

**National Information Assurance Partnership**  
**Common Criteria Evaluation and Validation Scheme**



**Validation Report**

**for**

**ATEN Secure KVM Switch Series (Non-CAC Models)**

**Report Number:** CCEVS-VR-VID11222-2022

**Dated:** March 10, 2022

**Version:** 1.0

National Institute of Standards and Technology  
Information Technology Laboratory  
100 Bureau Drive  
Gaithersburg, MD 20899

Department of Defense  
Attn: NIAP, Suite 6982  
9800 Savage Road  
Fort Meade, MD 20755-6982

VALIDATION REPORT  
ATEN Secure KVM Switch Series (Non-CAC Models)

**ACKNOWLEDGEMENTS**

**Validation Team**

Patrick Mallett, PhD  
Daniel Faigin  
*The Aerospace Corporation*

**Common Criteria Testing Laboratory**

Leidos  
Columbia, MD

## Table of Contents

1	Executive Summary .....	1
2	Identification .....	5
2.1	Threats.....	6
2.2	Organizational Security Policies.....	7
3	Architectural Information .....	8
4	Assumptions.....	12
4.1	Clarification of Scope .....	13
5	Security Policy .....	14
5.1	Security Audit .....	15
5.2	User Data Protection.....	16
5.3	Identification and Authentication .....	17
5.4	Security Management .....	18
5.5	Protection of the TSF.....	19
5.6	TOE Access .....	20
6	Documentation.....	21
7	Independent Testing.....	22
7.1	Evaluation team independent testing .....	23
7.2	Vulnerability Survey.....	24
8	Evaluated Configuration .....	25
9	Results of the Evaluation .....	26
10	Validator Comments/Recommendations .....	27
11	Annexes.....	28
12	Security Target.....	29
13	Abbreviations and Acronyms .....	30
14	Bibliography .....	32

## List of Figures

Figure 1	Simplified block diagram of a 2-Port KVM TOE.....	10
----------	---	----

VALIDATION REPORT  
ATEN Secure KVM Switch Series (Non-CAC Models)

VALIDATION REPORT  
ATEN Secure KVM Switch Series (Non-CAC Models)

## List of Tables

Table 1: ATEN Secure KVM Switch Series TOE Models.....	2
Table 2: Evaluation Details.....	4
Table 3: Security Target Identification.....	5
Table 4: ATEN Secure KVM Switch Console Interfaces and TOE Models.....	9
Table 5: ATEN Secure KVM Switch Computer Interfaces and TOE Models.....	10
Table 6: TOE Security Assurance Requirements.....	26
Table 7: Security Target Identification.....	29

VALIDATION REPORT  
ATEN Secure KVM Switch Series (Non-CAC Models)

## 1 Executive Summary

This report is intended to assist the end-user of this product and any security certification agent for that end-user to determine the suitability of this Information Technology (IT) product in their environment. End-users should review the Security Target (ST) [6]1 (which is where specific security claims are made) as well as this Validation Report (VR) (which describes how those security claims were evaluated, tested, and any restrictions that may be imposed upon the evaluated configuration) to help in that determination. Prospective users should carefully read the Assumptions and Clarification of Scope in section 4 and the Validator Comments in section 10, where any restrictions on the evaluated configuration are highlighted.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the ATEN Secure KVM Switch Series (Non-CAC Models) of peripheral sharing switches. It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied. This VR applies only to the specific version and configuration of the product as evaluated and as documented in the ST.

The evaluation of the ATEN Secure KVM Switch Series (Non-CAC Models) of peripheral sharing switches was performed by Leidos Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, in the United States and was completed in March 2022. The evaluation was conducted in accordance with the requirements of the Common Criteria and Common Methodology for IT Security Evaluation (CEM), version 3.1, revision 5 [4] and the assurance activities specified in the following materials:

- *Protection Profile for Peripheral Sharing Device*, Version 4.0, 19 July 2019 (PP\_PSD\_V4.0) or [PSD]
  - including the following optional and selection-based SFRs: FAU\_GEN.1, FDP\_RIP\_EXT.2, FDP\_SWI\_EXT.2, FIA\_UAU.2, FIA\_UID.2, FMT\_MOF.1, FMT\_SMF.1, FMT\_SMR.1, FPT\_PHP.3, FPT\_STM.1, and FTA\_CIN\_EXT.1.
- *PP-Module for Analog Audio Output Devices*, Version 1.0, 19 July 2019 (MOD\_AO\_V1.0).
- *PP-Module for Keyboard/Mouse Devices*, Version 1.0, 19 July 2019 (MOD\_KM\_V1.0)
  - including the following optional and selection-based SFRs: FDP\_FIL\_EXT.1/KM, FDP\_RIP.1/KM, and FDP\_SWI\_EXT.3.
- *PP-Module for Video/Display Devices*, Version 1.0, 19 July 2019 (MOD\_VI\_V1.0)
  - including the following selection-based SFRs: FDP\_CDS\_EXT.1, FDP\_IPC\_EXT.1, FDP\_SPR\_EXT.1/DP(DP), FDP\_SPR\_EXT.1/DVI-I(D), and FDP\_SPR\_EXT.1/HDMI(H).

The following NIAP Technical Decisions are applicable to the claimed Protection Profile and Modules:

## VALIDATION REPORT

### ATEN Secure KVM Switch Series (Non-CAC Models)

- [TD0593](#) – Equivalency Arguments for PSD
- [TD0586](#) – DisplayPort and HDMI Interfaces in FDP\_IPC\_EXT.1
- [TD0585](#) – Update to FDP\_APC\_EXT.1 Audio Output Tests
- [TD0584](#) – Update to FDP APC\_EXT.1 Video Tests
- [TD0583](#) – FPT\_PHP.3 modified for PSD remote controllers
- [TD0557](#) – Correction to Audio Filtration Specification Table in FDP\_AFL\_EXT.1
- [TD0539](#) – Incorrect Selection Trigger in FTA\_CIN\_EXT.1 in MOD\_VI\_V1.0

The TOE does not fit the Combiner Use Case and so the specific assignment required by the VI Module does not apply.

- [TD0518](#) – Typographical Error in Dependency Table
- [TD0514](#) – Correction to MOD\_VI FDP\_APC\_EXT.1 Test 3 Step 6
- [TD0507](#) – Clarification on USB Plug Type
- [TD0506](#) – Missing Steps to Disconnect and Reconnect Display

The evaluation was consistent with NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on their web site ([www.niap-ccevs.org](http://www.niap-ccevs.org)).

The Leidos evaluation team determined that the ATEN Secure KVM Switch Series (Non-CAC Models) of peripheral sharing switches is conformant to the claimed Protection Profile (PP) and PP-Modules, and when installed, configured and operated as specified in the evaluated guidance documentation, satisfied all of the security functional requirements stated in the ST. The information in this VR is largely derived from the publicly available Evaluation Activities Report (AAR) [7] and the associated proprietary test report [8] produced by the Leidos evaluation team.

Each device in the ATEN Secure KVM Switch (Non-CAC Modules) series is a peripheral sharing switch that allows for securely sharing one set of peripherals between multiple computers. A user may connect a mouse, keyboard, speaker, and one or two video displays to a Secure KVM Switch. The user may switch the set of peripherals between connected computers. The maximum number of connected computers is two, four, or eight depending on model. The user can switch the peripherals between any of the connected computers while preventing unauthorized data flows or leakage between computers.

The TOE is the following models of the ATEN Secure KVM Switch Series. The firmware version for all models is v1.1.101

**Table 1: ATEN Secure KVM Switch Series TOE Models**

Configuration	2-Port	4-Port	8-Port
---------------	--------	--------	--------

VALIDATION REPORT

ATEN Secure KVM Switch Series (Non-CAC Models)

DisplayPort	Single Head	CS1182DP4	CS1184DP4	CS1188DP4
	Dual Head	CS1142DP4	CS1144DP4	CS1148DP4
HDMI	Single Head	CS1182H4	CS1184H4	N/A
	Dual Head	CS1142H4	CS1144H4	N/A
DVI	Single Head	CS1182D4	CS1184D4	CS1188D4
	Dual Head	CS1142D4	CS1144D4	CS1148D4

The TOE includes a wired remote controller: Remote Peripheral Selector (RPS) that is available to customers as an additional purchase. This device has the same firmware version as the models above.

In Table 1, DisplayPort and HDMI configurations support HDMI monitor peripherals. DVI configurations support DVI monitors. All TOE devices support USB keyboards and mice.

The validation team monitored the activities of the evaluation team, examined evaluation evidence, provided guidance on technical issues and evaluation processes, and reviewed the evaluation results produced by the evaluation team. The validation team found that the evaluation results showed that all assurance activities specified in the claimed PP had been completed successfully and that the product satisfied all of the security functional and assurance requirements as stated in the ST.

Therefore, the validation team concludes that the testing laboratory’s findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

The products, when configured as specified in the guidance documentation, satisfy all of the security functional requirements stated in the ATEN Secure KVM Switch Security Target.

Item	Identifier
<b>Evaluated Product</b>	ATEN Secure KVM Switches Series devices identified in Table 1
<b>Sponsor &amp; Developer</b>	ATEN 3F, No. 125, Section 2, Datung Road, Sijhih District, New Taipei City, 221 Taiwan



VALIDATION REPORT  
 ATEN Secure KVM Switch Series (Non-CAC Models)

<b>Item</b>	<b>Identifier</b>
<b>CCTL</b>	Leidos Common Criteria Testing Laboratory 6841 Benjamin Franklin Drive Columbia, MD 21046
<b>Completion Date</b>	March 2022
<b>CC</b>	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017
<b>Interpretations</b>	There were no applicable interpretations used for this evaluation.
<b>CEM</b>	Common Methodology for Information Technology Security Evaluation: Version 3.1, Revision 5, April 2017
<b>PP</b>	Protection Profile for Peripheral Sharing Switch, Version 4.0
<b>Disclaimer</b>	The information contained in this Validation Report is not an endorsement of the ATEN Secure KVM Switch Series by any agency of the U.S. Government and no warranty of the ATEN Secure KVM Switch Series is either expressed or implied.
<b>Evaluation Personnel</b>	Gregory Beaver Justin Fisher Allen Sant Sindhu Veerabhadru Madhav Nakar
<b>Validation Personnel</b>	Patrick Mallet, Lead Validator Daniel Faigin, Senior Validator

**Table 2: Evaluation Details**

## VALIDATION REPORT

### ATEN Secure KVM Switch Series (Non-CAC Models)

## 2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Product Compliant List (PCL) (<https://www.niap-ccevs.org/Product/>).

The following table identifies the evaluated Security Target and TOE.

Name	Description
<b>ST Title</b>	ATEN Secure KVM Switch Series (Non-CAC Models) Security Target
<b>ST Version</b>	v1.1
<b>Publication Date</b>	March 8, 2022
<b>Vendor and ST Author</b>	ATEN International Co., Ltd
<b>TOE Reference</b>	ATEN Secure KVM Switch Series identified in Table 1
<b>TOE Software Version</b>	Firmware version v1.1.101
<b>Keywords</b>	KVM Switch, Peripheral Sharing Switch

**Table 3: Security Target Identification**

## VALIDATION REPORT

### ATEN Secure KVM Switch Series (Non-CAC Models)

## 2.1 Threats

The ST identifies the following threats that the TOE and its operational environment are intended to counter the following threats.

- A connection via the PSD between one or more computers may allow unauthorized data flow through the PSD or its connected peripherals.
- A connection via the PSD between one or more computers may allow unauthorized data flow through bit-by-bit signaling.
- A PSD may leak (partial, residual, or echo) user data between the intended connected computer and another unintended connected computer.
- A PSD may connect the user to a computer other than the one to which the user intended to connect.
- The use of an unauthorized peripheral device with a specific PSD peripheral port may allow unauthorized data flows between connected devices or enable an attack on the PSD or its connected computers.
- An attached device (computer or peripheral) with malware, or otherwise under the control of a malicious user, could modify or overwrite code or data stored in the PSD's volatile or non-volatile memory to allow unauthorized information flows.
- A malicious user or human agent could physically modify the PSD to allow unauthorized information flows.
- A malicious human agent could replace the PSD during shipping, storage, or use with an alternate device that does not enforce the PSD security policies.
- Detectable failure of a PSD may cause an unauthorized information flow or weakening of PSD security functions.
- A malicious agent could use an unauthorized peripheral device such as a microphone, connected to the TOE audio out peripheral device interface to eavesdrop or transfer data across an air-gap through audio signaling.
- A malicious agent could repurpose an authorized audio output peripheral device by converting it to a low-gain microphone to eavesdrop on the surrounding audio or transfer data across an air-gap through audio signaling.

## VALIDATION REPORT

ATEN Secure KVM Switch Series (Non-CAC Models)

### **2.2 Organizational Security Policies**

There are no Organizational Security Policies for the *Protection Profile for Peripheral Sharing Switch* [5].

## VALIDATION REPORT

### ATEN Secure KVM Switch Series (Non-CAC Models)

## 3 Architectural Information

The ATEN Secure KVM Switch (Non-CAC Model) series are keyboard, video, mouse (KVM) switches with the following characteristics:

- 2/4/8 port USB DisplayPort single and dual display for DisplayPort (6 devices)
- 2/4 port USB HDMI single and dual display for HDMI (4 devices)
- 2/4/8 port USB DVI single and dual display for DVI (6 devices).

The Secure KVM Switch products allow for the connection of a mouse, keyboard, speaker, and one or two video displays (depending on specific device type) to the Secure KVM Switch, which is then connected to 2, up to 4, or up to 8 separate computers (again depending on specific device type). The user can then switch the connected peripherals between any of the connected computers using a push button on the front of the device or on the RPS. The selected device is always identifiable by a bright orange LED associated with the applicable selection button.

To interface with connected computers, the Secure KVM Switch products support analog audio output and USB connections for the keyboard, and mouse. Depending on model, they support DisplayPort, DVI-I, or HDMI for the computer video display interface. The switched peripherals on the console side are analog audio output, USB keyboard and mouse, and DisplayPort, HDMI or DVI-I video output (depending on model).

Separate USB cables are used to connect the keyboard/mouse combination to the connected computers. The Secure KVM Switch products supporting DisplayPort convert the DisplayPort video signal to HDMI. The HDMI signal inside the KVM will be converted again to DisplayPort signal for output to the connected video display(s) and the AUX channel is monitored and converted to EDID. The Secure KVM Switch products also support audio output connections from the computers to a connected audio output device. Only speaker connections are supported and the use of an analog microphone or line-in audio device is prohibited. The tables below identify the interfaces of the Secure KVM console and computer ports according to model number.

Model No.	Console Video Output Interface			Console Keyboard	Console Mouse	Console Audio output
	DisplayPort	HDMI	DVI-I	USB 1.1/2.0	USB 1.1/2.0	3.5mm Analog Audio output (Speaker)
CS1182DP4	•			•	•	•
CS1142DP4	•			•	•	•
CS1182H4		•		•	•	•
CS1142H4		•		•	•	•
CS1182D4			•	•	•	•
CS1142D4			•	•	•	•

VALIDATION REPORT

ATEN Secure KVM Switch Series (Non-CAC Models)

Model No.	Console Video Output Interface			Console Keyboard	Console Mouse	Console Audio output
	DisplayPort	HDMI	DVI-I	USB 1.1/2.0	USB 1.1/2.0	3.5mm Analog Audio output (Speaker)
CS1184DP4	•			•	•	•
CS1144DP4	•			•	•	•
CS1184H4		•		•	•	•
CS1144H4		•		•	•	•
CS1184D4			•	•	•	•
CS1144D4			•	•	•	•
CS1188DP4	•			•	•	•
CS1148DP4	•			•	•	•
CS1188D4			•	•	•	•
CS1148D4			•	•	•	•

**Table 4: ATEN Secure KVM Switch Console Interfaces and TOE Models**

Model No.	Computer Video Input Interface			Computer Keyboard / Mouse	Computer Audio Input
	DisplayPort	HDMI	DVI-I	USB 1.1/2.0	3.5mm Analog Audio Input (Speaker)
CS1182DP4	•			•	•
CS1142DP4	•			•	•
CS1182H4		•		•	•
CS1142H4		•		•	•
CS1182D4			•	•	•
CS1142D4			•	•	•
CS1184DP4	•			•	•
CS1144DP4	•			•	•
CS1184H4		•		•	•
CS1144H4		•		•	•
CS1184D4			•	•	•
CS1144D4			•	•	•
CS1188DP4	•			•	•
CS1148DP4	•			•	•

VALIDATION REPORT

ATEN Secure KVM Switch Series (Non-CAC Models)

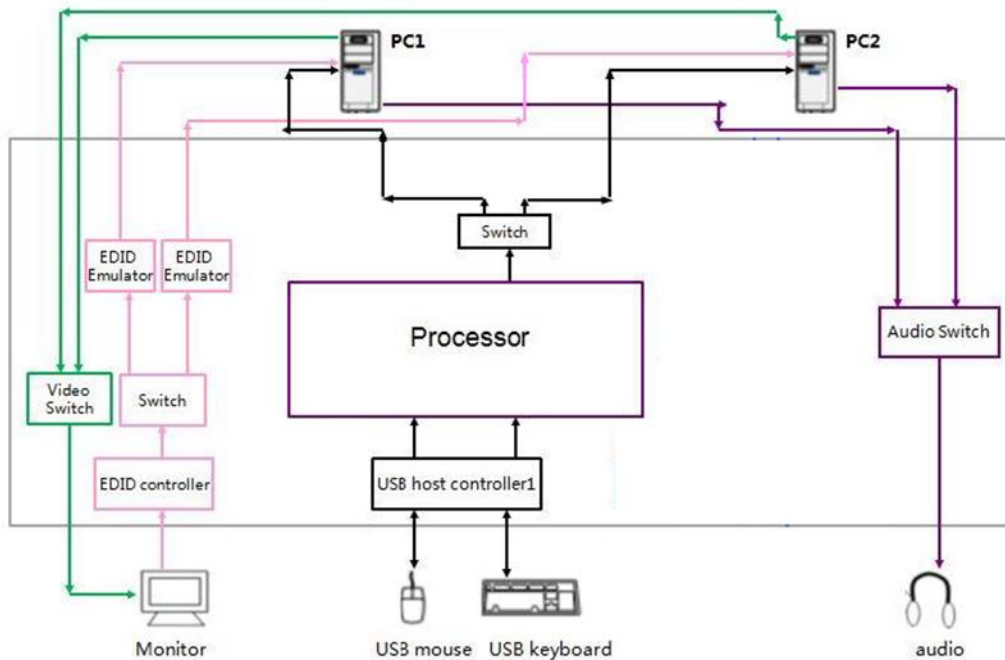
Model No.	Computer Video Input Interface			Computer Keyboard / Mouse	Computer Audio Input
	DisplayPort	HDMI	DVI-I	USB 1.1/2.0	3.5mm Analog Audio Input (Speaker)
CS1188D4			•	•	•
CS1148D4			•	•	•

**Table 5: ATEN Secure KVM Switch Computer Interfaces and TOE Models**

The ATEN Secure KVM products implement a secure isolation design for all models to share a single set of peripheral components. Each peripheral has its own dedicated data path. USB keyboard and mouse peripherals are filtered and emulated. DisplayPort video from the selected computer is converted internally to HDMI, then back to DisplayPort for communication with the connected video display and the AUX channel is monitored and converted to EDID.

The Secure KVM Switch products are designed to enforce the allowed and disallowed data flows between user peripheral devices and connected computers as specified in [PSD]. Data leakage is prevented across the TOE to avoid compromise of the user's information. The Secure KVM Switch products automatically clear the internal TOE keyboard and mouse buffers.

The following figure shows the data path design using a 2-Port KVM as an example.



**Figure 1 Simplified block diagram of a 2-Port KVM TOE**

The data flow of USB keyboard/mouse is controlled by the host controller for console HID keyboard and pointing devices. Details of the data flow architecture are provided in the

## VALIDATION REPORT

### ATEN Secure KVM Switch Series (Non-CAC Models)

proprietary Secure KVM Isolation Document. All keyboard and mouse connections are filtered first, and only authorized devices will be allowed. The TOE emulates data from authorized USB keyboard and mouse to USB data for computer sources.

The TOEs proprietary design ensures there is no possibility of data leakage from a user's peripheral output device to the input device; ensures that no unauthorized data flows from the monitor to a connected computer; and unidirectional buffers ensure that the audio data can travel only from the selected computer to the audio device. There is no possibility of data leakage between computers or from a peripheral device connected to a console port to a non-selected computer. Each connected computer has its own independent Device Controller, power circuit, and EEPROM. Additionally, keyboard and mouse are always switched together.

All Secure KVM Switch components including the RPS, feature hardware security mechanisms including tamper-evident labels, always active chassis-intrusion detection, and tamper-proof hardware construction, while software security includes restricted USB connectivity (non-Human Interface Devices (HIDs) are ignored when switching), an isolated channel per port that makes it impossible for data to be communicated between computers, and automatic clearing of the keyboard and mouse buffer.



## 4 Assumptions

The ST identifies the following assumptions about the use of the product:

- Computers and peripheral devices connected to the PSD are not TEMPEST approved.
- The environment provides physical security commensurate with the value of the TOE and the data it processes and contains.
- The environment includes no wireless peripheral devices.
- PSD Administrators and users are trusted to follow and apply all guidance in a trusted manner.
- Personnel configuring the PSD and its operational environment follow the applicable security configuration guidance.
- All PSD users are allowed to interact with all connected computers. It is not the role of the PSD to prevent or otherwise control user access to connected computers. Computers or their connected network shall have the required means to authenticate the user and to control access to their various resources.
- Users are trained not to connect a microphone to the TOE audio output interface.
- The TSF may or may not isolate the ground of the keyboard and mouse computer interfaces (the USB ground). The Operational Environment is assumed not to support TEMPEST red-black ground isolation.
- The computers connected to the TOE are not equipped with special analog data collection cards or peripherals such as analog to digital interface, high performance audio interface, digital signal processing function, or analog video capture function.

## VALIDATION REPORT

ATEN Secure KVM Switch Series (Non-CAC Models)

### 4.1 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarification. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

1. As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance (the assurance activities specified in the claimed PPs and performed by the evaluation team).
2. This evaluation covers only the specific hardware products, and firmware versions identified in this document, and not any earlier or later versions released or in process.
3. The evaluation of security functionality of the product was limited to the functionality specified in the claimed PPs. Any additional security related functional capabilities of the product were not covered by this evaluation. Any additional non-security related functional capabilities of the product, even those described in the ST, were not covered by this evaluation.
4. This evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not “obvious” or vulnerabilities to objectives not claimed in the ST. The CEM [4] defines an “obvious” vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication, and resources.

## VALIDATION REPORT

ATEN Secure KVM Switch Series (Non-CAC Models)

### **5 Security Policy**

ATEN Secure KVM Switch series devices enforce the following TOE security functional policies as specified in the ST.

## VALIDATION REPORT

ATEN Secure KVM Switch Series (Non-CAC Models)

### **5.1 Security Audit**

The TOE generates audit records for the authorized administrator actions. Each audit record records a standard set of information such as date and time of the event, type of event, and the outcome (success or failure) of the event.

## VALIDATION REPORT

ATEN Secure KVM Switch Series (Non-CAC Models)

### **5.2 User Data Protection**

The TOE controls and isolates information flowing between the peripheral device interfaces and a computer interface. The peripheral devices supported include USB keyboard; USB mouse; audio output; and (depending on device type) DisplayPort, DVI-I, or HDMI video. Some TOE models accept DisplayPort signals at the computer interface and internally convert the signals to HDMI signals and then convert back to DisplayPort for output to the console interface.

The TOE authorizes peripheral device connections with the TOE console ports based on the peripheral device type.

The TOE ensures that any previous information content of a resource is made unavailable upon the deallocation of the resource from a TOE computer interface immediately after the TOE switches to another selected computer and on start-up of the TOE.

The TOE provides a Reset to Factory Default function allowing authenticated authorized Administrators to remove all settings previously configured by the Administrator (such as USB device whitelist/blacklist). Once the Reset to Factory Default function has been completed, the Secure KVM will terminate the Administrator Logon mode, purge keyboard/mouse buffer, and power cycle the Secure KVM automatically.

## VALIDATION REPORT

ATEN Secure KVM Switch Series (Non-CAC Models)

### **5.3 Identification and Authentication**

The TOE provides an identification and authentication function for the administrative user to perform administrative functions such as configuring the keyboard/mouse device filtering blacklist. The authorized administrator must logon by providing a valid password.

## VALIDATION REPORT

ATEN Secure KVM Switch Series (Non-CAC Models)

### **5.4 Security Management**

The management functions are restricted to the authorized administrator and allow the TOE to be configured to reject specific USB keyboard/mouse devices using CDF blacklist parameters. Additionally, the TOE provides security management functions to Reset to Factory Default and to change the administrator password.

## VALIDATION REPORT

ATEN Secure KVM Switch Series (Non-CAC Models)

### **5.5 Protection of the TSF**

The TOE runs a suite of self-tests during initial startup and after activating the reset button that includes a test of the basic TOE hardware and firmware integrity; a test of the basic computer-to-computer isolation; and a test of critical security functions (i.e., user control and anti-tampering). The TOE provides users with the capability to verify the integrity of the TSF and the TSF functionality.

The TOE resists physical attacks on the main TOE enclosure as well as the RPS enclosure for the purpose of gaining access to the internal components or to damage the anti-tampering battery by becoming permanently disabled. The TOE preserves a secure state by disabling the TOE when there is a failure of the power on self-test, or a failure of the anti-tampering function.

The TOE provides unambiguous detection of physical tampering that might compromise the TSF. The TSF provides the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.



## VALIDATION REPORT

ATEN Secure KVM Switch Series (Non-CAC Models)

### **5.6 TOE Access**

The TOE displays a continuous visual indication of the computer to which the user is currently connected, including on power up, and on reset.

## VALIDATION REPORT

ATEN Secure KVM Switch Series (Non-CAC Models)

### 6 Documentation

The guidance documentation examined during the course of the evaluation and delivered with the TOE is as follows:

- ATEN PSD PP v4.0 Secure KVM Switch Series 2/4/8-Port USB DVI/HDMI/DisplayPort Single/Dual Display PP v4.0 Secure KVM Switch Administrator Guide, Version 1.03, 2021-1-25
- ATEN PSD PP v4.0 Secure KVM Switch Series 2/4/8-Port USB DVI/HDMI/DisplayPort Single/Dual Display PP v4.0 Secure KVM Switch User Manual, Version 1.03, 2021-1-25
- ATEN PSD PP v4.0 Secure KVM Switch Series 2/4/8-Port USB DVI/HDMI/DisplayPort Single/Dual Display PP v4.0 Secure KVM Switch Admin Log Audit Code, Version 1.03, 2021-1-25

TOE Documentation:

PP4.0 Secure KVM Isolation Document, Version 1.1 (Proprietary)

- **Note:** The PP4.0 Secure KVM Isolation Document is **proprietary** as permitted by PSD 4.0 Annex D.1 Isolation Document and Assessment.

The isolation document supplements the security target Section 6 TOE Summary Specification in order to demonstrate the TOE provides isolation between connected computers. In particular, the isolation document describes how the TOE mitigates the risk of each unauthorized data flow listed in PSD 4.0 Annex D and Evaluation Activities specified in the PP v4.0 and modules.

## **7 Independent Testing**

## VALIDATION REPORT

ATEN Secure KVM Switch Series (Non-CAC Models)

### 7.1 Evaluation team independent testing

This section describes the testing efforts of the evaluation team. It is derived from information contained in the following proprietary document:

- *ATEN PSD PP 4.0 Common Criteria Test Report and Procedures* Version 1.2, March 8, 2022, [8]

A non-proprietary summary of the test configuration, test tools, and tests performed may be found in:

- *Assurance Activities Report for ATEN Secure KVM Switch Series (Non-CAC Models), Version 1.2, March 8, 2022, [7]*

The purpose of the testing activity was to confirm the TOE behaves in accordance with the TOE security functional requirements as specified in the ST for a product claiming conformance to *Protection Profile for Peripheral Sharing Switch* [5].

The evaluation team devised a Test Plan based on the Testing Assurance Activities specified in *Protection Profile for Peripheral Sharing Switch* [5]. The Test Plan described how each test activity was to be instantiated within the TOE test environment. The evaluation team executed the tests specified in the Test Plan and documented the results in the team test report listed above.

Independent testing took place at the Leidos facility in Columbia, Maryland from August 29, 2021 to March 8, 2022.

The evaluators received the TOE in the form that normal customers would receive it, installed and configured the TOE in accordance with the provided guidance, and exercised the Team Test Plan on equipment configured in the testing laboratory.

Given the complete set of test results from the test procedures exercised by the evaluators, the testing requirements for *Protection Profile for Peripheral Sharing Switch* [5] were fulfilled.

## VALIDATION REPORT

### ATEN Secure KVM Switch Series (Non-CAC Models)

## 7.2 Vulnerability Survey

A search of public domain sources for potential vulnerabilities in the TOE did not reveal any known vulnerabilities. The database searched was National Vulnerability Database (<https://nvd.nist.gov/>). The Table below lists the search terms and the type of search. The final search was conducted on March 8, 2022.

Search Term	Search Type	Rationale
aten	Advanced: Vendor	TOE vendor
belkin	Advanced: Vendor	Comparable vendor
black box	Advanced: Vendor	Comparable vendor
blackbox	Advanced: Vendor	Comparable vendor
iogear	Advanced: Vendor	Comparable vendor
ipgard	Advanced: Vendor	Comparable vendor
kvm	Basic: Keyword	General type
kvm switch	Basic: Keyword	TOE type
peripheral switch	Basic: Keyword	TOE type
Raritan	Advanced: Vendor	Comparable vendor
Smartavi	Advanced: Vendor	Comparable vendor
Triplite	Advanced: Vendor	Comparable vendor
Sekuryx	Advanced: Vendor	Comparable vendor

While some results were returned, no results applied to the specific TOE models or to the technology used by the TOE (for example, “kvm” returns results for the Linux Kernel-based Virtual Machine technology which is not applicable to the TOE).

In the absence of public vulnerabilities, the evaluation team determined that the test assurance activities prescribed by the claimed PP, specifically related to unintended switching, connectivity of unauthorized peripherals, attempts to reverse audio signal, and attempts to breach the physical boundary of the TOE demonstrate sufficient resilience of the TOE to an attacker of Basic attack potential.

## VALIDATION REPORT

ATEN Secure KVM Switch Series (Non-CAC Models)

### **8 Evaluated Configuration**

The evaluated version of the TOE consists of the ATEN Secure KVM Switch series devices identified in Table 1.

The TOE must be deployed as described in section 4 Assumptions of this document and be configured in accordance with the documentation identified in Section 6.

## VALIDATION REPORT

ATEN Secure KVM Switch Series (Non-CAC Models)

### 9 Results of the Evaluation

The evaluation was conducted based upon the assurance activities specified in *Protection Profile for Peripheral Sharing Switch* [5] in conjunction with version 3.1 revision 4 of the CC and the CEM ([1], [2], [3] and [4]). A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements.

The validation team's assessment of the evidence provided by the evaluation team is that the evidence demonstrates the evaluation team performed the assurance activities in the claimed PPs, and correctly verified that the product meets the claims in the ST.

The details of the evaluation are recorded in the Evaluation Technical Report (ETR) [9], which is controlled by the Leidos CCTL. The security assurance requirements are listed in the following table.

**Table 6: TOE Security Assurance Requirements**

<b>Assurance Component ID</b>	<b>Assurance Component Name</b>
ADV_FSP.1	Basic function specification
AGD_OPE.1	Operational user guidance
AGD_PRE.1	Preparative procedures
ALC_CMC.1	Labeling of the TOE
ALC_CMS.1	TOE CM coverage
ATE_IND.1	Independent testing – conformance
AVA_VAN.1	Vulnerability survey

## 10 Validator Comments/Recommendations

NIAP established a Peripheral Sharing Switch Technical Rapid Response Team (PSS-TRRT) to address questions and concerns related to evaluations claiming conformance to *Protection Profile for Peripheral Sharing Switch*. A Technical Decision is an issue resolution statement that clarifies or interprets protection profile requirements and assurance activities

The following NIAP Technical Decisions are applicable to the claimed Protection Profile and Modules:

- [TD0593](#) – Equivalency Arguments for PSD
- [TD0586](#) – DisplayPort and HDMI Interfaces in FDP\_IPC\_EXT.1
- [TD0585](#) – Update to FDP\_APC\_EXT.1 Audio Output Tests
- [TD0584](#) – Update to FDP APC\_EXT.1 Video Tests
- [TD0583](#) – FPT\_PHP.3 modified for PSD remote controllers
- [TD0557](#) – Correction to Audio Filtration Specification Table in FDP\_AFL\_EXT.1
- [TD0539](#) – Incorrect Selection Trigger in FTA\_CIN\_EXT.1 in MOD\_VI\_V1.0



VALIDATION REPORT  
ATEN Secure KVM Switch Series (Non-CAC Models)

## **11 Annexes**

Not applicable.

VALIDATION REPORT  
ATEN Secure KVM Switch Series (Non-CAC Models)

## 12 Security Target

**Table 7: Security Target Identification**

<b>Name</b>	<b>Description</b>
<b>ST Title</b>	ATEN Secure KVM Switch Series (Non-CAC Models)
<b>ST Version</b>	v1.1
<b>Publication Date</b>	March 8, 2022

## 13 Abbreviations and Acronyms

AAR	Assurance Activity Report
AUX	Auxiliary (Channel)
CAC	Common Access Card
CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Criteria Test Lab
CDF	Configurable Device Filtration
CEM	Common Evaluation Methodology
DP	DisplayPort
DVI	Digital Visual Interface
EEPROM	Electrically Erasable Programmable Read-Only Memory
ETR	Evaluation Technical Report
HDMI	High Definition Multimedia Interface
HID	Human Interface Device
IT	Information Technology
KVM	Keyboard, Video and Mouse
LED	Light-Emitting Diode
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Assessment Program
PC	Personal Computer
PCL	Product Compliant List
PP	Protection Profile
PSS	Peripheral Sharing Switch
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
USB	Universal Serial Bus

VALIDATION REPORT  
ATEN Secure KVM Switch Series (Non-CAC Models)

VR      Validation Report

VALIDATION REPORT  
ATEN Secure KVM Switch Series (Non-CAC Models)

## 14 Bibliography

The Validation Team used the following documents to produce this Validation Report:

- [1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction, Version 3.1, Revision 5, April 2017.
- [2] Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 3.1 Revision 5, April 2017.
- [3] Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Components, Version 3.1 Revision 5, April 2017.
- [4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 5, April 2017.
- [5] Protection Profile for Peripheral Sharing Switch (PSS), Version 4.0, 19 July 2019 (PP\_PSD\_V4.0) or [PSD]
- [6] ATEN Secure KVM Switch Series (Non-CAC Models) Security Target, version 1.1, March 8, 2022
- [7] Assurance Activities Report for ATEN Secure KVM Switch Series (Non-CAC Models), Version 1.2, March 8, 2022
- [8] ATEN PSD PP 4.0 Common Criteria Test Report and Procedures, Version 1.2, March 8, 2022
- [9] Evaluation Technical Report for ATEN Secure KVM Switch (Non-CAC Models), Version 1.1, March 8, 2022
- [10] *PP-Module for Analog Audio Output Devices*, Version 1.0, 19 July 2019 (MOD\_AO\_V1.0).
- [11] *PP-Module for Keyboard/Mouse Devices*, Version 1.0, 19 July 2019 (MOD\_KM\_V1.0)
- [12] *PP-Module for Video/Display Devices*, Version 1.0, 19 July 2019 (MOD\_VI\_V1.0)