



Simply Better Connections

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

EMC Information

FEDERAL COMMUNICATIONS COMMISSION STATEMENT:

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at their own expense.

Achtung: Der Gebrauch dieses Geräts in Wohnumgebung kann Funkstörungen verursachen.

Warning: Operation of this equipment in a residential environment could cause radio interference

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- (1) this device may not cause harmful interference, and
- (2) this device must accept any interference received, including interference that may cause undesired operation.

KCC Statement

유선 제품용 / A 급 기기 (업무용 방송 통신 기기)
이 기기는 업무용 (A 급) 전자파적합기기로서 판매자 또는 사용자는 이
점을 주의하시기 바라며, 가정 외의 지역에서 사용하는 것을 목적으로
합니다.

RoHS

This product is RoHS compliant.



HDMI Trademark Statement

The terms HDMI, HDMI High-Definition Multimedia Interface, and the HDMI Logo are trademarks or registered trademarks of HDMI Licensing Administrator, Inc.



China RoHS

产品中有害物质的名称及含量

部件名称 Parts Name	有害物质					
	铅 (Pb)	汞 (Hg)	镉 (Cd)	六价铬 (Cr(VI))	多溴联苯 (PBB)	多溴二苯醚 (PBDE)
电缆线/电源 Cable/Adaptor	X	O	O	O	O	O
印刷电路部件 PCBA	X	O	O	O	O	O
塑料/其它部件 Plastic /Others parts	O	O	O	O	O	O
金属部件 Metal parts	X	O	O	O	O	O

本表格依据 SJ/T 11364 的规定编制。

O：表示该有害物质在该部件所有均质材料中的含量均在 GB/T26572 规定的限量要求以下

X：表示该有害物质至少在该部件的某一均质材料中的含量超出 GB/T26572 规定的限量要求

表中标有“X”的情况,是按照欧盟 RoHS 采用了容许的豁免指标。



在中国大陆销售的相应电子电器产品 (EEP) 都必须遵照中国大陆《电子电气产品有害物质限制使用标识要求》标准 (SJ/T11364) 贴上环保使用期限 (EPUP) 标签。该产品所采用的 EPUP 标签是基于中国大陆的《电子信息产品环保使用期限通则》标准。

User Information

Online Registration

Be sure to register your product at our online support center:

<https://eservice.aten.com/eServiceCx/Common/productRegister.do>

Telephone Support

For telephone support, call this number:

International	+886-2-8692-6959
China	+86-10-5255-0110
Japan	+81-3-5615-5811
Korea	+82-2-467-6789
North America	+1-888-999-ATEN ext 4988
United Kingdom	+44-8-4481-58923

User Notice

All information, documentation, and specifications contained in this manual are subject to change without prior notification by the manufacturer. The manufacturer makes no representations or warranties, either expressed or implied, with respect to the contents hereof and specifically disclaims any warranties as to merchantability or fitness for any particular purpose. Any of the manufacturer's software described in this manual is sold or licensed *as is*. Should the programs prove defective following their purchase, the buyer (and not the manufacturer, its distributor, or its dealer), assumes the entire cost of all necessary servicing, repair and any incidental or consequential damages resulting from any defect in the software.

The manufacturer of this system is not responsible for any radio and/or TV interference caused by unauthorized modifications to this device. It is the responsibility of the user to correct such interference.

The manufacturer is not responsible for any damage incurred in the operation of this system if the correct operational voltage setting was not selected prior to operation. PLEASE VERIFY THAT THE VOLTAGE SETTING IS CORRECT BEFORE USE.

*Please visit our website to download the most up to date version of the manual.

© Copyright 2011–2017 ATEN® International Co., Ltd.

Manual Version: v1.03

Manual Date: 2021-1-25

ATEN and the ATEN logo are registered trademarks of ATEN International Co., Ltd. All rights reserved.

All other brand names and trademarks are the registered property of their respective owners.

Contents

EMC Information	ii
China RoHS	iii
User Information	iv
Online Registration	iv
Telephone Support	iv
User Notice	iv
About the Administrator Guide	vii
Overview	viii
Conventions	ix
Product Information	ix
Chapter 1	1
Introduction	1
Overview.....	1
Administrative Functions.....	1
Chapter 2	2
Precautions and Preparation	2
Before You Begin	2
Chapter 3	5
Operation	5
Powering On	5
Manual Switching	6
LED Display	6
Chassis Intrusion Detection	8
Administrator Functions	8
Appendix	14
Safety Instructions	14
General.....	14
Consignes de Sécurité.....	16
Général.....	16
Technical Support.....	18
International	18
North America	18
Limited Warranty.....	19

ATTENTION

If the tamper-evident seal is missing or peeled, avoid using the product and contact your ATEN dealer.

If all front panel LEDs on the Secure KVM Switch (except Power) flash continuously, all Remote Port Selector (RPS) LEDs flash, or either enclosure appears breached, avoid using the product and contact your ATEN dealer.

The Secure KVM Switch and the Remote Port Selector (RPS) are equipped with active always-on chassis intrusion detection security. Any attempt to open the enclosure will permanently disable the switch/ RPS, and void the warranty.

To maximize security and to prevent unauthorized access to the Secure KVM Switch, please change the default password after your first successful log in.



About the Administrator Guide

This Administrator Guide is intended for authorized administrators only.

This Administrator Guide is provided to help authorized administrators audit logs and configure the ATEN Secure KVM switch. To maximize security, it is recommended that administrators audit log event records and the Secure KVM Switch configuration on a routine basis.

This Administrator Guide is applied to the following ATEN Secure KVM Switches

Configuration (with CAC function)			2-Port	4-Port	8-Port
PC Video Connection	Console Video Connection	No. of Displays			
DisplayPort	DisplayPort	Single	CS1182DP4C	CS1184DP4C	CS1188DP4C
		Dual	CS1142DP4C	CS1144DP4C	CS1148DP4C
HDMI	HDMI	Single	CS1182H4C	CS1184H4C	NA
		Dual	CS1142H4C	CS1144H4C	NA
DVI	DVI	Single	CS1182D4C	CS1184D4C	CS1188D4C
		Dual	CS1142D4C	CS1144D4C	CS1148D4C

Configuration (without CAC function)			2-Port	4-Port	8-Port
PC Video Connection	Console Video Connection	No. of Displays			
DisplayPort	DisplayPort	Single	CS1182DP4	CS1184DP4	CS1188DP4
		Dual	CS1142DP4	CS1144DP4	CS1148DP4
HDMI	HDMI	Single	CS1182H4	CS1184H4	NA
		Dual	CS1142H4	CS1144H4	NA
DVI	DVI	Single	CS1182D4	CS1184D4	CS1188D4
		Dual	CS1142D4	CS1144D4	CS1148D4

Overview

Chapter 1, Introduction, introduces you to the ATEN Secure KVM Switch system and administration function.


Chapter 2, Precautions and Preparation, provides step-by-step instructions for setting up your installation.

Chapter 3, Operation, explains the concepts involved in operating the ATEN Secure KVM Switch.

An Appendix, provides specifications and other technical information regarding the ATEN Secure KVM Switch.

Conventions

This manual uses the following conventions:

- | | |
|---|--|
| Monospaced | Indicates text that you should key in. |
| [] | Indicates keys you should press. For example, [Enter] means to press the Enter key. If keys need to be chorded, they appear together in the same bracket with a plus sign between them: [Ctrl+Alt]. |
| 1. | Numbered lists represent procedures with sequential steps. |
| ◆ | Bullet lists provide information, but do not involve sequential steps. |
| → | Indicates selecting the option (on a menu or dialog box, for example), that comes next. For example, Start → Run means to open the <i>Start</i> menu, and then select <i>Run</i> . |
|  | Indicates critical information. |

Product Information

For information about all ATEN products and how they can help you connect without limits, visit ATEN on the Web or contact an ATEN Authorized Reseller. Visit ATEN on the Web for a list of locations and telephone numbers:

International <https://www.aten.com/global/en/>

North America <https://www.aten.com/us/en/>

This Page Intentionally Left Blank

Chapter 1

Introduction

Overview

The ATEN Secure KVM Switch series is NIAP¹-certified and compliant with NIAP PPv4.0 (Protection Profile for Peripheral Sharing Device version 4.0)² requirements, satisfying the latest security requisites set by the U.S. Department of Defense for peripheral sharing devices. Compliance ensures maximum information security while sharing a single set of keyboard, mouse, monitor, speakers, and CAC (Common Access Card) Reader³ between multiple computers. Conformity with Protection Profile v4.0 certifies that other USB peripherals cannot be connected to the console ports of the Secure KVM Switch, and that only a keyboard and mouse are accommodated, therefore providing high-level security, protection and safekeeping of data.

The ATEN Secure KVM Switch hardware security includes tamper-evident tape, chassis intrusion detection, and tamper-proof hardware, while software security features include restricted USB connectivity – non-HIDs (Human Interface Devices) or non-predefined CAC/HIDs are ignored when switching, an isolated channel per port that makes it impossible for data to be transferred between secure and unsecure computers, and automatic clearing of the keyboard and mouse buffer when switching port focus.

By combining physical security with controlled USB connectivity and controlled unidirectional data flow from devices to connected computers only, the ATEN Secure KVM Switch series offers you the means to consolidate multiple workstations of various security classification levels with one keyboard, monitor and mouse (KVM) console.

Administrative Functions

To be compliant with Protection Profile v4.0 while providing higher deployment flexibility, wider product support for new authentication devices and maximum security, the ATEN Secure KVM Switch supports administrative functions. Through secured access, an authorized administrator can audit log data, configure the Secure KVM Switch, and configure device filtering.

Note:

1. The National Information Assurance Partnership (NIAP) is a United States government initiative to meet the security testing needs of IT consumers and manufacturers. It is operated by the National Security Agency (NSA) and the National Institute of Standards and Technology (NIST).
2. The ATEN Secure KVM Switch series additionally satisfies Protection Profile version 4.0 for Peripheral Sharing Device (PSD).
3. USB 1.1 for keyboard, mouse connections, and USB 2.0 for CAC reader connection.

Chapter 2

Precautions and Preparation

Before You Begin

If the tamper-evident seal is missing or peeled, avoid using the product and contact your ATEN dealer.

If all front panel LEDs on the Secure KVM Switch (except Power) flash continuously, all Remote Port Selector (RPS) LEDs flash, or either enclosure appears breached, avoid using the product and contact your ATEN dealer.

The Secure KVM Switch and the Remote Port Selector (RPS) are equipped with active always-on chassis intrusion detection security. Any attempt to open the enclosure will permanently disable the switch/ RPS, and void the warranty.

To maximize security and to prevent unauthorized access to the Secure KVM Switch, please change the default password after your first successful log in.

Tampering prevention and detection

1. The ATEN Secure KVM Switch and the optional Remote Port Selector (RPS) include tamper-evident tape to provide visual indications of intrusion to the switch/ RPS enclosure. If the tamper-evident seal is missing, peeled, or looks as if it has been adjusted, avoid using the product and contact your ATEN dealer.
2. The ATEN Secure KVM Switch and ATEN RPS are equipped with active always-on chassis intrusion detection:
 - If a mechanical intrusion is detected on the switch, the switch (without RPS connected) will be permanently disabled and all the front panel LEDs (except the Power LED) will flash continuously.
 - If a mechanical intrusion is detected by the RPS (connected with the switch and aligned), this will permanently disable both the RPS itself and the switch, and all LEDs (on RPS) and the front panel LEDs except the Power LED (on switch) will flash continuously.

If the switch or RPS enclosure appears breached or all the LEDs are flashing continuously, stop using it, remove it from service immediately and contact your ATEN dealer.
3. Any attempt to open the switch or RPS enclosure will activate the chassis intrusion detection security, which will render it inoperable and void the warranty.
4. The ATEN Secure KVM Switch cannot be upgraded, serviced or repaired.
5. The ATEN Secure KVM Switch and ATEN RPS contain an internal battery which is non-replaceable. Never attempt to replace the battery or open the switch or RPS enclosure.

Always use qualified and authorized peripheral devices

1. For security, the ATEN Secure KVM Switch supports only standard USB devices (or pointing device). Do not connect a wireless keyboard/mouse, or any keyboard/mouse with an internal USB hub or composite device with Non-HID functions to the switch.
2. If a non-qualified keyboard is connected, the keyboard will not function. No keystrokes will be seen on the screen.
3. If a non-qualified mouse is connected, the mouse will not function. No cursor movement will be seen on the screen.
4. For security, the USB console keyboard/mouse ports by default only support the following – standard USB keyboards/mice, standard USB keyboards/mice via a USB hub, and the HID functions of a composite device. Do not connect other USB devices to the USB console keyboard/mouse ports. Non-qualified or non-authorized USB devices will be rejected. For administrative configuration, please refer to the Administrator Guide.
5. Num Lock LED, Caps Lock LED, and Scroll Lock LED on the keyboard will be disabled due to the security policy.
6. Special multimedia keys on the keyboard will be disabled due to the security policy.
7. For security, the ATEN Secure KVM Switch does not support an analogue microphone or line-in audio input. Never connect a microphone or headset microphone to the audio output port. Standard analogue speakers and headsets are supported.
8. For security, the USB CAC port by default only supports authorized user authentication devices such as USB Smartcard or CAC readers. Do not connect other USB devices to the USB CAC port. Non-qualified or non-authorized USB devices will be rejected. For administrative configuration, please refer to the Administrator Guide and Port Authentication Utility Guide for details.
9. For security, do not use any USB CAC authentication device or other peripherals that adopt an external power source.
10. Always use a qualified monitor. Non-qualified monitors will be rejected.
11. Do not use wireless video transmitters or any docking device.
12. Do not connect any Thunderbolt device to the Secure KVM Switch.
13. Any cable connector or non-ATEN remote controller plugged into the console RPS port will be ignored.

Secure Installation

1. Do not attempt to connect or install the following devices to the computers connected to the ATEN Secure KVM Switch: TEMPEST computers; telecommunication equipment; frame grabber video cards; or special audio processing cards.
2. Important safety information regarding the placement of this device is provided on page 24. Please review it before proceeding.
3. Before installation, make sure the power sources to all devices connected to the installation are

turned off. You must unplug the power cords of any computers that have the Keyboard Power On function.

4. Hot-swapping of the console monitor is not allowed. Power off the Secure KVM Switch and the monitor before changing the console monitor.
5. A computer connected to the Secure KVM Switch should only be powered on after all of the connections to the device are made (video, USB and audio).
6. Please refer to the ATEN Secure KVM Switch user manual for hardware installation information.

Secure Administrative Operation

1. The ATEN Secure KVM Switches' administration functions (such as log data and configuration of the authenticated devices filter) can only be performed by an authorized administrator.
2. To maximize security and to prevent unauthorized access to the Secure KVM Switch, please change the default logon password after your first successful log in.
3. The Administrator's session will be terminated if the administrator logs out, or the Secure KVM Switch is powered off.
4. Please refer to the Operation section for details about the administrator functions.

Chapter 3

Operation

Powering On

When you power on, reset, or power cycle the ATEN Secure KVM Switch, the switch will perform a self-test to check the unit's integrity and security functions.

During the self-test

- All Port LEDs, all CAC LEDs (if supported), Num Lock LED, Caps Lock LED, and Scroll Lock LED on the Secure KVM will turn ON and then OFF.
- The KVM focus will be switched to Port 1 when the self-test completes successfully (Port 1 LED lights bright orange).

Self-test failure

In the case of a self-test failure, the Secure KVM Switch becomes inoperable, with front panel LED combinations (on the Secure KVM) indicating the potential cause of the failure (such as button jam or KVM integrity compromise)

- A pre-defined combination of port and CAC LEDs indicate the cause of the failure.
- If all front panel LEDs on the Secure KVM (except the Power LED) flash continuously, it means KVM tampering is detected or a self-test failure has occurred (except for Pushbutton jam; see below).
- If Pushbutton jam is detected, both the port's LEDs (Port LED and CAC LED) will flash.

For security, the ATEN Secure KVM Switch becomes inoperable if the self-test fails. Please verify your KVM installation by checking that the front panel pushbuttons are not stuck and then power cycle the Secure KVM Switch. If the self-test failure remains, stop using the ATEN Secure KVM Switch immediately, remove it from service and contact your ATEN dealer.

Reset the Secure KVM Switch (Reboot the Secure KVM switch)

Press the Reset button on the front panel to reset the ATEN Secure KVM Switch.

When you press the Reset button for more than 5 seconds, the keyboard/mouse buffer will be purged, the Secure KVM Switch will reboot and a self-test will initiate. After a successful self-test, the port focus will be switched to Port 1, and the CAC function of each port will be set back to the factory default setting (enabled). An administrator Reset KVM to Default function is also available (see page 13).

If the Secure KVM Switch fails to generate video on the console monitor after a reset, power off the Secure KVM Switch and all connected devices, check the cables, and follow the operational

instructions in user manual to power on the installation.

Manual Switching

For increased security, the ATEN Secure KVM Switch offers manual port switching only. Press and release a port selection pushbutton (on the switch, or on the RPS if connected and aligned) to bring the KVM focus to the computer attached to its corresponding port. To meet maximum security and channel isolation requirements, the keyboard, mouse, video, audio, and USB CAC reader ports will be switched together.

The PC that has the port focus should be able to detect the peripherals after port switching.

If the PC fails to detect your keyboard, mouse, or the CAC card reader:

- Verify that the keyboard, mouse, and/or CAC reader is qualified.
- Verify that the keyboard, mouse, or CAC reader hasn't failed.
- For USB CAC reader (USB authentication device), please make sure that the USB CAC cable has been securely connected, and the CAC function is enabled.
- For USB CAC reader port, please contact your administrator to verify if the device has been authorized.

LED Display

In addition to the Power LED, the ATEN Secure KVM Switch (and ATEN RPS) has Port LEDs (Online and Selected), keyboard lock (Num Lock/Caps Lock/Scroll Lock) LEDs and CAC LEDs that are built into the front panel to indicate port / keyboard / CAC reader operating status. A video LED is located on the back panel (of the switch) to indicate the operating status of the video connection. These LEDs also serve as the alarm notification for KVM security issues.

LED	Indication
Power LED (on the Secure KVM switch)	The Power LED is on the front panel and lights green to indicate that the KVM switch is powered on.
Video LED (on the Secure KVM switch)	The Video LED is located on the back panel next to each video connector. <input type="checkbox"/> The LED lights green when the video connection is up and running. <input type="checkbox"/> The LED flashes when a non-qualified monitor is connected.
Port LED (on the Secure KVM switch and the RPS)	The Port LEDs are located on the front panel (of the switch) and the upper-left side of each pushbutton (of the RPS) to indicate the port selection or connection status. <input type="checkbox"/> Online – Lights dim orange to indicate that the computer attached

	<p>to its corresponding port connected and powered on.</p> <ul style="list-style-type: none"> <input type="checkbox"/> Selected – Lights bright orange to indicate that the computer attached to its corresponding port has the KVM focus. <input type="checkbox"/> Warning - Flashes to indicate that a non-qualified USB HID device is connected to console USB keyboard port or mouse port when the corresponding port has the focus. <p>Note:</p> <ol style="list-style-type: none"> 1. Port and CAC LEDs will flash constantly when a chassis intrusion is detected. See Chassis Intrusion Detection section for details. 2. Port and CAC LEDs also indicate the status of the Secure KVM self-test status. See Operation section for further details.
<p>CAC LED (on the Secure KVM switch and the RPS) CAC models only</p>	<p>The CAC LEDs are located on the front panel (of the switch) and the far right of the upper bar on the panel (of the RPS) to indicate CAC reader selection or connection status.</p> <ul style="list-style-type: none"> <input type="checkbox"/> Online – Lights dim green to indicate that the computer attached to its corresponding port has a USB CAC reader cable connection and the CAC function is enabled. <input type="checkbox"/> Selected – Lights bright green to indicate that the CAC function is enabled and the computer attached to its corresponding port has the CAC focus. <input type="checkbox"/> None – No lights indicate that the cable is not connected or CAC has been disabled. <input type="checkbox"/> Warning - Flashes to indicate that a non-qualified USB Smart card / CAC reader is connected when the corresponding port has the focus. <p>Note:</p> <ul style="list-style-type: none"> - The CAC function of each port can be enabled or disabled by pressing the port selection button (on the switch) for more than 3 seconds (this is a toggle feature). Please refer to Operation section for details. - Port and CAC LEDs will flash constantly when a chassis intrusion is detected. See Chassis Intrusion Detection section for further details.
<p>Num Lock LED (on the Secure KVM switch and the RPS)</p>	<p>Lights green to indicate the Num Lock is enabled</p>
<p>Caps Lock LED (on the Secure KVM switch and the RPS)</p>	<p>Lights green to indicate the Caps Lock is enabled</p>
<p>Scroll Lock LED (on the Secure KVM switch and the RPS)</p>	<p>Lights green to indicate the Scroll Lock is enabled</p>

Chassis Intrusion Detection

To help prevent malicious tampering with the ATEN Secure KVM Switch, the switch (or the RPS) becomes inoperable and all front panel LEDs on the Secure KVM switch (except Power) or all Remote Port Selector (RPS) LEDs flash constantly when a chassis intrusion (such as the cover being removed) is detected (by the switch or by the RPS).

The intrusion detection protection is an always-on function. If all front panel LEDs on the Secure KVM Switch (except Power) flash continuously, all Remote Port Selector (RPS) LEDs flash, or either enclosure appears breached, avoid using the product and contact your ATEN dealer.

Administrator Functions

Administrator functions of the ATEN Secure KVM Switch enable authorized administrators to configure the switch, configure the user authenticated devices or HID device filters, and audit log data generated by the Secure KVM Switch.

- Log Data Audit:** This function enables authorized administrators to view log data and events generated by the Secure KVM Switch. The Log Data Audit function is enabled as soon as the Secure KVM Switch is manufactured. This capability cannot be terminated; it is not affected by KVM power-cycle, KVM Reset, or Reset KVM to Default.
- User Authentication Device and HID Device filtering configuration:** This function enables authorized administrators to assign a whitelist and blacklist for the user authenticated devices, and a blacklist for HID devices.
- Secure KVM Configuration:** This function enables authorized administrators to perform functions such as reset to factory default.

An administrator must first log in and be authenticated to use the Secure KVM Switch administrator functions. To maximize security, before performing other administrative functions, the administrator must set a new password after the first successful log in. The administrator password can be changed at anytime via the Administrator Configuration.

Setup for Administrator Logon

The administrator must log on and be authenticated for Secure KVM Switch administrative operations. This section helps you setup the installation for administrator logons.

1. Connect a qualified keyboard, mouse, and display to the Secure KVM Switches console section. (Please refer to the Secure KVM Switch user manual for details.)
2. Connect a source computer to Port 1 of the Secure KVM Switches' KVM port section via a KVM cable set. The USB cable that attaches to your computer's keyboard / mouse must be plugged into the KVM USB port on the switch. (Please refer to the Secure KVM Switch user manual for

details.)

3. Power on the ATEN Secure KVM Switch, and then power on the source computer. The ATEN Secure KVM Switch will switch to Port 1 after a successful self-test.

Administrator Logon

After setting up the switch, do the following to log in:

1. Open a text editor on the computer connected to Port 1.
2. Use the console keyboard to:
 - a. Press and hold down the [Ctrl] key.
 - b. Press and hold down the [F12] key:
 - c. First release the [F12] key, followed by the [Ctrl] key.
 - d. Press and release the [L] key, then press and release [Enter].

Please make sure not to exceed 2 seconds between each key. After a successful input of the key sequence above, you will be in Administrator Logon mode and will be prompted in text editor to be authenticated.

3. In the text editor, you will be prompted to input the default administrator password.

ATTENTION

- The default administrator password should only be used for the first-time the administrator logs in.
- To maximize security and to prevent unauthorized access to the Secure KVM Switch, change the default password after the first successful login. Once it's changed, the default administrator password will not be restored EVEN after a reset to factory default is initiated.

4. The default administrator password for the first-time log in is:

ABCD@xyz#2468!

- a. The password is case-sensitive.
 - b. The Caps Lock function is disabled in administrator logon mode. Use the [Shift] key for upper case letters and special characters.
5. A [Logon OK] message appears if the password is correct; you will be prompt to enter the password again if the password is incorrect.
 - a. With three failed attempts to log in, the administrator logon mode will be terminated and locked for 15 minutes.
 - b. With nine failed log in attempts, the Secure KVM Switch will become permanently inoperable.

Please remove it from service immediately and contact your ATEN dealer.

6. After a [Logon OK] message, type LIST and press [Enter] for a list of the administrator functions. (For a completed list of administrator functions, please access the eService section on the ATEN website. An “Admin log audit code” document is available for registered customers to download.)
7. For maximum security, the administrator must change the password after the first successful login. The new password must contain:
 - a. At least 8 characters, but no longer than 22 characters.
 - b. At least 1 lower case letter and,
 - c. At least 1 upper case letter and,
 - d. At least 1 numeric character and,
 - e. At least 1 special character.

Do not use the default administrator password for your new password.

The administrator will be asked to enter the new password a second time for confirmation.

Once the new administrator password is entered, the default administrator password will not be restored even after a Reset to Factory Default.

Log Data Audit

Log Data Audit is enabled when the Secure KVM Switch is manufactured and cannot be terminated.

After a successful administrator log in, type: LIST and press [Enter] for administrator functions.

Administrator Logon Mode

ID: Administrator

Please enter password: *****

Logon ok.

```
LIST
DATE-TIME= 25-12-2021_17:23:05_UTC
MFG_DATE= 23-12-2021
TAMP_TEST= PASS
HW_TEST= PASS
FW_TEST= PASS
KVM_BATT_TEST= 3.0V
```

KVM Information Area

```

RPS_BATT_TEST= 3.0V
RPS_TEST= PASS
FW_CHECKSUM= xxxx
AUDT_ST 23-12-2021_17:23:05_UTC
AUDT_SP NA
FW_VER= v1.1.101
TTL_LOGS= 8
    
```

KVM Information Area

No.	Cat.	DATE-TIME	Code	Crit
01	ADM	25-12-2021_17:23:05_UTC	ADIO	
02	CAC	25-12-2021_17:25:02_UTC	ADCWO	
03	CAC	25-12-2021_17:26:12_UTC	ADCBO	
04	ADM	25-12-2021_17:30:27_UTC	ADOO	

Log Data Area

Operation ok

1. KVM Information Area

This area displays the Secure KVM Switch status and critical information

- a. DATE-TIME: Current Date and Time (in UTC).
 - b. MFG_DATE: Manufacturing Date (in UTC) of the Secure KVM Switch.
 - c. TAMP_TEST: The Secure KVM Switch tamper protection test status.
 - d. HW_TEST: The Secure KVM Switch hardware self-test status.
 - e. FW_TEST: The Secure KVM Switch firmware self-test status.
 - f. KVM_BATT_TEST: The Secure KVM Switch battery self-test status. (The battery voltage will be displayed if the battery for Secure KVM switch is still working)
 - g. RPS_BATT_TEST: The Remote Port Selector battery self-test status. (The battery voltage will be displayed if the Remote Port Selector is connected and detected successfully)
 - h. RPS_TEST: The Secure KVM Switch Remote Port Selector connection self-test status. (“PASS” will be displayed if the Remote Port Selector is successfully detected and connected)
 - i. FW_CHECKSUM: The Secure KVM Switch firmware checksum for firmware integrity.
 - j. AUDT_ST: Date and Time (in UTC) when the Secure KVM Switch activates all protection mechanism and Log Data Audit function.
 - k. AUDT_SP: “NA” will be displayed if the Secure KVM Switch functions normally.
- If events that trigger the Secure KVM Switch’s protection mechanism are detected, and the switch shuts down and becomes inoperable, a Date/Time log will be recorded. (This particular Date/Time

log can only be decoded by the Secure KVM manufacturer.)

l. FW_VER: Firmware version.

m. TTL_LOGS: Total number of event logs

2. Log Data Area:

The Log Data Area is an area where critical and non-critical Events and Log Data can be displayed. Each Event /Log Data is recorded with time/date stamp and special codes to indicate the type and content of the event. The clock inside the KVM is used to print out timestamps for each event in the log. The internal battery inside the KVM ensures that the clock is active at all times and allows for accurate time recordings for all events. The initial date is set in each KVM manually at the time of manufacturing. These special codes can only be decoded by the Secure KVM Switch manufacturer if the device becomes inoperable.

a. Critical Log Data:

Critical log data includes administrator logon events, administrator password change events, critical administrator KVM configuration events, and self-test / tampering events, etc.

Maximum thirty-two critical event logs will be kept on the Secure KVM Switch.

For critical events that do not result in a Secure KVM lockdown, only a record of the most recent occurrence will be kept, which overwrites the records of prior occurrences of the same event.

b. Non-Critical Log Data:

Non-critical log data includes administrator logon records (including Administrator log in and log out events), administrator configuration events, device filter configuration events, self-test events, and power cycle events.

Maximum thirty-two non-critical event logs will be kept on the Secure KVM Switch. New log entries will overwrite the oldest one (for example, the thirty-third log entry will overwrite the first log).

User Authentication Device and HID Device Filtering Configuration

Administration functions enable authorized administrators to configure device filtering (CDF). This function allows the administrator to configure the Secure KVM Switch to accept or reject specific USB devices (for CAC port)¹, and reject specific HID devices (for Keyboard/Mouse Ports)²

CAC Port device filtering can also be configured via the ATEN Port Authentication Utility. Please refer to the ATEN Port Authentication Utility Guide for details.

Reset KVM to Default (Restore KVM to Factory Default)

This administrator function enables the authorized administrator to reset the Secure KVM Switch configuration to the factory default settings.

1. When the administrator performs Reset KVM to Default, settings previously configured by the administrator (such as USB device whitelist/blacklist and HID device blacklist) will be cleared and reset to the factory default settings.
2. Once Reset KVM to Default has been completed, the Secure KVM Switch will terminate the administrator logon mode, purge keyboard/mouse buffers, and power cycle the Secure KVM Switch automatically. After a successful self-test, the KVM port focus will be switched to Port 1, and the CAC function of each port will be set to the factory default (enabled).
3. Reset KVM to Default will not affect or erase the log data.
4. Reset KVM to Default will not affect the previously changed administrator password.
5. Reset KVM to Default will clear the whitelist/blacklist created by both the Secure KVM administrator functions and the ATEN Port Authentication Utility.

Note:

1. The CAC port does not support USB hub. The USB hub cannot be added to whitelist/blacklist via either administrator functions or ATEN Port Authentication Utility.
2. The user can only blacklist an HID device within the default HID devices* for the Keyboard/ Mouse Ports. Please connect the HID device (you would like to blacklist) directly to the Mouse Port (do not connect it to the KVM via a USB hub), and perform the configuration via administrator functions. After configuration, the blacklisted HID device will be rejected by both Keyboard/ Mouse Ports. A USB hub cannot be added to blacklist via administrator functions.

* The default HID devices for Keyboard/ Mouse Ports could be referred to bullet 4. in the section “Always use qualified and authorized peripheral devices” on page 3.

Appendix

Safety Instructions

General

- This product is for indoor use only.
- Read all of these instructions. Save them for future reference.
- Follow all warnings and instructions marked on the device.
- Do not place the device on any unstable surface (cart, stand, table, etc.). If the device falls, serious damage will result.
- Do not use the device near water.
- Do not place the device near, or over, radiators or heat registers.
- The device cabinet is provided with slots and openings to allow for adequate ventilation*. To ensure reliable operation, and to protect against overheating, the cabinet must never be blocked or covered.
- The device should never be placed on a soft surface (bed, sofa, rug, etc.) as this will block its ventilation openings*. Placing devices without slots or openings on a soft surface will affect the heat dissipation.
- The device should not be placed in a built in enclosure unless adequate ventilation has been provided.
- Never spill liquid of any kind on the device.
- Unplug the device from the wall outlet before cleaning. Do not use liquid or aerosol cleaners. Use a damp cloth for cleaning.
- The device should be operated from the type of power source indicated on the marking label. If you are not sure of the type of power available, consult your dealer or local power company.
- The device is designed for IT power distribution systems with 230V phase-to-phase voltage.
- To prevent damage to your installation it is important that all devices are properly grounded.
- The device is equipped with a 3-wire grounding type plug. This is a safety feature. If you are unable to insert the plug into the outlet, contact your electrician to replace your obsolete outlet. Do not attempt to defeat the purpose of the grounding-type plug. Always follow your local/national wiring codes.
- Do not allow anything to rest on the power cord or cables. Route the power cord and cables so that they cannot be stepped on or tripped over.
- If an extension cord is used with this device make sure that the total of the ampere ratings of all products used on this cord does not exceed the extension cord ampere rating. Make sure that the total of all products plugged into the wall outlet does not exceed 15 amperes.
- To help protect your system from sudden, transient increases and decreases in electrical power, use a surge suppressor, line conditioner, or uninterruptible power supply (UPS).
- Position system cables and power cables carefully; Be sure that nothing rests on any cables.

- Never push objects of any kind into or through cabinet slots. They may touch dangerous voltage points or short out parts resulting in a risk of fire or electrical shock.
- Do not attempt to service the device yourself. Refer all servicing to qualified service personnel.
- If the following conditions occur, unplug the device from the wall outlet and bring it to qualified service personnel for repair.
 - The power cord or plug has become damaged or frayed.
 - Liquid has been spilled into the device.
 - The device has been exposed to rain or water.
 - The device has been dropped, or the cabinet has been damaged.
 - The device exhibits a distinct change in performance, indicating a need for service.
 - The device does not operate normally when the operating instructions are followed.
 - Suitable for installation in Information Technology Rooms in accordance with Article 645 of the National Electrical Code and NFPA 75.

CAUTION: Never attempt to replace the internal battery or open the switches' enclosure.

*Note: Not all devices have slots or openings to allow for ventilatio

Consignes de Sécurité

Général

- Ce produit est destiné exclusivement à une utilisation à l'intérieur.
- Veuillez lire la totalité de ces instructions. Conservez-les afin de pouvoir vous y référer ultérieurement.
- Respectez l'ensemble des avertissements et instructions inscrits sur l'appareil.
- Ne placez jamais l'unité sur une surface instable (chariot, pied, table, etc.). Si l'unité venait à tomber, elle serait gravement endommagée.
- N'utilisez pas l'unité à proximité de l'eau.
- Ne placez pas l'unité à proximité de ou sur des radiateurs ou bouches de chaleur.
- Le boîtier de l'unité est destiné à assurer une ventilation adéquate*. Pour garantir un fonctionnement fiable et protéger l'unité contre les surchauffes, le boîtier de l'unité ne doit jamais être obstrué ou couvert.
- L'unité ne doit jamais être placée sur une surface molle (lit, canapé, tapis, etc.) car ceci obstruerait les ouvertures de ventilation*. Le fait de placer des appareils sans fente ni ouverture sur une surface souple affecte la dissipation thermique.
- L'appareil ne doit pas être placé dans une enceinte intégrée à moins de lui fournir une ventilation adéquate.
- Ne renversez jamais de liquides de quelque sorte que ce soit sur l'unité.
- Débranchez l'appareil de la prise secteur avant nettoyage. Ne pas utiliser de nettoyeur liquide ou en aérosol. Utiliser un chiffon humidifié pour le nettoyage.
- L'appareil doit être alimenté par le type de source indiqué sur l'étiquette. Si vous n'êtes pas sûr du type d'alimentation disponible, consultez votre revendeur ou le fournisseur local d'électricité.
- L'appareil est conçu pour les systèmes de distribution d'alimentation informatique avec une tension phase à phase de 230V
- Afin de ne pas endommager votre installation, vérifiez que tous les périphériques sont correctement mis à la terre.
- L'unité est équipée d'une fiche de terre à trois fils. Il s'agit d'une fonction de sécurité. Si vous ne parvenez pas à insérer la fiche dans la prise murale, contactez votre électricien afin qu'il remplace cette dernière qui doit être obsolète. Respectez toujours les codes de câblage en vigueur dans votre région/pays.
- Veuillez à ce que rien ne repose sur le cordon d'alimentation ou les câbles. Acheminez le cordon d'alimentation et les câbles de sorte que personne ne puisse marcher ou trébucher dessus.
- En cas d'utilisation d'une rallonge avec cette unité, assurez-vous que le total des ampérages de tous les produits utilisés sur cette rallonge ne dépasse pas l'ampérage nominal de cette dernière. Assurez-vous que le total des ampérages de tous les produits branchés sur la prise murale ne dépasse

pas 15 Ampères.

- Pour contribuer à protéger votre système contre les augmentations et diminutions soudaines et transitoires de puissance électrique, utilisez un parasurtenseur, un filtre de ligne ou un système d'alimentation sans coupure (UPS).
- Placez les câbles du système et les câbles d'alimentation avec précaution ; veillez à ce que rien ne repose sur aucun des câbles.
- N'insérez jamais d'objets de quelque sorte que ce soit dans ou à travers les fentes du boîtier. Ils pourraient entrer en contact avec des points de tension dangereuse ou court-circuiter des pièces, entraînant ainsi un risque d'incendie ou de choc électrique.
- N'essayez pas de réparer l'unité vous-même. Confiez toute opération de réparation à du personnel qualifié.
- Si les conditions suivantes se produisent, débranchez l'unité de la prise murale et amenez-la à un technicien qualifié pour la faire réparer:
 - Le cordon d'alimentation ou la fiche ont été endommagés ou éraillés.
 - Du liquide a été renversé dans l'unité.
 - L'unité a été exposée à la pluie ou à l'eau.
 - L'unité est tombée ou le boîtier a été endommagé.
 - Les performances de l'unité sont visiblement altérées, ce qui indique la nécessité d'une réparation.
 - L'unité ne fonctionne pas normalement bien que les instructions d'utilisation soient respectées.
 - Peut être installé dans des salles de matériel de traitement de l'information conformément à l'article 645 du National Electrical Code et à la NFPA 75.

ATTENTION : Ne jamais tenter de remplacer la batterie interne ni d'ouvrir le boîtier du commutateur.

*Remarque : Tous les appareils ne disposent pas de fentes ou d'ouvertures qui permettent la ventilation.

Technical Support

International

- For online technical support – including troubleshooting and documentation:
<http://eservice.aten.com>
- For telephone support, See *Telephone Support*, page iv:

North America

Email Support		support@aten-usa.com
Online Technical Support	Troubleshooting Documentation Software Updates	https://eservice.aten.com/eServiceCx/supportIndex.do?lang=en_US
Telephone Support		1-888-999-ATEN ext 4988

When you contact us, please have the following information ready beforehand:

- Product model number, serial number, and date of purchase.
- Your computer configuration, including operating system, revision level, expansion cards, and software.
- Any error messages displayed at the time the error occurred.
- The sequence of operations that led up to the error.
- Any other information you feel may be of help.

Limited Warranty

IN NO EVENT SHALL THE DIRECT VENDOR'S LIABILITY EXCEED THE PRICE PAID FOR THE PRODUCT FROM DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES RESULTING FROM THE USE OF THE PRODUCT, DISK, OR ITS DOCUMENTATION.

The direct vendor makes no warranty or representation, expressed, implied, or statutory with respect to the contents or use of this documentation, and especially disclaims its quality, performance, merchantability, or fitness for any particular purpose.

The direct vendor also reserves the right to revise or update the device or documentation without obligation to notify any individual or entity of such revisions, or update. For further inquiries, please contact your direct vendor.