel switching is controlled only from the front panel buttons. No keyboard or mouse switching commands are permitted. Two port and four port sizes are available as standard or enhanced <hyperlink to enhanced page> versions.
- **Smartcard Reader Sharing:** The ADDERView SecureSwitch Analogue Enhanced product allows you to attach a smartcard reader that can be securely shared between the connected systems. This variant also contains anti-subversion features to guard against intrusion as well as authentication to verify that the unit is genuine.
- **Hardwired port isolation:** Data Diodes implemented within hard-wired electronic circuitry ensure unidirectional flow of critical data paths, safeguarding any compromised peripheral by preventing reading of information or transfer of data by another system. Peripherals are always powered down and re-initialized in the event of a change of channel, providing an additional of protection against hidden peripheral malware.
- **No critical software reliance:** Minimized use of software within the unit avoids the possibility of subversive reprogramming. One-time programmable storage replaces flash memory in all security critical areas of the device
- **Designed for minimal emissions and isolation of electrical crosstalk:** Electromagnetic emissions are reduced and transmission of signals to other computers are prevented due to extensive shielding of the outer casing and of internal circuitry. External probing and unauthorized internal access are prevented through the unit design, with as few apertures as possible.