Raritan Secure Switch Administrator Guide

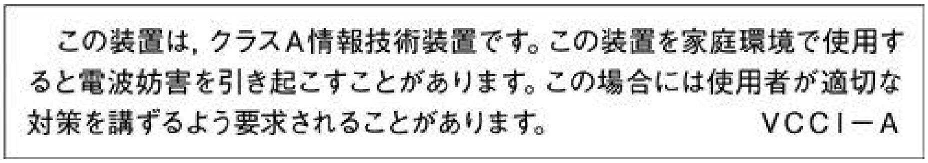
SecureSwitch-AdminGuide-0A-v1.0-E
August 2022
Release 1.0

Contents

FCC Information

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 in a commercial installation. This equipment generates, uses, and can radiate radio frequency energy and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. Operation of this equipment in a residential environment may cause harmful interference.

VCCI Information (Japan)



この装置は，クラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。　ＶＣＣＩ－Ａ

Raritan is not responsible for damage to this product resulting from accident, disaster, misuse, abuse, non-Raritan modification of the product, or other events outside of Raritan's reasonable control or not arising under normal operating conditions.

If a power cable is included with this product, it must be used exclusively for this product.

About This Administrators Guide

This Administrators Guide is intended for authorized administrators.

The guide helps you audit logs and configure your Raritan Secure Switch system. To maximize security, the administrator should audit logs/events record and the Raritan Secure Switch configuration on a routine basis.

The following Raritan Secure Switch models and are covered in this Administrators Guide.

► *Raritan Secure Switch models:*

Configuration (with CAC function)		2-Port models	4-Port models	8-port models
DisplayPort	Single Head	RSS4-102-DP	RSS4-104-DP	RSS4-108-DP
	Dual Head	RSS4-102-Dual-DP	RSS4-104-Dual-DP	RSS4-108-Dual-DP
HDMI	Single Head	RSS4-102	RSS4-104	NA
	Dual Head	RSS4-102-Dual	RSS4-104-Dual	NA

Attention

Read the following sections before operating the Secure Switch.

► *Important Message:*

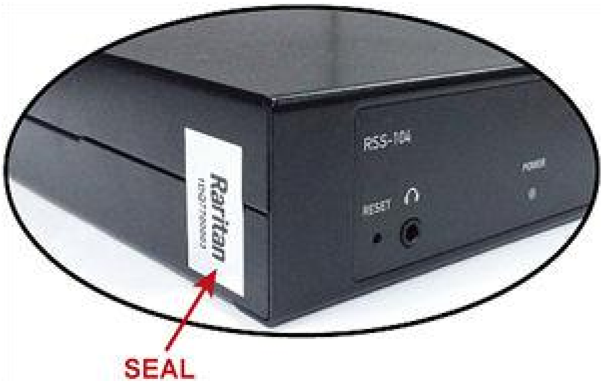
The device is equipped with a 3-wire grounding type plug as safety. If you are unable to insert the plug into the outlet, contact your electrician to replace your obsolete outlet.

Do not attempt to defeat the purpose of the grounding-type plug. Always follow your local/national wiring codes.

► *DO NOT use the product in these scenarios:*

When you observe any issues below, do *not* use the product and contact your dealer immediately.

- The tamper-evident seal is missing or peeled. The diagram below indicates the location of the seal.



- All front panel LEDs flash continuously.
- The Secure Switch's enclosure appears breached.

► *Chassis-intrusion-detection security:*

- This Secure Switch is equipped with active always-on chassis intrusion detection. Any attempt to open the enclosure will permanently damage or disable the Secure Switch, and void the warranty.

► *Change the default password:*

- To maximize security and to prevent unauthorized access to Secure Switch, change the default password after your first successful login.

Introduction

In This Chapter

Overview

Raritan Secure Switch series is NIAP-certified and compliant with NIAP PP 4.0 (Protection Profile for Peripheral Sharing Switch version 4.0) requirements, meeting the latest security requirements set by the U.S. Department of Defense for peripheral sharing switches. Compliance ensures maximum information security while sharing a single set of HIDs (keyboards, mice, speakers, and CAC readers) between multiple computers. Conformity with Protection Profile v4.0 certifies that other USB peripherals cannot be connected to the console ports of Secure Switch, and that only a keyboard and a mouse are accommodated, therefore providing high-level security, protection and safe-keeping of data.

The Secure Switch's hardware security includes tamper-evident tape, chassis intrusion detection, and tamper-proof hardware, while software security includes restricted USB connectivity – non HIDs (Human Interface Devices) are ignored on port switching. An isolated channel per port makes it impossible for data to be transferred between secure and unsecure computers. In addition, the keyboard and mouse buffer are cleared on port switching.

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

Notes:

- 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).
- Raritan Secure Switch series additionally satisfies Protection Profile version 4.0 for Peripheral Sharing Device (PSD).
- USB 1.1 for keyboard, mouse connections, and USB 2.0 for CAC reader connection.

Administrative Functions

To be compliant with Protection Profile 4.0 while providing higher deployment flexibility, wider product support for new authentication devices, and maximum security, Raritan Secure Switch supports Administrative Functions.

Through secured access, authorized Administrator can audit log data, configure Secure Switch, and perform configurable device filtering.

Hardware Setup

In This Chapter

Before You Begin

Before using the Secure Switch, make sure you have read Attention (on page 5).

Safety Instructions

- 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 allows 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. Likewise, 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 100-240V, 1A, 50-60 Hz input line 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.

CAUTION: Never attempt battery replacement or open the switches' enclosure.

► *CAUTION for MAINTENANCE STAFF:*

- RISK OF EXPLOSION IF BATTERY IS REPLACED BY AN INCORRECT TYPE.
- DISPOSE OF USED BATTERIES ACCORDING TO THE INSTRUCTIONS.

Tampering Prevention and Detection

- The Secure Switch and Remote Port Selector include a tamper-evident tape to provide visual indications of intrusion to its enclosure. If the tamper-evident seal is missing, peeled, or looks as if it's been adjusted, DO NOT use it and contact your Raritan dealer immediately
- The Secure Switch and Remote Port Selector are equipped with active always-on chassis intrusion detection. If a mechanical intrusion is detected, the Secure Switch will be permanently disabled and its front panel LEDs will flash continuously. If this product's enclosure appears breached or all LEDs are flashing continuously, stop using it, remove it from service immediately and contact your dealer.
- Never attempt to open the Secure Switch's or Remote Port Selector's enclosure. Any attempt to open the enclosure will permanently damage and disable this product. The attempt to open its enclosure will activate the chassis intrusion detection security, which will render it inoperable and void the warranty.
- The Secure Switch and Remote Port Selector cannot be upgraded, serviced or repaired.
- The Secure Switch contains an internal battery which is non-replaceable. Never attempt battery replacement or open the Secure Switch's enclosure. 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.

Using Qualified Peripheral Devices Only

For security purposes, you must always connect supported and authorized peripheral devices to the Secure Switch. Otherwise, the Secure Switch may not function properly.

► *USB keyboard and mouse:*

- The Secure Switch only supports a *standard* USB keyboard and mouse (or pointing device).
- DO NOT use the following keyboards and/or mice.
  - A wireless keyboard or mouse
  - A keyboard or mouse with internal USB hub
  - Composite device with Non-HID Fucntions
- If connecting an unsupported keyboard, the keyboard will *not* function. No keystrokes will be displayed on the screen.

  Note that the Secure Switch automatically disables some functions on the connected keyboard for security purposes.
  - *Num Lock LED*
  - *Caps Lock LED*
  - *Scroll Lock LED*
  - *Special multimedia keys*
- If connecting an unsupported mouse, the mouse will *not* function. No mouse cursor movement will be displayed on the screen.
- 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 Functions section.

► *Video:*

- You can use a HDMI or DisplayPort monitor connected to the HDMI or DisplayPort port of the Secure Switch User Console, depending on the selected model
- Only use a supported monitor. When connecting a monitor to the Secure Switch, the Secure Switch will filter the connected monitor by checking the monitor's EDID (Extended display identification data). If the check fails, the Secure Switch will reject the monitor and the video content will not be displayed on the monitor.
- DO NOT use wireless video transmitters or any docking device.

► *Audio:*

- Connect *standard* "analog" speakers or headphones only.
- The Secure Switch does not support an analog microphone or line-in audio input.

Do not connect a microphone to the Secure Switch's audio output port, including a headset with the microphone.

► *NO Thunderbolt™ technology devices:*

- DO NOT connect any Thunderbolt™ technology device.

► *USB card reader (optional):*

- The Secure Switch's USB CAC port supports only authorized User-Authentication Devices by default, such as a USB smart card or CAC reader.
- DO NOT connect non-User-Authentication USB devices to the USB CAC port. Unqualified or unauthorized USB devices will be rejected.
- DO NOT use a USB CAC Authentication Device or other peripheral devices that adopt an external power source.
- For a list of supported card readers, see: Supported Card Readers (on page 10).

Supported Card Readers

The following USB smart card or CAC readers are supported by Secure Switch. Other types of card readers may also work but Raritan has not tested their operation.

- ACS ACR38U-A1
- ACS ACR38U-BMC-R
- ACS ACR38T-IBS-R
- Omnikey6121
- SCM_SCR3310
- CHERRY_ST-1044U
- EasyATM Pro2
- EasyATM AU9520
- Galileo RU056
- Kinyo KCR352
- Esense 17-SCR680
- EZ100PU

Important: It is highly recommended that you install the proprietary driver of your card reader onto the computer(s), which is either shipped with the card reader or can be downloaded from the official website of the card reader's vendor. If not, the card reader may not function properly.

Secure Installation Guidelines

- DO NOT attempt to connect or install the following devices to the computers connected to the Secure Switch.

  - TEMPEST computers
  - Telecommunications equipment
  - Frame grabber video cards
  - Special audio processing cards
- Before installation, make sure the power sources to all devices involved in the installation are turned off.
- Hot-swapping of the console monitor is NOT supported.

  You must power OFF the Secure Switch and console monitor before changing or re- connecting the monitor. Power them back ON after finishing the monitor connection.
- A computer should only be powered on after all of the cable connections to the Secure Switch are finished, including video, USB and audio.
- Important safety information regarding the placement of this device is provided in the topic titled Safety Instructions (on page 7) in the Administrators Guide. Please review it before proceeding.
- Refer to Raritan Secure Switch User Guide for hardware installation.

Secure Administrative Operation

- The Raritan Secure Switch Administration function, such as Log data audit and configuration of authentication devices filter, can only be performed by authorized Administrator.
- To maximize security and to prevent unauthorized access to Secure Switch, please change the default logon password right after your first successful logon.
- Administrator’s Logon session will be terminated if Administrator logs off the session or the KVM is powered off.
- Please refer to Operation section for detail Administrator functions.

Operation

In This Chapter

Power ON

When you power on, reset, or power cycle the Secure Switch, the Secure Switch will perform a self-test on the following items to check the device's integrity and security functions.

- Firmware integrity
- Accessibility of internal memory of the micro-controller
- Key stuck test
- Anti-tampering test
- Port isolation test

► *Self-test process:*

- All Port LEDs will turn ON and then OFF one by one.
- When the self-test completes successfully, it will switch to Port 1, with the Port 1's LED turning GREEN.

► *Self-test failure:*

In case of self-test failure, the Secure Switch becomes inoperable, with the port LED(s) flashing, which indicates a potential cause to the failure.

- The pre-defined port LED status indicates the failure cause.
    - Button jammed: The port LED of a jammed button will flash green.
- When all port LEDs flash, it means the KVM tampering is detected or there is an integrity issue.

For security, the Secure Switch becomes inoperable after self test fails.

Please verify your KVM installation, pushbuttons, and then power cycle the Secure Switch. If the self-test failure remains, stop using the Secure Switch, remove it from service and contact your Raritan reseller.

► *KVM reset:*

This Administrator function allows the authorized Administrator to reset the KVM configuration to factory default. For actual instructions, refer to Reset to Factory Default (on page 19) in the Administrator Functions Section.

Manual Switching

For enhanced security, the Secure Switch offers manual port switching only. This is achieved by pressing the port-selection pushbuttons located on the Secure Switch’s front panel.

Press and release a port-selection pushbutton to select the corresponding port where the desired computer is attached. For information on port IDs, see: Port ID Numbering (on page 13). To meet maximum security and channel isolation requirements, control of the keyboard, mouse, video, audio, and USB CAC reader will be switched together.

The selected port's LED turns GREEN to indicate that the connected keyboard, mouse, monitor, speakers (or headset), and CAC reader are redirected to the computer attached to the corresponding port. The selected computer should be able to detect the peripherals after port switching.

If the computer fails to detect your keyboard, mouse, or CAC card reader, check the following:

- Verify if you are using a supported keyboard, mouse, or CAC card reader. See: Using Qualified Peripheral Devices Only (on page 8) and Supported Card Readers (on page 10).
- Verify if your keyboard, mouse, or CAC reader fails to operate properly.
- For USB CAC card reader (USB authentication device), verify the USB CAC cable has been securely connected, and the CAC function is enabled.
- For USB CAC card reader port, verify if the device you use has been authorized. See: Supported Card Readers (on page 10) or consult your administration.

Port ID Numbering

Each KVM port on the Secure Switch is assigned a port number. 1 and 2 for 2-port models, 1 to 4 for 4-port models, and 1 to 8 for 8-port models. The port numbers are marked on the rear of the Secure Switch. See Secure Switch Ports and Connectors.

The port ID of a computer is derived from the KVM port number it is connected to.

LED Indicators

In addition to the power LED, there are port LEDs and CAC LED on the Secure Switch's front panel to indicate Port / CAC reader operation status. These LEDs also serve as the alarm notification for KVM security issues.

LED	Indication
Power LED	The power LED is on the front panel and becomes lit (white) to indicate that the Secure Switch is powered on.

Port LED	The port LEDs are located on the front panel to indicate the port selection or computer connection status. - *Online* – Lights up in WHITE to indicate that the computer attached to its corresponding port is up and running. - *Selected* – Turns GREEN to indicate that the computer attached to its corresponding port has the KVM focus. Note: Port LEDs will flash constantly when a chassis intrusion is detected. For details, see Chassis Intrusion Detection (on page 14). Port LEDs also indicate the status of the Secure Switch's self-test status. For details, see Operation (on page 12).
CAC LED	The CAC LED is located on the front panel to indicate CAC reader selection or connection status. - *Green LED*: A supported USB authentication device is connected. - *Green LED Blinking*: The connected USB device is rejected, such as a USB thumb drive, USB camera, and so on
CAP NUM PWR LED	CAP: The LED is lit (Green) to indicate that Caps Lock Function has been turned on. NUM: The LED is lit (Green) to indicate that Num Lock Function has been turned on. PWR: The LED is lit (Green) to indicate that the Secure Switch is powered on
Video LED(s)	This Video LED(s) lights green when the video connection is up and running. The LED flashes when a non-qualified monitor is connected. Note: With the dual-display model, each console video connection has a video LED

Chassis Intrusion Detection

To help prevent malicious tampering with the Secure Switch, when a chassis intrusion, such as the cover being removed, is detected, the Secure Switch becomes inoperable, and front panel LEDs flash GREEN continuously.

The Chassis Intrusion Detection is an always-on function. If all your front panel LEDs flash continuously, or the Secure Switch's enclosure appears breached, DO NOT use this product and contact your Raritan dealer immediately.

Administrator Functions

The Secure Switch's Administrator Functions allow authorized Administrator to configure this product, configure user authentication device filtering, and audit log data generated by the Secure Switch.

- Log data audit:

  Log data generating and recording is activated when the Secure Switch is manufactured, and cannot be disabled or erased. The Secure Switch's Administrator Functions allow authorized Administrator to download, view, and audit important log data and events.
- User Authentication Device and HID Device filtering configuration:

  This function enables authorized Administrator to assign Allowlist and Blocklist for the User Authentication Devices, and a blacklist for HID devices.
- Secure Switch's configuration:

  This function enables authorized Administrator to perform functions like "Reset to Factory Default."
- The "Reset to Factory Default" command:

  This command clears Allowlists/Blocklists with both Administrator Functions and Port Authentication Utility.

Administrator must first log in and be authenticated for the Secure Switch Administrator Functions. To maximize security, Administrator must set a new password after the first successful login, before performing other administrative functions. Note that the Administrator password can be changed anytime via Administrator Configuration.

In This Chapter

Installation for Administrator Logon

Administrator must log on and be authenticated for the Secure Switch administrative operations. This section helps you set up the installation for Administrator Logon.

1. Connect a qualified Keyboard, Mouse, and Display to the Secure Switch's User Console section.

Refer to the Secure Switch User Guide for details.

2. Connect a secure computer to Port 1 of the Secure Switch KVM Port section via a Secure Switch KVM cable. The USB cable connected to that computer for Keyboard / Mouse must be plugged into the Secure Switch's KVM USB Port.

Refer to the Secure Switch User Guide for details.

3. First power on the Secure Switch, and then the computer. The Secure Switch will switch to Port 1 after KVM self-test completes successfully.

Administrator Logon

After Installation for Administrator Logon (on page 15),

1. Open a text editor on the connected computer.
2. Use the console keyboard for the following procedure:
    a. Press and hold down the [Ctrl] key, and then press the [F12] key.

       Ctrl + F12

    b. Release the [Ctrl] and [F12] keys.
    c. Press the [L] key. Then press [Enter].

       After successful input of the key sequence, you will enter the Administrator Logon mode and be prompted for authentication in the text editor.
3. In the text editor, you will be prompted for the default Administrator password.

ATTENTION:
-- The default Administrator password is used for the first-time Administrator Logon only.
-- To maximize security and to prevent unauthorized access to Secure Switch, change the default logon password after your first successful logon. Once changed, the default Administrator password CANNOT be restored with Reset to Factory Default.

---

4. The default Administrator password for the first-time logon is:

ABCD@xyz#2468!

- The password is case-sensitive.
- Press the [Shift] key for uppercase letters and special characters.

5. A [Logon OK] message appears when the password input is correct. If the password input is wrong, you will be prompted for password input again.
    a. If logon attempts fail for 3 times, the Administrator Logon mode will be terminated automatically. Access to the Administrator Logon mode will be blocked for 15 minutes.
    b. If logon attempts fail for 9 times, the Secure Switch becomes inoperable permanently. Remove it from service immediately and contact your Raritan dealer.
6. After the [Logon OK] message appears, type the command "LIST" and press [Enter] for Administrator Functions.
    - The command "LIST" displays Administrator Functions.
7. For maximum security, Administrator must change the Administrator Logon password via Administrator Functions after the first successful logon. The new password should comprise:
    - 8 to 22 characters in length
    - A minimum of 1 lowercase letter
    - A minimum of 1 uppercase letter
    - A minimum of 1 numeric character
    - A minimum of 1 special character

    DO NOT use the default Administrator password as your new password. Administrator will be prompted for entering the new password again for confirmation.

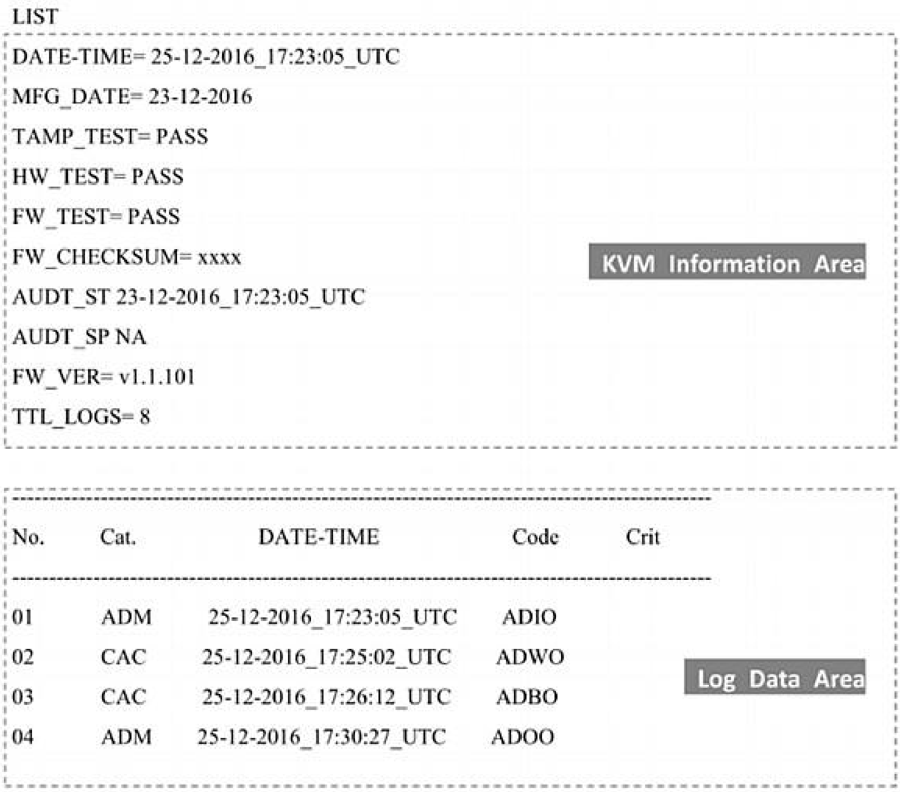
    After the new Administrator Logon password is set, the default Administrator Logon password will NOT be restored even with the "Reset to Factory Default" command.

Log data audit

Log data recording is activated when the Secure Switch is manufactured, and cannot be disabled or erased. After the successful Administrator Logon, type the command [LIST] to view logs data in the text editor.

- The command "LIST" displays Administrator Functions.

```
Administrator Logon Mode
ID: Administrator
Please enter password: ********
Logon ok.
```



```
LIST
DATE-TIME= 25-12-2016_17:23:05_UTC
MFG_DATE= 23-12-2016
TAMP_TEST= PASS
HW_TEST= PASS
FW_TEST= PASS
FW_CHECKSUM= xxxx
AUDT_ST 23-12-2016_17:23:05_UTC
AUDT_SP NA
FW_VER= v1.1.101
TTL_LOGS= 8

------------------------------------------------------------------------
No.     Cat.          DATE-TIME              Code      Crit
------------------------------------------------------------------------
01      ADM     25-12-2016_17:23:05_UTC      ADIO
02      CAC     25-12-2016_17:25:02_UTC      ADWO
03      CAC     25-12-2016_17:26:12_UTC      ADBO
04      ADM     25-12-2016_17:30:27_UTC      ADOO
```

```
Operation ok
```

For the menu interface information, refer to Raritan's PP4.0 Secure Switch Admin Log Audit Code Document.

Note: Secure Switch users do not need the Admin Log Audit Code Document for proper operations. Besides, this document is provided only when Raritan approves.

► *KVM Information Area*

This area displays the Secure Switch's status and critical information.

- DATE-TIME: Current Date and Time in UTC.
- MFG_DATE: Manufacturing Date (in UTC) of the Secure Switch.
- TAMP_TEST: The Secure Switch's Tamper protection test status.
- HW_TEST: The Secure Switch's hardware self-test status.
- FW_TEST: The Secure Switch's firmware self-test status.
- FW_CHECKSUM: The Secure Switch's firmware checksum for firmware integrity check.
- AUDT_ST: Date and Time (in UTC) when the Secure Switch activates all protection mechanism and starts generating log data.
- AUDT_SP: "NA" will be displayed if the Secure Switch functions properly.

  If events that trigger the Secure Switch protection mechanism are detected, and make the Secure Switch shut down and become inoperable, a Date/Time log will be recorded for the Secure Switch manufacturer.

  This particular Date/Time log can be decoded by the Secure Switch manufacturer only.
- FW_VER: Firmware version.
- TTL_LOGS: Total numbers of Log data.

► *Log Data Area*

The Log Data Area is an area where critical and non-critical Log data can be displayed. Each Log/Event is recorded with data like Date, Time and special codes to indicate the type and content of the event. These special codes can only be decoded and interpreted by the Secure Switch manufacturer.

- Critical Log Data: Critical Log Data includes the following events.
  - *Administrator Logon events -- up to four events*
  - *Administrator password change events -- up to two events*
  - *Critical Administrator KVM configuration -- one event*
  - *Self-test / Tampering events -- up to five events*

    The last one of Critical Log data will be kept for audit. That means New Critical Log events will overwrite the old Log data while still keeping the last one record.
- Non-critical Log Data: Non-critical Log Data includes the following events.
  - *Administrator Logon records, including Administrator login and log-off events*
  - *Administrator password change events*
  - *Administrator configuration events*
  - *Device filter configuration events*
  - *Self-test events, and power cycle events*

    A maximum of thirty-two Non-critical Log Data logs will be logged in the Secure Switch. The new log entry 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 Administrator to configure device filtering (CDF).

This function allows the Administrator to configure the Secure Switch to accept or reject specific USB devices (for CAC Port), and reject specific HID devices (for Keyboard / Mouse Ports). CAC Port device filtering can also be configured via Raritan's Port Authentication Utility. For detailed information on port authentication utility, refer to Raritan's Port Authentication Section in this Administrator Guide.

Note:

1. The CAC port does not support USB hub. The USB hub cannot be added to allowlist/blocklist via either administrator functions or ATEN Port Authentication Utility.

2. The user can only blocklist an HID device within the default HID devices* for the Keyboard/ Mouse Ports. Please connect the HID device (you would like to blocklist) 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 blocklisted HID device will be rejected by both Keyboard/ Mouse Ports. A USB hub cannot be added to blocklist via administrator functions.

* The default HID devices for Keyboard/ Mouse Ports could be referred to “Using Qualified Peripheral Device Only” - “USB keyboard and mouse” section on page 9.

Reset KVM to Default (Restore KVM to Factory Default)

This Administrator Functions enable the authorized Administrator to reset the Secure Switch's configuration to factory default.

1. When Administrator performs Reset KVM to Default, settings previously configured by Administrator, such as USB device's blocklist/allowlist, will be cleaned and reset to factory default settings.
2. Once the operation of Reset KVM to Default is completed, the Secure Switch will terminate the Administrator Logon mode, purge keyboard/mouse buffer, and power cycle the Secure Switch automatically.

After a successful self-test, KVM port focus will be switched to Port 1, and CAC function of each port will be reset to factory default (enabled).

3. Reset to Factory Default will NOT affect or erase Log data.
4. Reset to Factory Default will NOT affect previously-changed Administrator password.
5. Reset to Factory Default will clear the blocklist/allowlist created by both the Secure Switch's Administrator Functions and Raritan's Port Authentication Utility.

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

Reset The Secure KVM Switch (Reboot the Secure KVM Switch) action does not reset the administrator configuration, such as USB device's blocklist/allowlilst to the factory default settings. Please refer to Reset KVM to Default Section for more details.

1. Press the Reset button on the front panel for more than 5 seconds to reset a Secure Switch.
2. When performing reset to Secure KVM Switch, Keyboard/Mouse buffer will be purged and the Secure Switch will reboot and perform self-test.
3. After a successful self-test, KVM port focus will be switched to Port 1, and CAC function of each port will be reset to factory default setting (enabled).
4. If the Secure Switch fails to generate video on the monitor after reset, power off the installation, check the installation, and follow the operation instructions in the Secure Switch User Guide to power on the installation.

Port Authentication Utility

The Raritan Secure Switch offers a Port Authentication Utility to allow authorized administrator to configure the Secure KVM to accept or reject specific USB devices. Through secured access and authentication process, device filtering can be done through the Port Authentication Utility. Administrators can create a list and add to Blocklist/Allowlist to the USB CAC Port filter which by default supports a USB Smartcard or a CAC reader as authentication device.

The Allowlist/Blocklist assigned by the Secure KVM Administrator Functions has higher priority over the lists by the Port Authentication Utility. Please refer to the Raritan Secure KVM Administrator Guide for detail.

When a device is assigned to both Blocklist and Allowlist area in Port Authentication Utility, the device will be treated as Blocklisted. (Device filtering rule by Blocklist has always the highest priority).

Reset to Factory Default is the only method to completely clear the filtering lists on the KVM switch.

In This Chapter

Setup Port Authentication Utility

Only authorized administrators are allowed to install and operate Port Authentication Utility. The Raritan Port Authentication Utility supports Microsoft Windows 8 and higher versions.

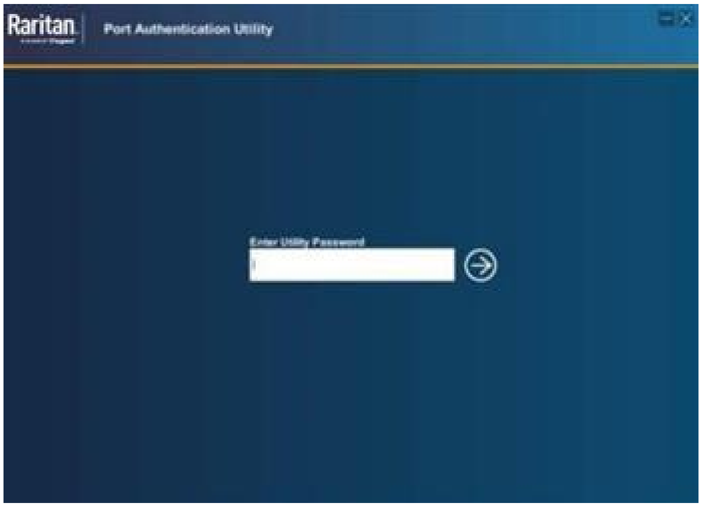
► *Steps to install*

1. Install the Raritan Port Authentication Utility to a secure source computer following the Installation Wizard. This secure source computer is for management only, and has its own monitor, keyboard, and mouse connected for installation and operation. Power off the source PC after Port authentication Utility installation.
2. Connect the qualified monitor, keyboard and mouse to the Raritan Secure KVM console section. Please refer to the Secure KVM User Guide for details.
3. Connect to the above secure source computer to Port 1 of the Secure KVM KVM Port section via the USB B-to-A cable of the KVM cable sets.
4. Turn on power of the Raritan Secure KVM first, and then the source computer. The Raritan Secure KVM will switch to Port 1 after a successful KVM self-test.
5. Use the monitor, keyboard, and mouse by the source computer to operate the Raritan Port Authentication Utility.

Set Password

Open the Port Authentication Utility installed on the secure source computer.

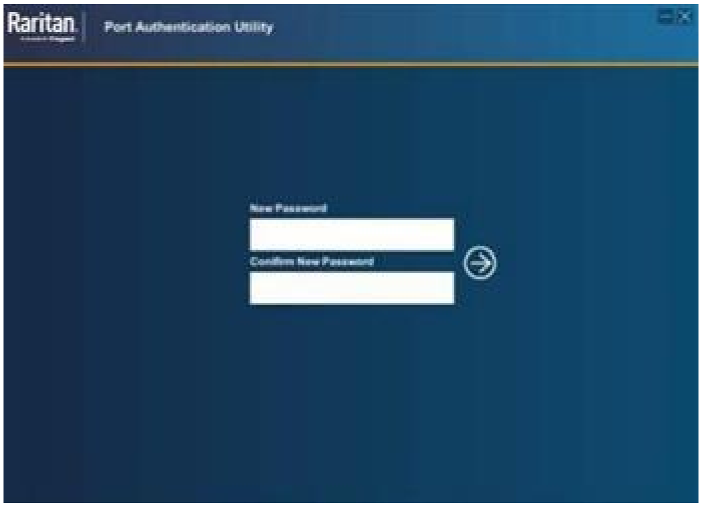
1. First time you will be prompted to enter the default password (abcd@XYZ#1357! (case sensitive)).



2. You will be forced to change the password. A strong password of 8 to 22 characters in length, should have 1 lower case letter, 1 upper case letter, 1 numeric character, and 1 special character.

Do not use the default password for your new password.

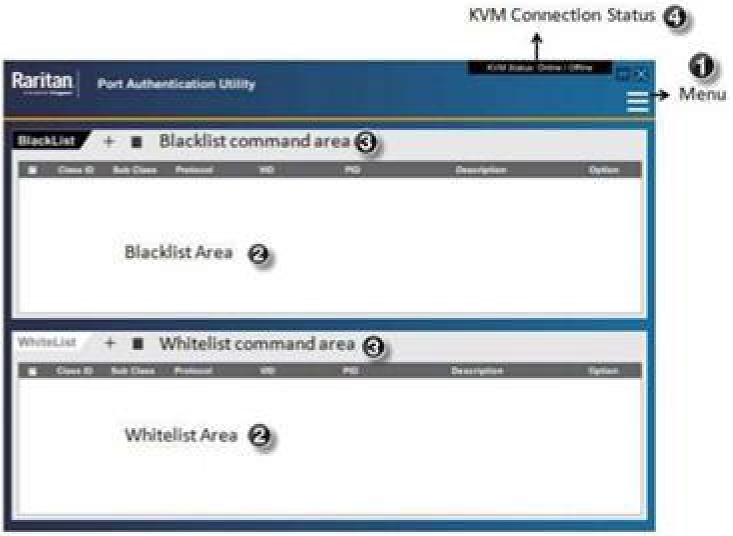
This password is for Port Authentication Utility only. Do not use the same password for Administrator Logon functions.

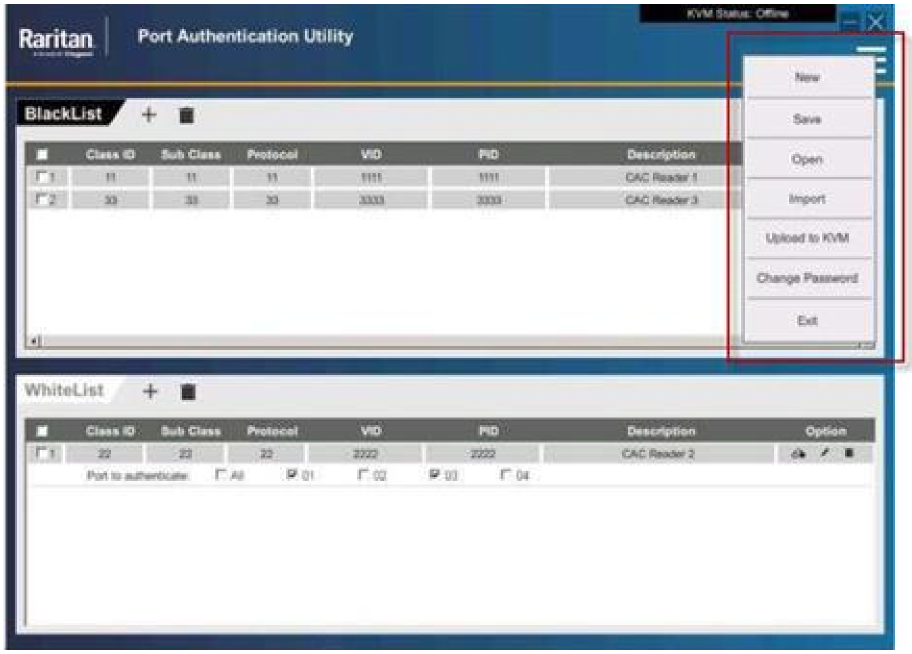


Operation Interface

After the new password has been confirmed, you will be prompted to create a new filter list or open an existing filter list.

The operation interface allows you to add, remove, or edit filtering rule entries to the Blocklist or the Allowlist.





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

❶ Menu: Menu offers options to create new Blocklist/ Allowlist filter, save an edited filter, open/import an existing filter in source computer, update the Secure KVM filter and change password.

❷ Blocklist /Allowlist Area: Filtering rules added to the Blocklist/Allowlist will be displayed in these areas.

❸ Blocklist/Allowlist command area: Click on"Add" and "Delete" icons to add a new rule or delete a selected rule from the BlacklList/Allowlist area.

❹ KVM connection status: This area shows the KVM connection status

► *To add a new filtering rule:*

Manual addition

To add a new filtering rule to the Blocklist, click on the "+" icon in the Blocklist command area, and choose "Manual Input" from the drop-down menu to edit a filtering rule. Enter values for Class ID, Sub Class, Protocol, VID, and PID field. A wild-card character asterisk "*" can be used in the field to represent one or more other characters.

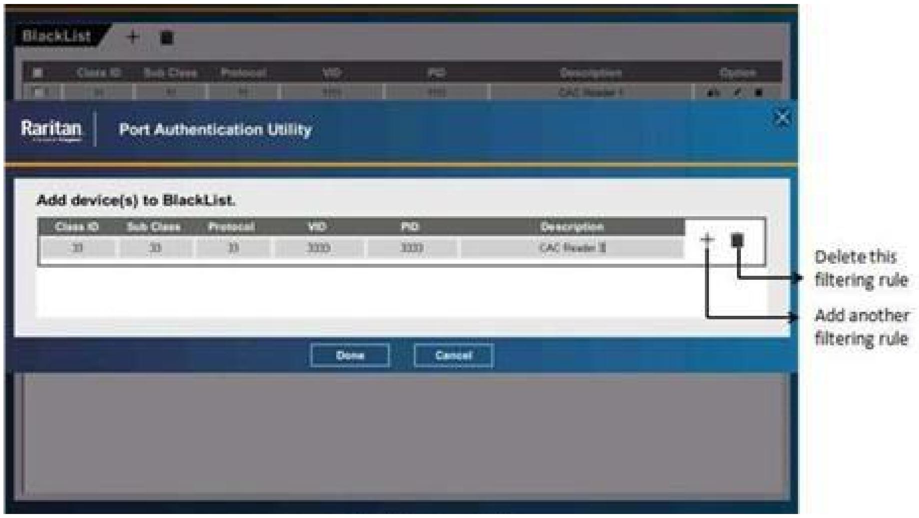
For example:The filtering rule below includes all the devices whose PID starts with number 5 or

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

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

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

A short description can be added to Description field to describe the device. After finishing a filtering rule entry, click the "+" icon on the right to add another filtering rule. Click on the recycle bin icon to discard an entry. Click "Done" button after editing all the entries. The added filtering rule will be added to Blocklist area.

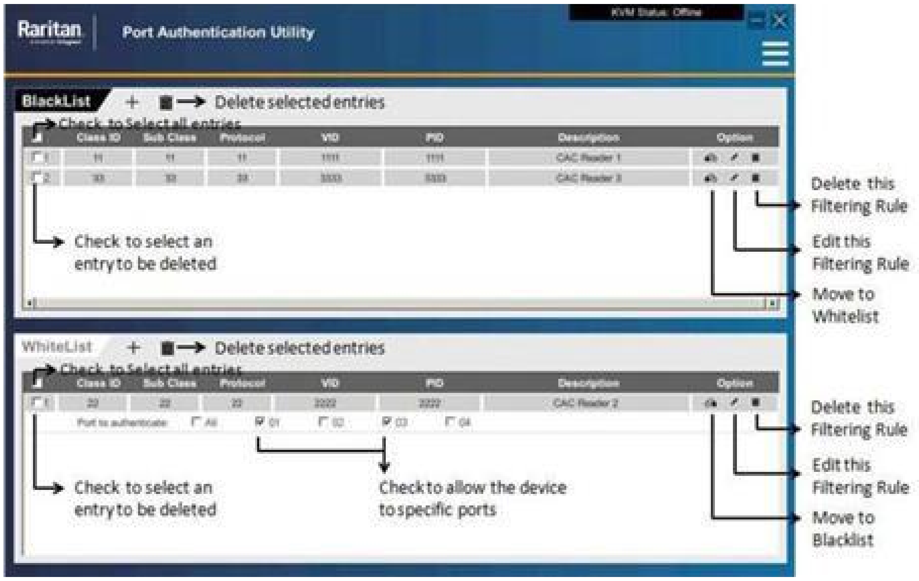


BlackList
Raritan
Port Authentication Utility
Done
Cancel
Delete this filtering rule
Add another filtering rule

Add device(s) to BlackList.

Class ID	Sub Class	Protocol	VID	PID	Description
33	33	33	3333	3333	CAC Reader 3

The filtering rules listed in the Blocklist area can be edited, deleted, or moved to the Allowlist and vice versa.



Raritan
Port Authentication Utility
KVM Status: Offline
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

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

A maximum of 32 filtering rules can be added to the Blocklist, and another 32 filtering rules can be assigned to the Allowlist.

Note: If a device is added to the Blocklist, it will be blocked from all Secure KVM ports.

If a device is added to the Allowlist, it can be allowed to the assigned ports.

Blocklist filtering rules always supersede the Allowlist filtering rules.

Retrieve from the device

Retrieve USB device value from the device on the Secure KVM USB CAC Port. In addition to manually typing the value for each filtering rule, you can retrieve the USB device info from the USB device connected to the Secure KVM USB CAC Port.

Connect the USB device to the Secure KVM USB CAC Port and use the Secure KVM console keyboard.

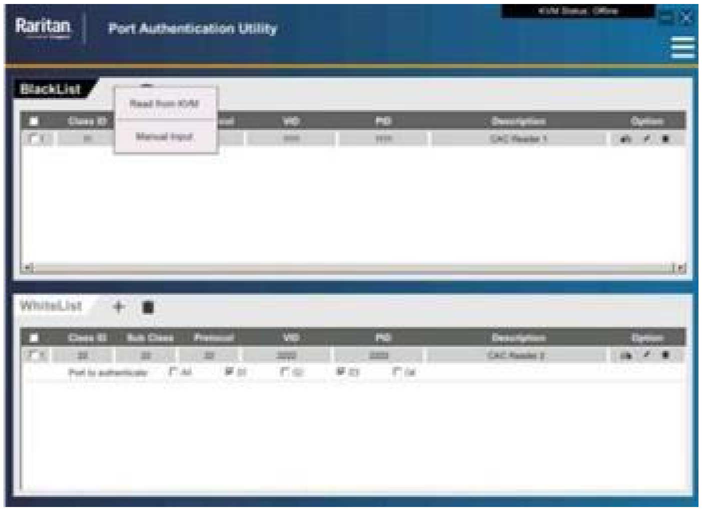
1. Press and hold down the Ctrl key
2. Press the F12 key ([Ctrl] + [F12])
3. Release the Ctrl and F12 key (First release the F12 key, followed by the Ctrl key), press [U] key, and then press [Enter]

The combination of key strokes enables the Secure KVM to be ready for you to retrieve the device info on USB CAC Port.

To add the values of USB device on USB CAC Port to filtering rules, click on the “+” icon in the command area, and choose “Read from KVM” from the drop-down menu. You will be prompted to login. Upon successful login values of USB device on the Secure KVM USB CAC Port will be displayed in the filtering rule area.

The session terminates automatically after the value of the device on the Secure KVM USB CAC Port is successfully retrieved.

Note: The session will be terminated and blocked for 15 minutes after 3 failed attempts to log on.



► *To edit existing filtering rule:*

You can edit filtering rules to block (Blocklist) or to allow (Allowlist) specific USB devices connected to USB CAC Port of the Secure KVM. A filtering rule is defined by USB (Base) Class ID, Sub-Class, Protocol, VID (Vendor ID), and PID (Product ID) of a USB device. For example, a Base Class ID of a Smart Card device is 0Bh. By completing the Class ID, Sub-Class, Protocol, VID and PID field of a filtering rule, you can assign this filtering rule to the Blocklist or Allowlist to block or allow a USB device.

Base class	Sub class	Protocol	Device
0Bh	xxh	xxh	Smart Card device

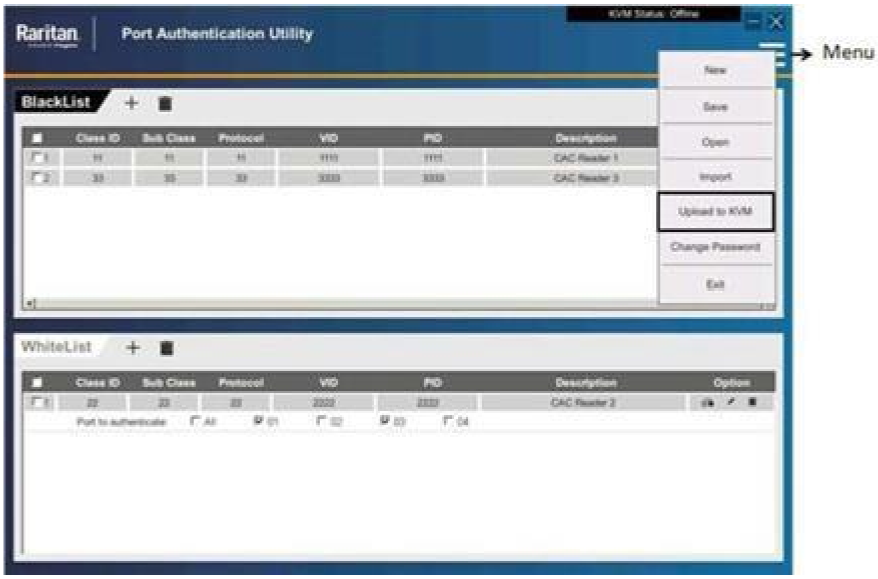
Note: When adding the value to Class, Sub-Class, Protocol, PID or VID field, the last digit “h” can be ignored. For example, when adding “0Bh” to the Class ID filed, just type “0B”

► *To upload filtering list:*

Before uploading the edited filtering list, you must make the Secure KVM ready for connection. Use the Secure kvm console keyboard as follows:

1. Press and hold down the Ctrl key
2. Press the F12 key ([Ctrl] + [F12])
3. Release the Ctrl and F12 key (First release the F12 key, followed by the Ctrl key), press [U] key, and then press [Enter]

Choose the "Upload to KVM" option from the drop-down Menu. After providing the correct credentials the list will be uploaded to the Secure KVM. The Secure KVM will allow or block USB devices on USB CAC Port based on the updated Blocklist/AllowLlist. The session terminates after the filtering list is updated.



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

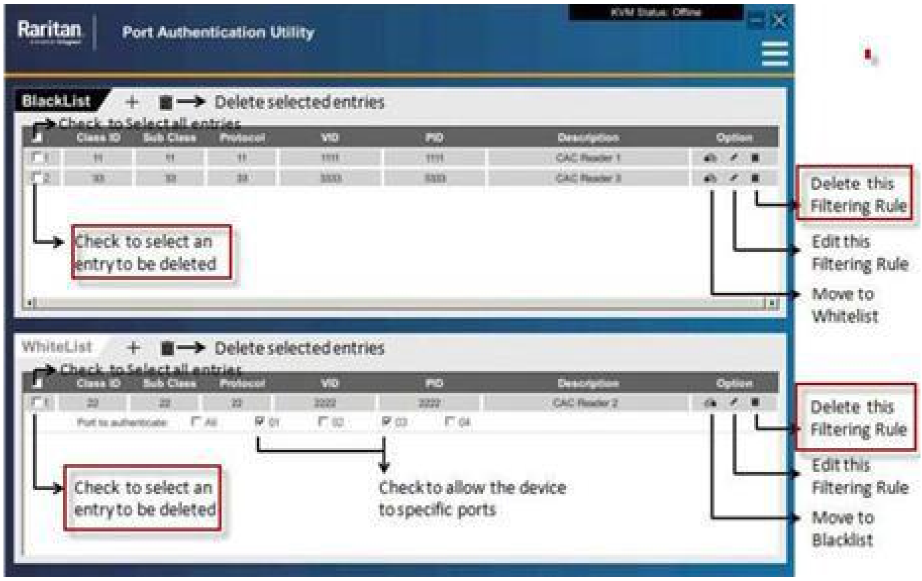
☐	Class ID	Sub Class	Protocol	VID	PID	Description	Option
☐ 1	22	22	22	2222	2222	CAC Reader 2	

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

To make the updated filtering list take effect, remove the Secure KVM from the installation and power cycle the Secure KVM.

► *To delete filtering rule:*

To delete a filtering rules from the Blocklist/Allowlist area, select the rule and click delete.


Raritan
Port Authentication Utility
KVM Status: Offline
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

	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	

	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

► *To exit the port authentication utility:*

Choose the "Exit" option in the drop-down menu to exit Port Authentication Utility.

Administrator Log Audit Code

- Basic Administrator Logon Functions has been described in the Administrator Guide.
- Details of Administrator Functions will be available only to Raritan Secure KVM Customers, rather than to the general public
- Some special Log/Event data logs (such as KVM shut down due to tampering, KVM locked) can only be decoded by the Secure KVM Switch manufacturer*

► *Notes*

* The following audit codes are generated which result in the Secure KVM Switch becoming inoperable. These Log/Event data logs can only be decoded by the Secure KVM Switch manufacturer. •

ADML – KVM locked due to Administrators' failed login

IHWN – H/W integration test failed

SUMN – Checksum test failed

MEMN – Memory test failed

ISON – Self-test port data check failed (different from jammed button BTNJ)

TMPH – Anti-Tamper triggered

TMPR – Anti-Tamper triggered by RSS4-WPS (Remote Port Selector)

In This Chapter

How does the Administrator Logon Function work?

After the authorized Administrator successfully logs on to the Secure KVM, the Secure KVM will dump the necessary information (text only) in the text editor previously opened in authorized Administrator's management computer.

All Administrator configuration options will be displayed in text editor upon Administrator's key command stroke.

If the Administrator choose an option, the result of execution will also be displayed in text editor

If the Administrator chooses to display available logs to audit, those logs will be displayed in text editor.

Format of Information Displayed in Text Editor

```
Administrator Logon Mode

ID: Administrator

Please enter password: ********

Logon ok.

LIST

DATE-TIME= 25-12-2016_17:23:05_UTC

MFG_DATE= 23-12-2016

TAMP_TEST= PASS

HW_TEST= PASS

FW_TEST= PASS

FW_CHECKSUM= xxxx

AUDT_ST 23-12-2021_18:23:07_UTC

AUDT_SP NA

FW_VER= v1.1.101

TTL_LOGS= 8

-----------------------------------------------------------------------------------------------

No. Cat. DATE-TIME Code Crit

-----------------------------------------------------------------------------------------------

01 ADM 25-12-2021_18:23:05_UTC ADIO

02 CAC 25-12-2021_18:25:02_UTC ADWO

03 CAC 25-12-2021_18:26:12_UTC ADBO

04 ADM 25-12-2021_18:30:27_UTC ADOO

Operation ok
```

Administrator Configuration Menu

This Administrator Configuration detail is available only to Raritan Secure KVM customers.

Administrator must press the number of an option to perform the configuration.

► *Example:*

If Administrator wants to audit logs and events, Administrator presses “1” to access the 2nd Level of text menu. If Administrator presses “2” after the options of second level menu are displayed in the text editor, all critical logs and events will be displayed in the text editor.

► *Text Menu Levels and Options*

Text Menu Level 1	***Text Menu Level 2***
1. Show logs and events	***[1-2] Display logs & events. Please choose an option.***
	1. Show all logs & events
	2. Show critical logs & events
	3. Show non-critical logs & events
	7. Return
2. Configure CAC filter	***[2-2] Configure CAC filter of Admin session. Please choose an option***
	1. Allow currently connected device on all Ports
	2. Block currently connected device on all Ports
	3. Show info of currently connected device
	4. Show info of all added devices*
	5. Reset Admin CAC Allow list
	6. Reset Admin CAC Block list
	Return
3. Configure KB_MS filter	***[3-2] Configure KB_MS filter of Admin session. Please choose an option***
	1. Block currently connected device on all Ports
	2. Show info of currently connected device
	3. Show info of all added devices
	4. Reset Admin KB_MS Block List
	7. Return
4. Change password	***[4-2] Change Admin password. Please choose an option***
	1. Continue
	7. Return
5. Check FW version	***[5-2] FW version: vx.x.xxxx***
	7. Return

6. Reset KVM to Default	***[6-2] Reset KVM & CAC filter, & KB_MS filter to factory default. Please choose an option***
	1. Continue
	7. Return
8. Exit logon session	

► *Notes:*

* The “Show info of all added devices” option lists only devices added by the Administrator on the KVM switch through the Administrator Logon function. It does not show the devices Blocklisted or Allowlisted by the Raritan Port Authentication Utility.

** Only the HID devices plugged into the Secure KVM console mouse port can be blocked. Once a certain device is blocked, it will be blocked on both Secure KVM console keyboard and mouse ports.

Log/Event Audit code

This Administrator Configuration detail will be available only to Raritan Secure KVM Customers

Some special Log/Event data logs (such as KVM shut down due to tampering, KVM locked) can only be decoded by the Secure KVM Switch manufacturer.

Cat. (Category)	**Code**	**Description**	**Critical Event area**
ADM (Administrator Tasks)	ADIO	Administrator Login ok	
	ADIN	Administrator Login fail (Critical area keeps only the last Login fail event; This event will also be logged in Non-critical area)	Yes
	ADOO	Administrator Logout	
	ADIL	Administrator last login ok	Yes
	APIO	AP connection login ok for Blocklist/Allowlist update	
	APIN	AP connection login fail for Blocklist/Allowlist update (Critical area keeps only the last AP login fail event; This event will also be logged in Non-critical area)	Yes
	APOO	AP connection terminated	
	APIL	AP last connection Login ok	Yes

	PWCO	Administrator password change (Critical area keeps only the last password change event; This event will also be logged in Non-critical area)	Yes
	RSTO	Administrator performs Reset to Factory Default (Critical area keeps only the last Administrator Reset to Factory Default event)	Yes
	ADML	KVM locked due to Administrator’s failure attempts to login	Yes
CAC **(CAC related)**	ADCWO	Administrator changes CAC port Allowlist	
	ADCBO	Administrator changes CAC port Blocklist	
	APCTO	AP changed CAC port Blocklist/Allowlist	
	USBCO	USB CAC port accepted the connected device	
	USBCR	USB CAC port rejected the connected device	Yes
KM **(KB/MS Related)**	ADMBO	Administrator changed KB/MS ports Blocklist	
	USBMO	USB KB/MS ports accepted the connected device	
	USBMR	USB KB/MS ports rejected the connected device	Yes
VI	VIO	Console video port accepted the conneted device	
	VIR	Console video port rejected the connected device	Yes
RPS **(RSS4-WPS Remote Port Selector Related)**	RPSO	This event will be logged when RPS_TEST=PASS	
	RPSR	This event will be logged when RPS_TEST=REJ or connecting the Remote Port Selector (RSS4-WPS) to KVM after KVM is powered on (This event will also be logged in non-critical area.)	Yes
TST* **(KVM Test related)**	IHWN	H/W integration test Fail.	Yes
	SUMN	checksum test Fail	
	MEMN	Memory Test Fail	
	ISON	self test-port data check Fail	

	BTNJ	Button jam detected	
TMP **(Anti-tempering)**	TMPH	Anti-Tampering triggered.	Yes
	TMPR	Anti-Tampering triggered by RPS being tampered.	Yes
SYS **(KVM system)**	PWR	KVM Power Cycle	
	RST	Reset by Front Panel	

*For TST event, the secure KVM self-test includes the hardware integration test, firmware checksum test, memory test, port data test, and pushbutton jam test. Only Pushbutton could occur more than once.