Australian Government
Department of Defence
Intelligence, Security and International Policy

DSD'S CONSUMER GUIDE

AVOCENT SWITCHVIEW SC4-UAD KEYBOARD/VIDEO/MOUSE SWITCH

Product Description

The Avocent SwitchView SC4-UAD is a keyboard/video/mouse (KVM) switch designed to connect a single set of human interface devices to up to four computers in multiple security domains. Users can operate on secure and insecure networks using a single set of peripherals without the risk of data from the secure networks transferring to the insecure networks. The unique architecture of the switch isolates and secures the data of each connected network at all times. The device implements DVI and USB connections.

Evaluation Scope and Summary

The scope of the evaluation included all functionality of the Avocent SwitchView SC4-UAD KVM Switch.

The product has been mutually recognised to meet the requirements of a High Grade (HG) product and has been given a High Grade Assurance Level.

DSD's Cryptographic Evaluation

Since there was no cryptography within scope of the evaluation, DSD did not conduct a cryptographic evaluation.

Condition of Use

For Australian Government users, the following conditions must be adhered to for use between Top Secret or Secret and Unclassified computer systems.

- The Avocent SC4-UAD can be used with digital or analogue video signals.
- The microphone and speaker functionality of the Avocent SC4-UAD may be used.
- Do not connect a KVM switch to another KVM switch.
- Do not use wireless peripherals or wireless capabilities in any of the computers.
- It is recommended that, as per ACSI33, agencies using the Avocent SC4-UAD should place uniquely numbered SCEC endorsed tamper seals on the device in addition to the Avocent seals.
- The KVM must be housed in a facility accredited to process data to at least the level of the highest classified system connected to the KVM. For example, if a system classified as Top Secret is connected to the KVM, the surrounding facility must be accredited to be able to process Top Secret data.

DSD's Recommendations

For Australian Government users it is recommended that the KVM be configured as per the Target of Evaluation (TOE) for this certification. In addition, DSD makes the following recommendations.

- Users should select different passwords for each system attached to the KVM.
- When switching between systems, the system not being used should be locked.
- Where possible, label the system classifications on attached systems.

For additional information regarding KVM usage for national security classifications, refer to blocks 3.10.56-57 of the SECURITY-IN-CONFIDENCE release of ACSI 33.

Point of Contact

For further information regarding the certification of these products or compliance with ACSI 33, please contact DSD on (02) 6265 0197 or email assist@dsd.gov.au.

ACSI 33

The advice given in this document is in accordance with ACSI 33 release date September 2007. Australian Government agencies are reminded to check the latest release of ACSI 33 at www.dsd.gov.au/library/infosec/acsi33.html.

Date of this Consumer Guide

This Consumer Guide was issued by DSD on 27 October 2008.