ATEN

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 Port Authentication Utility 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

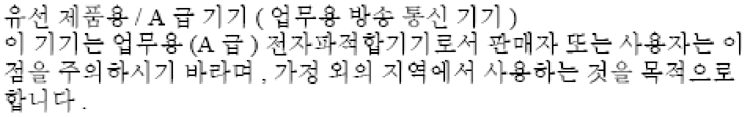
FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

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 .

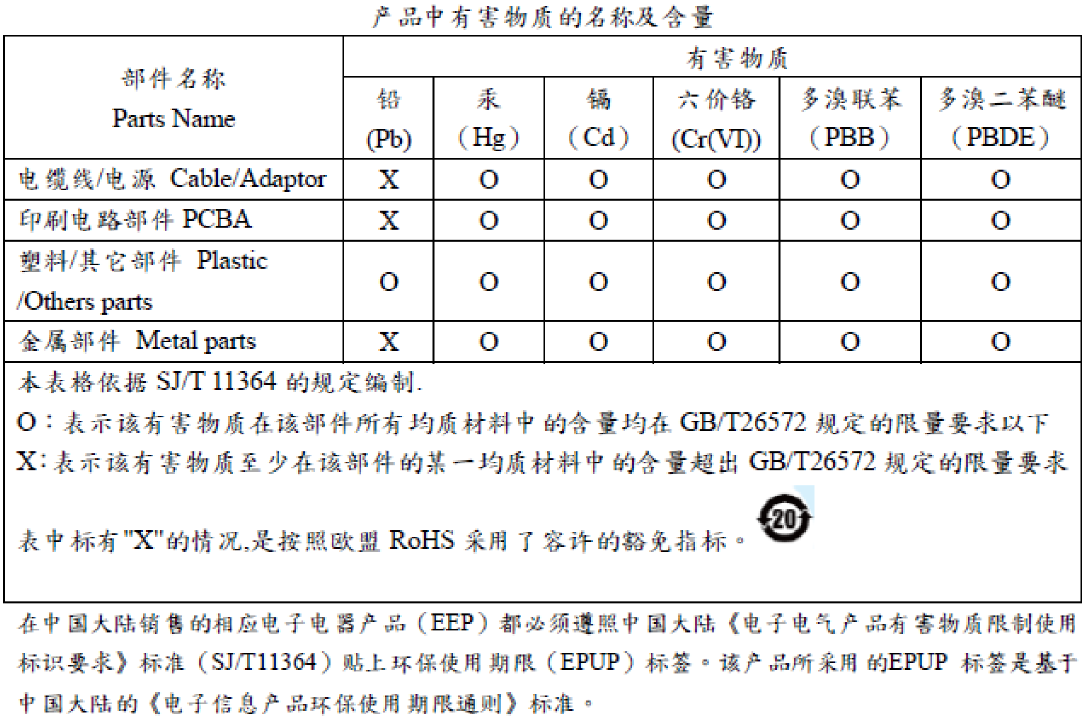
RoHS

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.

Manual Version: v1.03
Manual Date: 2021-1-25

Contents

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.

Tamper-evident seal

About This Port Authentication Utility Guide

This Port Authentication Utility Guide is intended for authorized administrators.

This Port Authentication Utility Guide is provided to help authorized administrators to configure authentication devices filters (whitelist / blacklist) on the ATEN Secure KVM Switch. To maximize security, the administrator is advised to audit log events recorded by the ATEN Secure KVM Switch on a routine basis.

This Port Authentication Utility Guide is applied to the following ATEN Secure KVM Switches.
The Port Authentication Utility is supported by models with CAC function only.

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

Overview

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

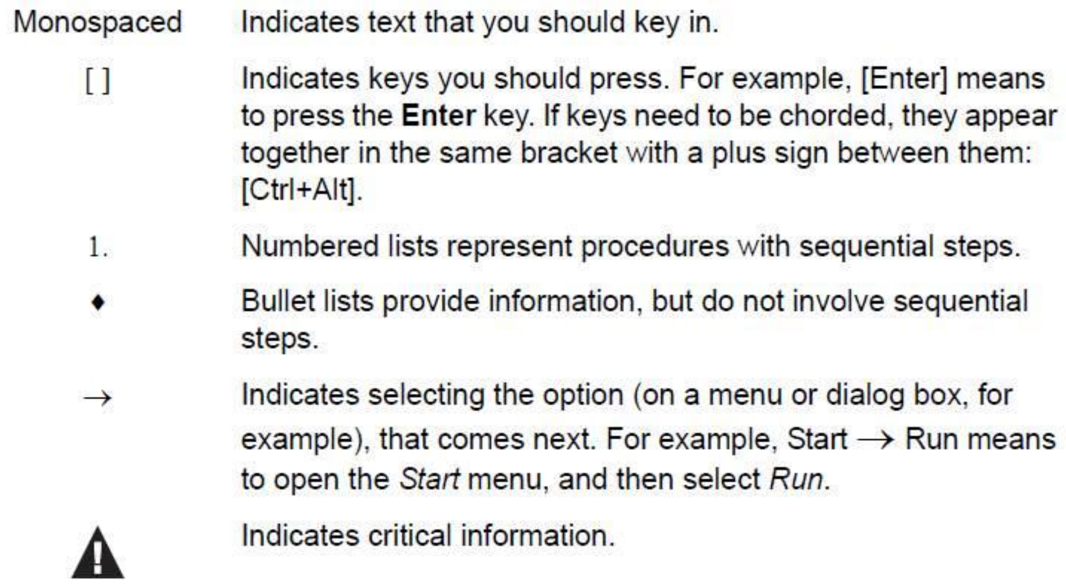
Chapter 2, Precautions and Preparation, provides step-by-step instructions for setting up your installation.

Chapter 3, Operation, explains the concepts involved in operating the ATEN Secure KVM Switch and Port Authentication Utility.

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 *Start* menu, and then select *Run*.
⚠	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 NIAP[1]-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) Reader 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.

Port Authentication Utility

To be complaint 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 offers a Port Authentication Utility to allow authorized administrators to configure the Secure KVM Switch to accept or reject specific USB devices. Through a secured access and authentication process, authorized administrators can perform configurable device filtering through the Port Authentication Utility.

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).

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 Secure KVM Switch, the administrator will be prompted to change the default password of the Port Authentication Utility after the first successful logon. The administrator is also advised to change the Port Authentication Utility password and audit event logs created by the ATEN Secure KVM Switch on a routine basis.

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 breeched 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’s 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’s 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 instructions.

Secure Administrative Operation

1. The ATEN Secure KVM Switch 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 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.

After the ATEN Secure KVM Switch is powered on and ready, power on your computers. By default the ATEN Secure KVM Switch will switch to Port 1 after a successful self-test.

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.

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 KVM 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. ☐ The LED lights green when the video connection is up and running. ☐ 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. ☐ Online – Lights dim orange to indicate that the computer attached to its corresponding port connected and powered on. ☐ Selected – Lights bright orange to indicate that the computer attached to its corresponding port has the KVM focus. ☐ 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. **Note:** 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.
CAC LED (on the Secure KVM switch and the RPS) CAC models only	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. ☐ 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. ☐ Selected – Lights bright green to indicate that the CAC function is enabled and the computer attached to its corresponding port has the CAC focus. ☐ None – No lights indicate that the cable is not connected or CAC has been disabled. ☐ Warning - Flashes to indicate that a non-qualified USB Smart card / CAC reader is connected when the corresponding port has the focus. **Note:** - 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.
Num Lock LED (on the Secure KVM switch and the RPS)	Lights green to indicate the Num Lock is enabled
Caps Lock LED (on the Secure KVM switch	Lights green to indicate the Caps Lock is enabled

and the RPS)	
Scroll Lock LED (on the Secure KVM switch and the RPS)	Lights green to indicate the Scroll Lock is enabled

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.

Port Authentication Utility

The Port Authentication Utility enables authorized administrators to configure user authentication device filtering. By default the USB CAC port on the ATEN Secure KVM Switch supports authorized User Authentication Devices such as USB Smartcard or CAC readers. The Port Authentication Utility enables authorized administrators to assign a whitelist and blacklist filter to the USB/CAC port.

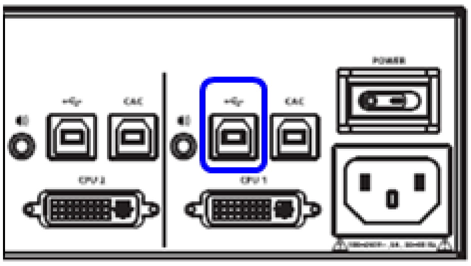
ATTENTION

- The whitelist and blacklist assigned by the Secure KVM Switch administrator functions has higher priority than the lists in the Port Authentication Utility. Please refer to the ATEN Secure KVM Switch Administrator's Guide for details.
- The reset of the whitelist and blacklist assigned by the Secure KVM administrator function does not affect the whitelist and blacklist uploaded by the Port Authentication Utility.
- With the Port Authentication Utility, when a device is assigned to both the blacklist and whitelist, the device will be treated as blacklisted. (Device Filtering Rule: blacklist always has priority over the whitelist.)
- The CAC port does not support USB hub. The USB hub can not be added to whitelist/blacklist via either administrator functions or ATEN Port Authentication Utility.

Setup for Port Authentication Utility

This section helps setup your installation with the Port Authentication Utility. Only authorized administrators are allowed to perform the installation and operate the Port Authentication Utility. The ATEN Port Authentication Utility supports Microsoft Windows 8 and higher.

1. Install the ATEN Port Authentication Utility to a separate secure source computer following the Installation instruction. This separate secure source computer is for management only, and has its own monitor, keyboard, and mouse connected for installation and operation. Power off this separate source PC after Port Authentication Utility installation.
2. Connect a qualified monitor, keyboard and mouse to the ATEN Secure KVM Switch's console section. (Refer to the Secure KVM Switch user manual for details.)
3. Connect the separate secure source computer (with the ATEN Port Authentication Utility previously installed) to Port 1 (demonstrated as below) of the Secure KVM Port section via the USB B-to-A cable of the KVM cable sets.



Port 1

4. Power on the ATEN Secure KVM Switch, and then power on the separate computer with Port Authentication Utility installed connected to Port 1. The ATEN Secure KVM Switch will switch to Port 1 after a successful self-test.
5. Use the monitor, keyboard, and mouse of the source computer to operate the ATEN Port Authentication Utility.

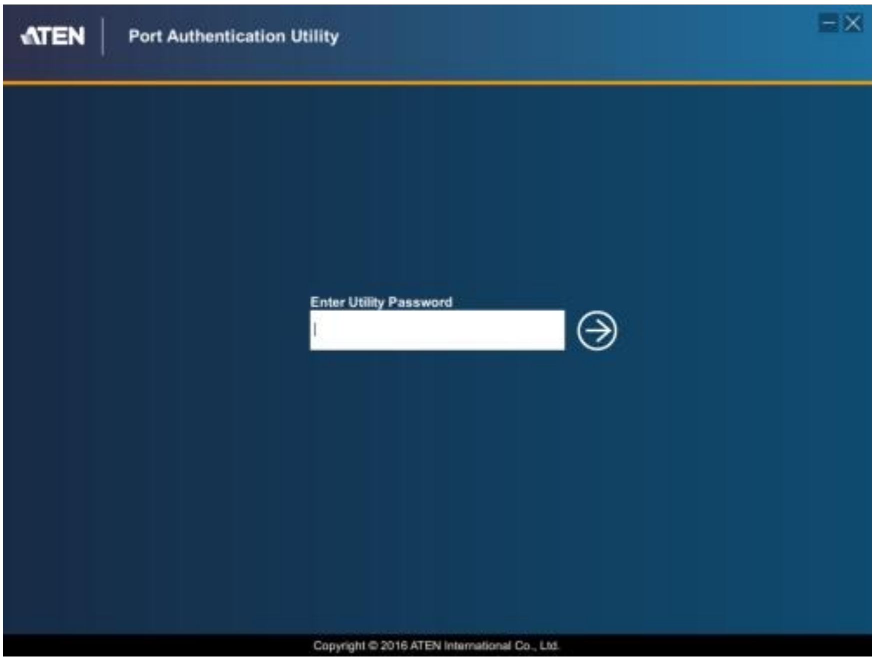
Port Authentication Utility Operation

After the separate secure computer and ATEN Secure KVM Switch are ready, open the Port Authentication Utility installed on the separate secure computer.

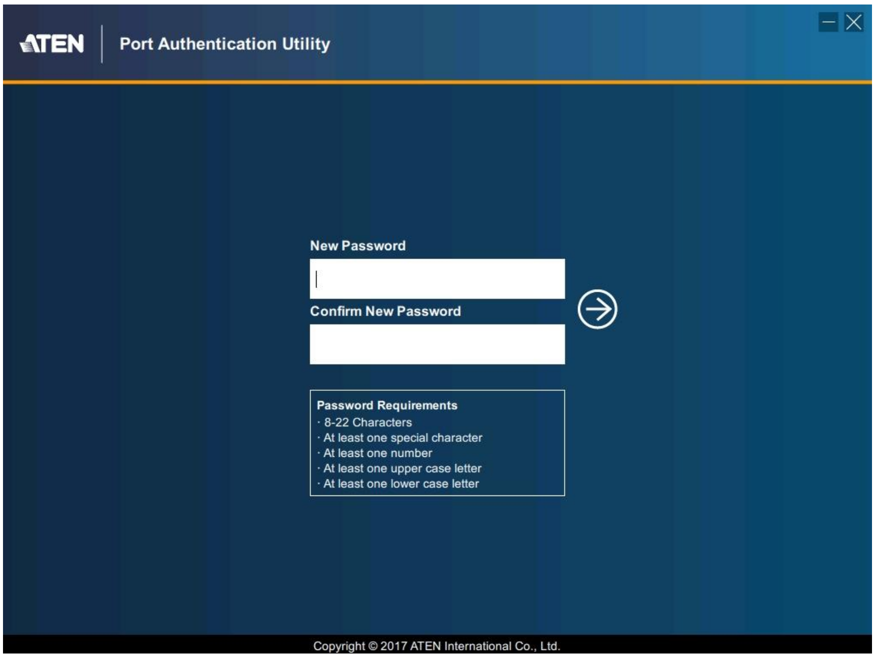
1. The first time you open the Port Authentication Utility, the Administrator will be prompted to enter the default password.

   The default password for the Port Authentication Utility is: abcd@XYZ#1357!

   The password is case-sensitive.


ATEN
Port Authentication Utility
Enter Utility Password
Copyright © 2016 ATEN International Co., Ltd.

2. After a successful password is input, the administrator will be prompted to change the password.



Password Requirements
· 8-22 Characters
· At least one special character
· At least one number
· At least one upper case letter
· At least one lower case letter

Copyright © 2017 ATEN International Co., Ltd.

The new password is case-sensitive. For maximum security, the new password must contain:

a. At least 8 characters, but no more than 22 characters.

b. A minimum of 1 lower case letter and,

c. A minimum of 1 upper case letter and,

d. A minimum of 1 numeric character and,

e. A minimum of 1 special character.

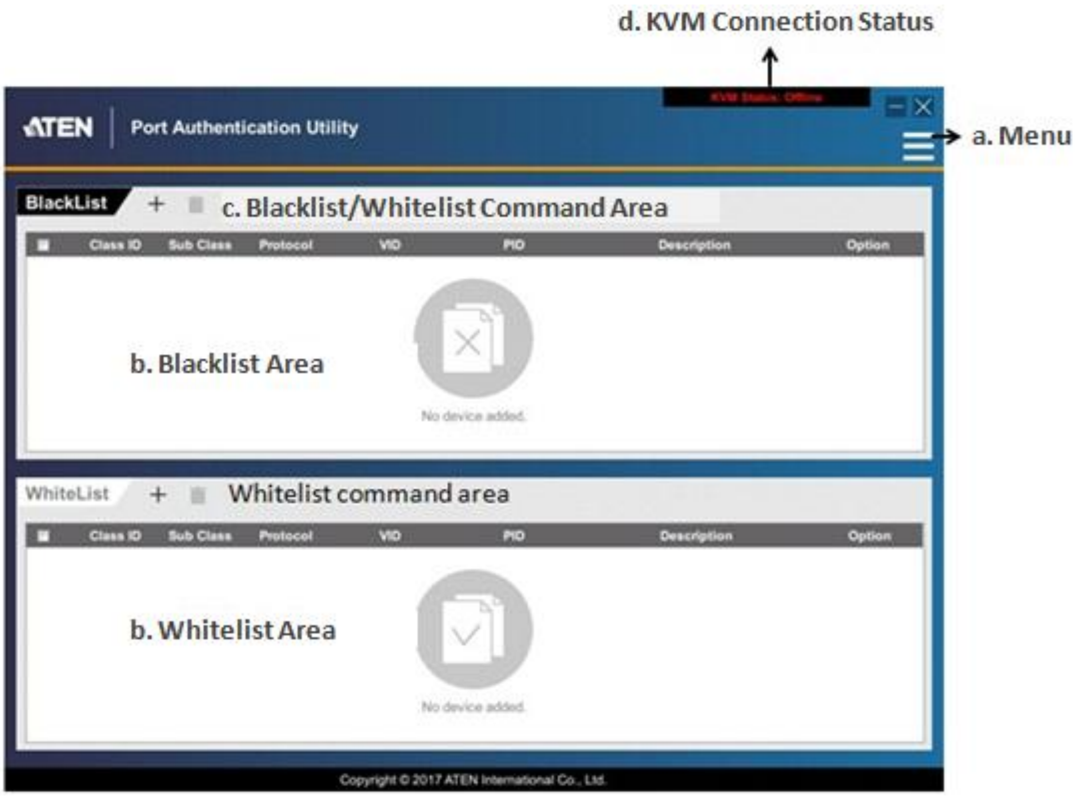
ATTENTION

- Do not use the default password for your new password.
- This password is for the Port Authentication Utility only. Do not use the same password for the Administrator Logon functions.
- The password for the Port Authentication Utility can be changed anytime via the password change option in the menu.

After the new password has been confirmed, the administrator can create a new filter list or open an existing filter list.

3. Port Authentication Utility Interface

The filter list contains a Blacklist and Whitelist. The Port Authentication Utility interface allows administrators to add, remove, or edit filtering rule entries to the Blacklist or Whitelist.



a. Menu:

A menu provides options to create a new blacklist or whitelist filter, save an edited filter, open/import an existing filter from the source computer, or update the Secure KVM Switch filter. A change password option is also available.

b. Blacklist and Whitelist Area:

Filtering rules added to the Blacklist or Whitelist will be displayed in these areas.

c. Blacklist/Whitelist Command Area:

By clicking on the “Add” or “Delete” icons the administrator can add new rules to, or delete selected rules from the Blacklist or Whitelist Area.

d. KVM Connection Status:

This area shows the KVM connection status.

4. Editing the Blacklist and Whitelist

The Port Authentication Utility enables authorized administrators to edit the filtering rules to block (Blacklist) or allow (Whitelist) specific USB devices connected to USB CAC port on the Secure KVM Switch.

A filtering rule is defined by USB (Base) Class ID, Sub-Class, Protocol, VID (device Vendor ID), and PID (device Product ID) of a USB device. For example, a Base Class ID of a Smart Card device is 0Bh.

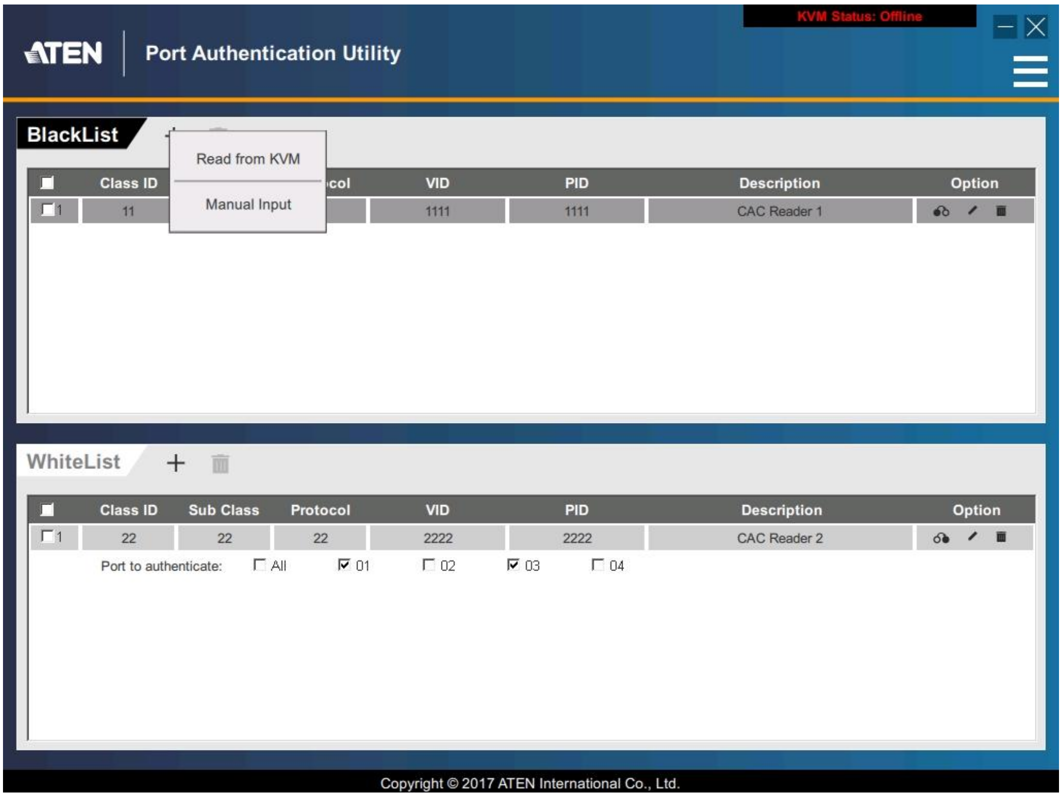
Base Class	Sub-Class	Protocol	Device
0Bh	xxh	xxh	Smart Card device

By completing the Class ID, Sub-Class, Protocol, VID and PID field of a filtering rule, the administrator can assign a filtering rule to the Blacklist or Whitelist to block or allow a USB device.

When adding the value to Class, Sub-Class, Protocol, PID or VID field, the last digit "h" can be ignored. For example, when adding "0Bh" to the Class ID filed, just type "0B"

a. Manually adding a filtering rule to the Blacklist or Whitelist:

To add a new filtering rule to the Blacklist, click on the "+" icon in Blacklist command area, and choose "Manual Input" from the menu to edit a filtering rule.



BlackList

□	Class ID		col	VID	PID	Description	Option
□ 1	11			1111	1111	CAC Reader 1	

WhiteList

□	Class ID	Sub Class	Protocol	VID	PID	Description	Option
□ 1	22	22	22	2222	2222	CAC Reader 2	

Port to authenticate: □ All ☑ 01 □ 02 ☑ 03 □ 04

Copyright © 2017 ATEN International Co., Ltd.

Manually type the value for the Class ID, Sub Class, Protocol, VID, and PID fields. For the PID value, 4 digits are required. A wildcard character asterisk "*" can be used in the field to represent one or more other characters. For example, the PID filtering rule (5***) shown below, would include all the devices whose PID starts with a 5.

Class ID	Sub Class	Protocol	VID	**PID**
0B	11	22	1234	**5*****

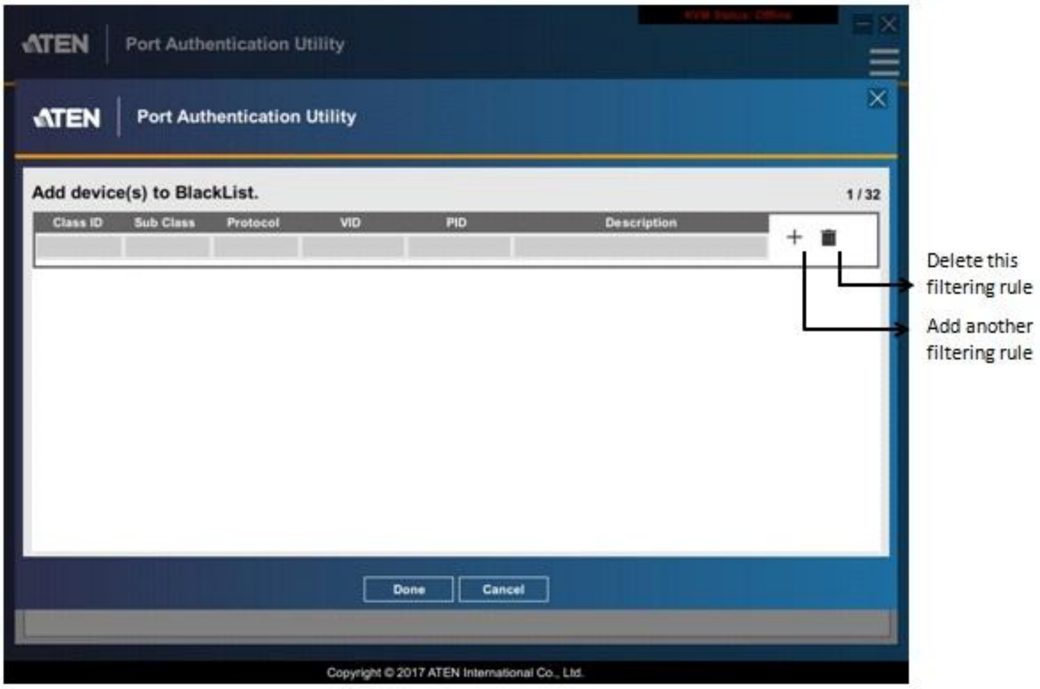
The filtering rule below includes all the devices whose PID starts with 5 and ends with 1

Class ID	Sub Class	Protocol	VID	PID
0B	11	22	1234	**5**1**

A short description can be added to the Description field to describe the device.

After finishing a filter rule entry, click the "+" icon on the right to add another filter rule. Click on the recycle bin icon to discard an entry.

Click the "Done" button after editing all the entries. The added filter rules will be added to the Blacklist area.


ATEN
Port Authentication Utility
KVM Status: Offline
ATEN
Port Authentication Utility
Done
Cancel
Copyright © 2017 ATEN International Co., Ltd.

Add device(s) to BlackList.

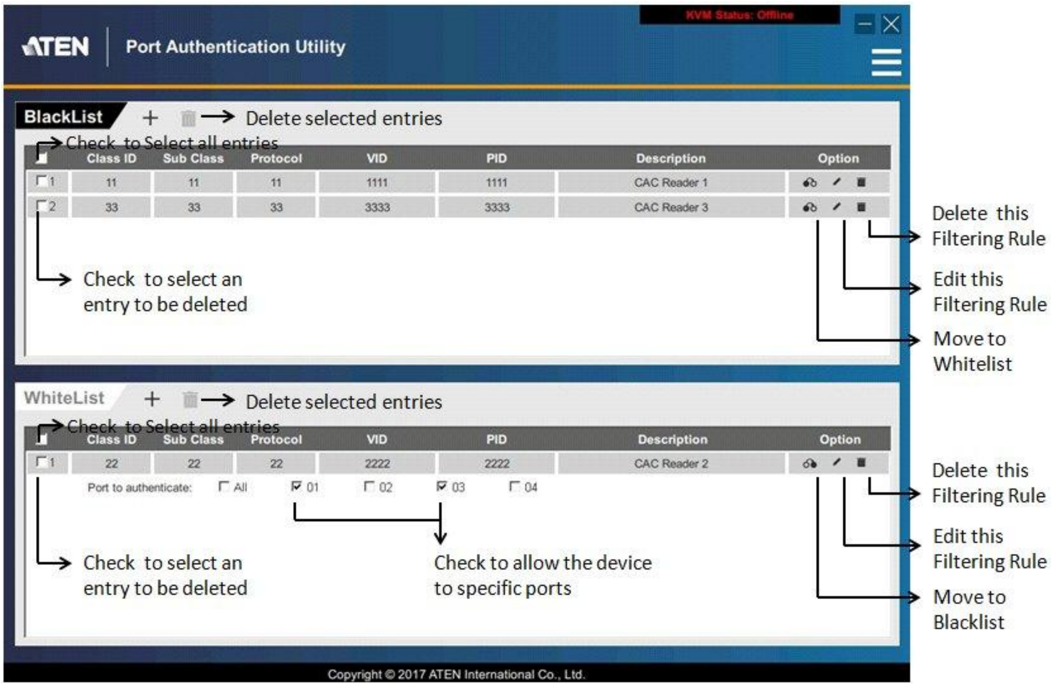
1 / 32

Class ID	Sub Class	Protocol	VID	PID	Description

Delete this filtering rule

Add another filtering rule

Filtering rules added and listed in the Blacklist area can be edited, deleted, or moved to the Whitelist.


KVM Status: Offline
ATEN
Port Authentication Utility
BlackList
Delete selected entries
Check to Select all entries
Check to select an entry to be deleted
Delete this Filtering Rule
Edit this Filtering Rule
Move to Whitelist
WhiteList
Delete selected entries
Check to Select all entries
Check to select an entry to be deleted
Check to allow the device to specific ports
Delete this Filtering Rule
Edit this Filtering Rule
Move to Blacklist
Copyright © 2017 ATEN International Co., Ltd.

BlackList

	Class ID	Sub Class	Protocol	VID	PID	Description	Option
□ 1	11	11	11	1111	1111	CAC Reader 1	
□ 2	33	33	33	3333	3333	CAC Reader 3	

WhiteList

	Class ID	Sub Class	Protocol	VID	PID	Description	Option
□ 1	22	22	22	2222	2222	CAC Reader 2	

Port to authenticate: □ All ☑ 01 □ 02 ☑ 03 □ 04

The administrator can use the same approach to add filtering rules to the Whitelist.

If a device is added to the Blacklist, it will be blocked from all Secure KVM Switch ports.
If a device is added to the Whitelist, it can be allowed access from the ports specifically assigned by the administrator.
Blacklist filtering rules always supersede the Whitelist filtering rules.
A maximum of 32 filtering rules can be added to the Blacklist, and a maximum of 32 filtering rules can be assigned to the Whitelist.

b. Retrieving the USB device value from the device on the Secure KVM USB CAC port.

In addition to manually typing the value for each filtering rule, administrators can retrieve the USB device info from the USB device when it is connected to the Secure KVM Switch USB CAC port.

Before retrieving the USB value from the USB CAC port, connect the USB device to the Secure KVM Switch USB CAC port. When the USB device is connected to the USB CAC port, use the Secure KVM Switch console keyboard to:

(a) Press and hold down the Ctrl key

(b) Press and hold down the F12 key:

[Ctrl + F12]

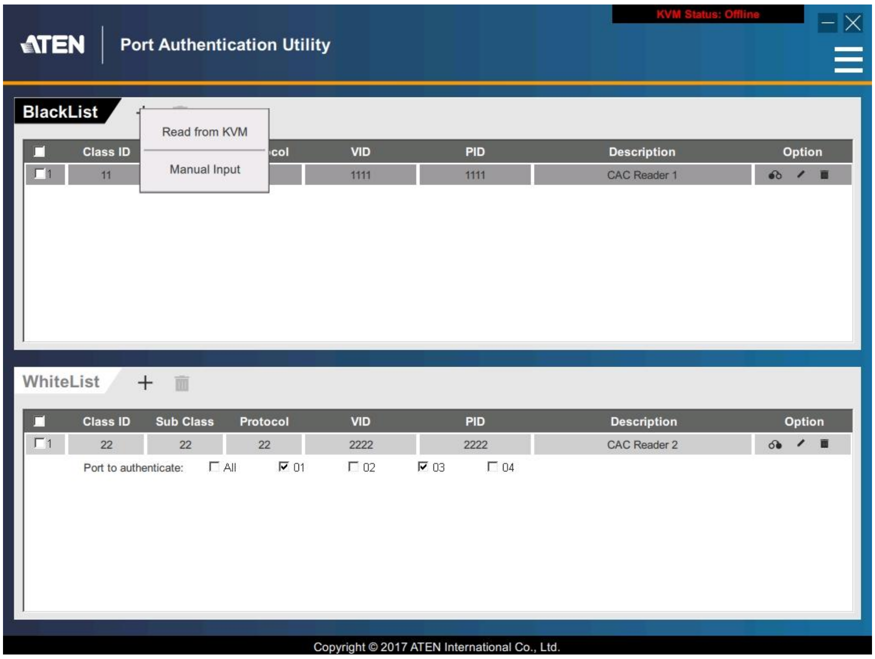
(c) First release the F12 key, followed by the Ctrl key

(d) Press and release the [U] key, then press and release [Enter]

Please make sure not to exceed 2 seconds between each key.

The combination of key strokes enables the Secure KVM Switch to be ready for the administrator logon authentication and administrator's retrieval of the device info from the USB CAC port.

To add the values of the USB device from the USB CAC port to the filtering rules, click on the "+" icon in the command area, and choose "Read from KVM".



BlackList

☐	Class ID		col	VID	PID	Description	Option
☐ 1	11			1111	1111	CAC Reader 1	

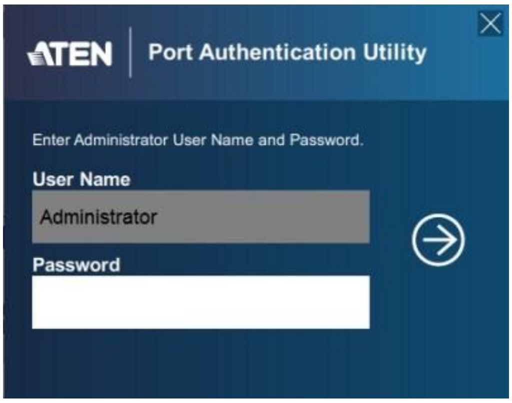
WhiteList

☐	Class ID	Sub Class	Protocol	VID	PID	Description	Option
☐ 1	22	22	22	2222	2222	CAC Reader 2	

Port to authenticate: ☐ All ☑ 01 ☐ 02 ☑ 03 ☐ 04

Copyright © 2017 ATEN International Co., Ltd.

The administrator will be prompted for user name and password authentication.



Enter Administrator User Name and Password.

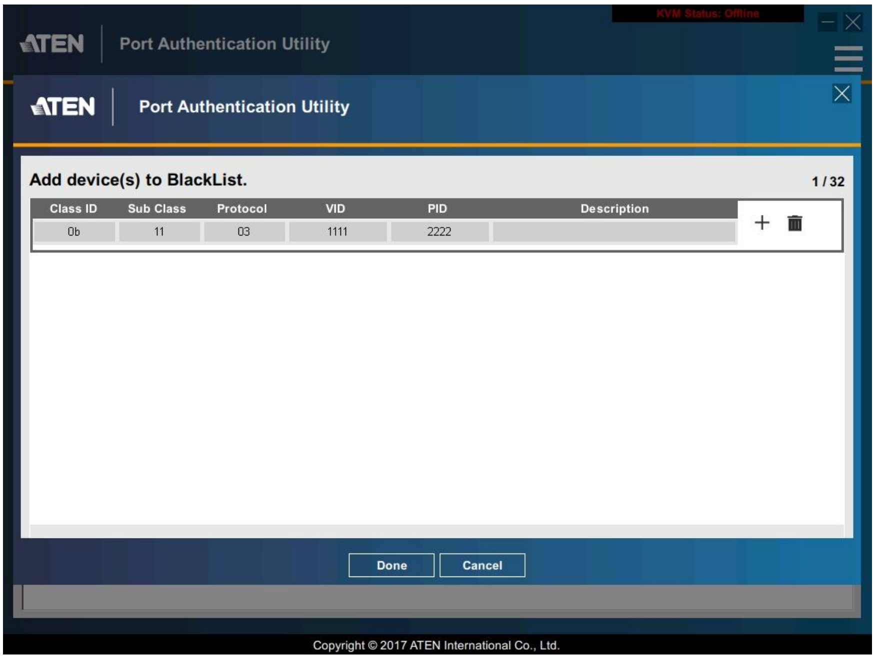
User Name: Administrator

Password:

ATTENTION

- The User Name and Password here refers to the ID and password for the Administrator Logon functions. Please refer to the Secure KVM Switch Administrator's Guide for detail.
- With three failed attempts to log in, the Administrator Logon mode will be terminated automatically. Access to the Administrator Logon mode will be blocked for 15 minutes.
- With nine failed attempts to log in, the Secure KVM Switch will become inoperable permanently. If this happens, please remove it from service immediately and contact your ATEN dealer.

After a successful Administrator Logon authentication, the values of the USB device connected to the Secure KVM Switch USB CAC port will be displayed in the filtering rule entry. The administrator can continue to edit this entry or move on to the Blacklist or Whitelist work area. The Administrator Logon session terminates automatically after the value of the device on the Secure KVM USB CAC port is successfully retrieved.


KVM Status: Offline
ATEN
Port Authentication Utility
ATEN
Port Authentication Utility
Done
Cancel
Copyright © 2017 ATEN International Co., Ltd.

Add device(s) to BlackList. 1 / 32

Class ID	Sub Class	Protocol	VID	PID	Description
0b	11	03	1111	2222	

5. Upload the Filtering List

The administrator can upload a filtering list when finished with the filter list editing.

a. Before uploading the filtering list, the administrator should make the Secure KVM Switch ready for the connection. Use the Secure KVM Switches' console keyboard to:

(a) Press and hold down the Ctrl key

(b) Press and hold down the F12 key:

[Ctrl + F12]

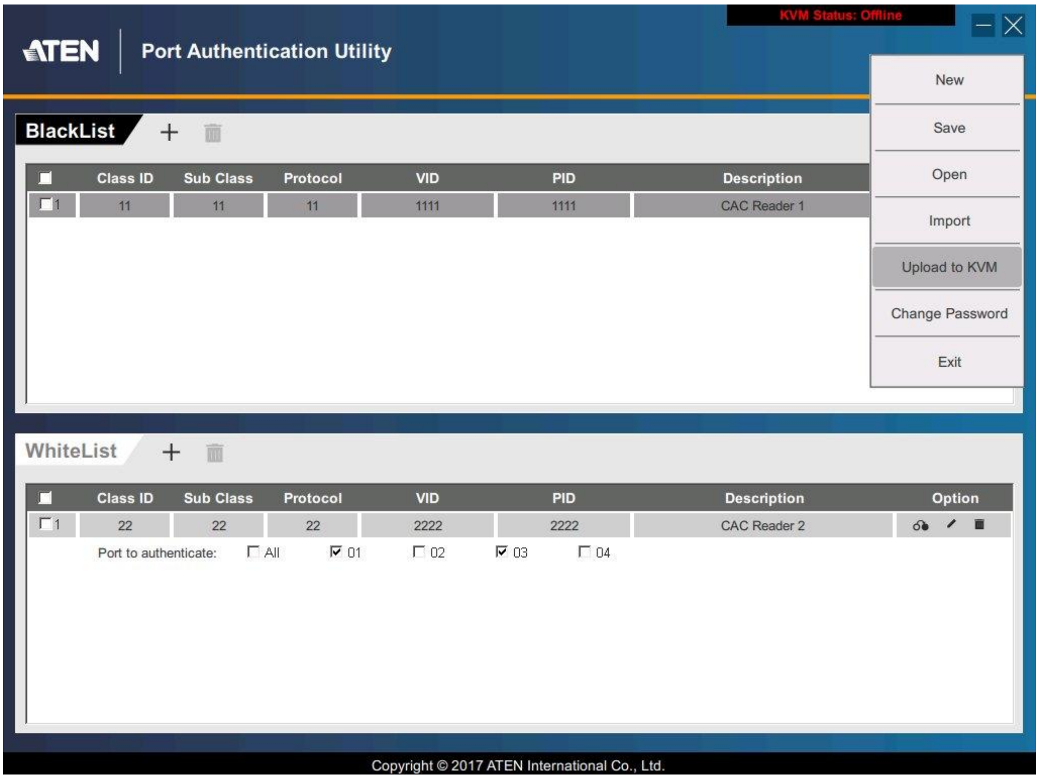
(c) First release the F12 key, followed by the Ctrl key

(d) Press and release the [U] key, then press and release [Enter]

Please make sure not to exceed 2 seconds between each key.

The Secure KVM Switch will be ready for the filtering list upload.

b. Choose the “Upload to KVM” option from the Menu.



BlackList

□	Class ID	Sub Class	Protocol	VID	PID	Description
□ 1	11	11	11	1111	1111	CAC Reader 1

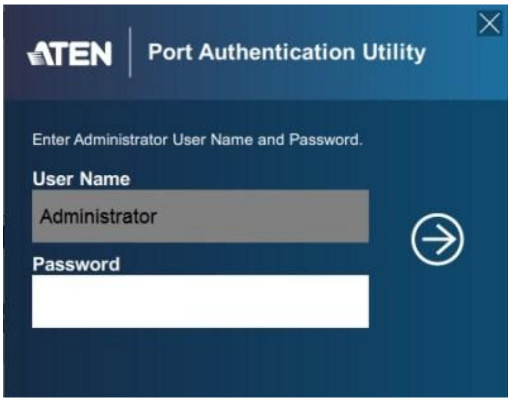
WhiteList

□	Class ID	Sub Class	Protocol	VID	PID	Description	Option
□ 1	22	22	22	2222	2222	CAC Reader 2	

Port to authenticate: □ All ☑ 01 □ 02 ☑ 03 □ 04

Copyright © 2017 ATEN International Co., Ltd.

After choosing the “Upload to KVM” option, the administrator will be prompted for user name and password authentication.



Enter Administrator User Name and Password.

User Name: Administrator

Password:

ATTENTION

- The User Name and Password here refers to the ID and password for Administrator Logon functions. Please refer to the Secure KVM Switch Administrator’s Guide for details.
- With three failed attempts to logon, the Administrator Logon mode will be terminated automatically. Access to Administrator Logon mode will be blocked for 15 minutes.
- With nine failed attempts to log in, the Secure KVM Switch becomes inoperable permanently. If this happens, please remove it from service immediately and contact your ATEN dealer.

After a successful Administrator Logon authentication, the Filter list will upload to the Secure KVM Switch. The Secure KVM Switch will allow or block USB devices connected to the USB CAC port based on the updated Blacklist and Whitelist.

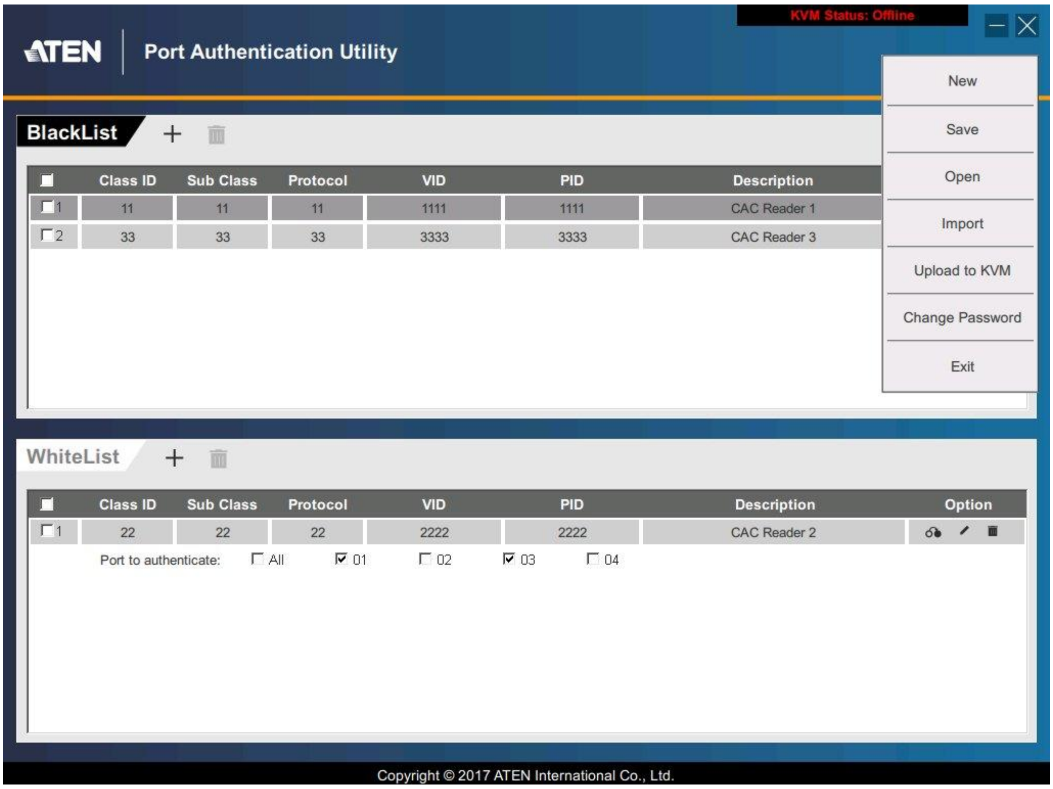
The Administrator Login session terminates automatically after the filtering list is updated.
To make the updated filtering list take effect, remove the Secure KVM Switch from the installation and power cycle the Secure KVM Switch.

ATTENTION

- The Blacklist and Whitelist defined by the Administrator Logon Functions always supersedes the filtering list created by the Port Authentication Utility. The administrator should make sure there is no conflict when editing device entries.
- The updated filtering list will overwrite the one previously uploaded to the Secure KVM Switch.
- A 2-port based filtering list can only be uploaded to 2-port Secure KVM Switch models (4-port list to 4-port models; 8-port list to 8-port models). An error message shows up when uploading the wrong filtering List.
- The only way to clear the Blacklist and Whitelist updated by the Port Authentication Utility is for the administrator to perform a Reset KVM to Default. (This Reset KVM to Default also clears the Blacklist and Whitelist created by the Secure KVM administrator functions. Please refer to the Administrator’s Guide for more details.)

6. Create, Save, Open, and Import a Filtering list

More options are available from the menu for filtering list operations.



BlackList

☐	Class ID	Sub Class	Protocol	VID	PID	Description
☐1	11	11	11	1111	1111	CAC Reader 1
☐2	33	33	33	3333	3333	CAC Reader 3

WhiteList

☐	Class ID	Sub Class	Protocol	VID	PID	Description	Option
☐1	22	22	22	2222	2222	CAC Reader 2	

Port to authenticate: ☐ All ☑ 01 ☐ 02 ☑ 03 ☐ 04

a. New

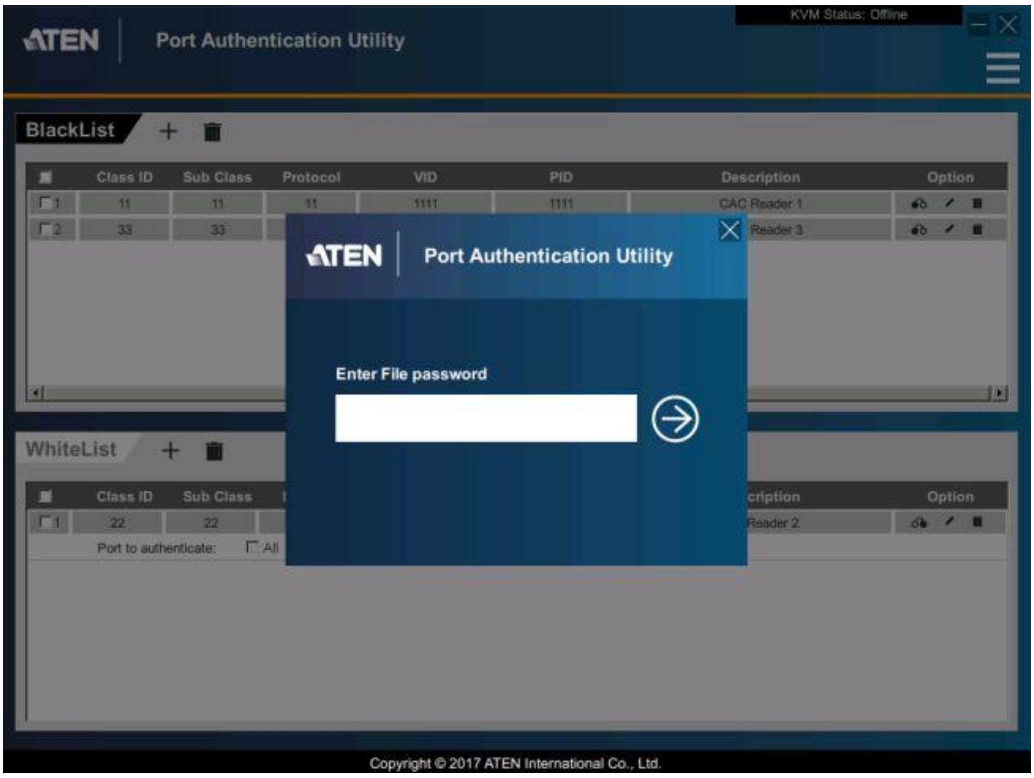
Use this option to create a new filtering list.

When creating a new filtering list, follow the instructions in the Port Authentication Utility to choose a proper model type (2, 4, or 8-port model) for the filtering list.

b. Save

The administrator can save a filtering list and edit it later.

All saved filtering lists will be protected by a password. When saving a filtering list, the administrator will be prompted to assign a password to the file. The password is case-sensitive. Do not use the same password as the Administrator Logon functions or Port Authentication Utility. After assigning the password, the administrator will be prompted to enter the filename, and choose a folder on the source computer to save the filtering list.


ATEN
Port Authentication Utility
KVM Status: Offline
BlackList
WhiteList
Port Authentication Utility
Enter File password
Copyright © 2017 ATEN International Co., Ltd.

	Class ID	Sub Class	Protocol	VID	PID	Description	Option
□ 1	11	11	11	1111	1111	CAC Reader 1	
□ 2	33	33				Reader 3	

	Class ID	Sub Class		cription	Option
□ 1	22	22		Reader 2	

Port to authenticate: □ All

c. Open

The administrator can open a previously saved filtering list and continue with editing.

When opening a saved filtering list, the administrator will be prompted to input the password created for the file.

d. Import

The administrator can import filtering rule entries of a previously saved filtering list to a current filtering list. When importing a saved filtering list, the administrator will be prompted to input the password for the file to be imported.

If the administrator is editing a 2-port filtering list, the filtering list to be imported must also be a 2-port based list.

7. Change Password

The administrator can change the password for the Port Authentication Utility at anytime.

Choose the “Change Password” option in the menu to change the password.

The new password is case-sensitive. For maximum security, the new password must contain:

a. At least 8 characters, but no more than 22 characters.

b. A minimum of 1 lower case letter and,

c. A minimum of 1 upper case letter and,

d. A minimum of 1 numeric character and,

e. A minimum of 1 special character.

8. Exit the Port Authentication Utility

   Choose the “Exit” option in the menu to exit the Port Authentication Utility.

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 ventilation

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 adequate*. 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 nettoyant liquide ou en aérosol. Utiliser une 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 function 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 risqué 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.