Raritan Secure Switch

User Guide

Release 1.0

SecureSwitch-0A-v1.0-E
February 2018
255-80-0050-00 RoHS

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.

Contents

About This User Guide

This User Guide is intended for both system administrators and end users.

The guide helps you get the most from your Raritan Secure Switch system. It covers all aspects of installation, configuration and operation. An overview of the information available in the manual is provided below.

The following Raritan Secure Switch models and cables are covered in this guide.

Raritan Secure Switch models:

Configuration			2-port models	4-port models
PC video connection	Console video connection	CAC support		
DVI	DVI	Yes	RSS-102C	RSS-104C
		No	RSS-102	RSS -104

Raritan Secure Switch KVM cable:

The Raritan KVM cables that connect the Raritan Secure Switch to servers or computers are NOT shipped with the Raritan Secure Switch. You must purchase them separately.

KVM cable	Description
DVI-to-DVI cable	Support DVI video, USB keyboard/mouse and analog audio. ▪ Raritan Part Number **RSS-CBL-DVI**

Where to download manuals:

1. Visit the Raritan Secure Switch's support page on the Raritan website.
   https://www.raritan.com/support/product/raritan-secure-switch
2. There are two guides available on this web page. Click the one you want to download.
   - User Guide
   - Administrators Guide

Note: The port authentication utility for Raritan Secure Switch and this utility's documentation are NOT available on the website because they are provided only to customers who obtain official approval from Raritan.

Attention

Read the following sections before operating the Secure Switch.

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.

Convention of the User Guide

Convention	Description
Note or **Notes**	Additional information for users' reference.
Important	Important information that users must pay attention.
1. Numbered data	Step-by-step instructions.
• Bulleted list	Non-procedural information.

Chapter 1 Introduction

In This Chapter

Overview

Raritan Secure Switch series is NIAP-certified and compliant with NIAP PP 3.0 (Protection Profile for Peripheral Sharing Switch version 3.0) 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 v3.0 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 3.0 for Peripheral Sharing Switch (PSS).

Features

Features	Benefits
2- or 4-port Secure Switch with or without CAC feature	Reduce the costs involved in controlling up to 4 computers while offering data isolation between shared peripherals and computers.
Superior ultra-high video resolution -- up to 4K UHD	Support the resolution up to 3840 x 2160 @30Hz (4K UHD) with crystal clear image quality.
NIAP PP PSS v3.0 certified	Provide the most advanced security features required by the latest Protection Profile (PP) v3.0 for Peripheral Sharing Switch (PSS).
Pushbutton port selection and secure port switching	Port selection via pushbuttons only to enhance security. Keyboard, mouse, video, audio and CAC reader switch together for secure switching.
Channel isolation	Isolated channel per port makes it impossible for data to be transferred between computers.
Shared peripherals and computer isolation	USB keyboards/mice are supported. The always-on keyboard, mouse, and display EDID emulation ensures isolation between peripherals and connected computers.
Keyboard, mouse, and video EDID emulation	Keyboard, mouse, and EDID emulation ensures isolation between peripherals and connected computers.
Restricted USB connectivity	Non-authorized HIDs (Human Interface Devices) or non-predefined CAC will be rejected / ignored.
Unidirectional data flow	Secure design enables unidirectional data flow between devices and connected computers.

Features	Benefits
Support analog audio	Only standard *analog* speakers or headphone *without line-in or microphone* are supported.
Chassis intrusion detection	If the cover is removed from the Secure Switch, the device becomes inoperable and front panel LEDs flash. ▪ When this occurs, contact Raritan Technical Support.
Clear keyboard buffer on port switching	Keyboard data buffer is automatically purged when switching between KVM ports.
Tamper-proof hardware	All integrated circuits are soldered directly to the circuit board to prevent tampering with the components.
Tamper-evident tape	Provide a visual indication of any attempt to gain access to the switch's internal components.
Firmware non-reprogrammable	Prevent tampering and attempts to reprogram the switch's firmware.
Metal enclosure	Rugged metal enclosure.

Product Photos

RSS-102C is functionally identical to RSS-104C, and RSS-102 is functionally identical to RSS-104. The only difference is that RSS-102C and RSS-102 have only two channels while RSS-104C and RSS-104 have four channels.

4-port Secure Switch with CAC (model: RSS-104C):

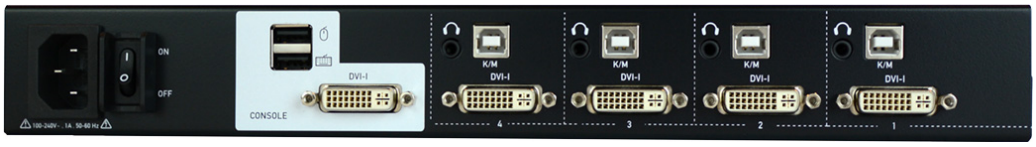
- Front View

- Rear View

4-port Secure Switch without CAC (model: RSS-104):

- Front View

- Rear View



Package Contents

A Raritan Secure Switch package consists of:

- 1 Secure Switch
- 1 power cord
- 1 user guide
- 1 warranty card
- 2 USB Type A-to-B cables for **RSS-102C**, or 4 USB Type A-to-B cables for **RSS-104C**

  (These USB cables are for card reader features so they are NOT available for RSS-102 and RSS-104.)

Note: Secure Switch KVM cables are NOT included with the Secure Switch. You must purchase them from Raritan separately.

Configuration Requirements

User Console Connection

Connect the following devices to the User Console on the Secure Switch. The video port on the User Console is DVI-I, supporting digital video.

- A DVI monitor capable of the highest resolution of any computer connected to the Secure Switch
- A USB mouse
- A USB keyboard
- Analog speakers or headphones (optional)
- A USB smart card or Common Access Card (CAC) reader (optional)

Important: Secure Switch does NOT support all USB keyboards or all card readers. For details, refer to *Using Qualified Peripheral Devices Only* **(on page 11).**

Connected Computers or Servers

The computers or servers to be connected to the Secure Switch must have the following ports and connectors.

- A DVI video output connector
- A USB Type A port for keyboard and mouse
- A USB Type A port for smart card or CAC reader (optional)
- A 3.5mm-jack audio port for speakers (optional)

Secure Switch KVM Cables

Raritan Secure Switch cables (DVI-to-DVI cable, Raritan Part Number **RSS-CBL-DVI**) are used to connect computers or servers to the Secure Switch. These cables support DVI video with USB for keyboard and mouse and analog audio.

The Raritan KVM cables that connect the Secure Switch to servers or computers are NOT shipped with the Secure Switch. You must purchase them separately.

Important: For security purposes, DO NOT connect any audio cable supporting Microphone audio input or Line in to the Secure Switch.

Operating Systems

It is suggested the connected computers (or servers) should only run one of the following operating systems.

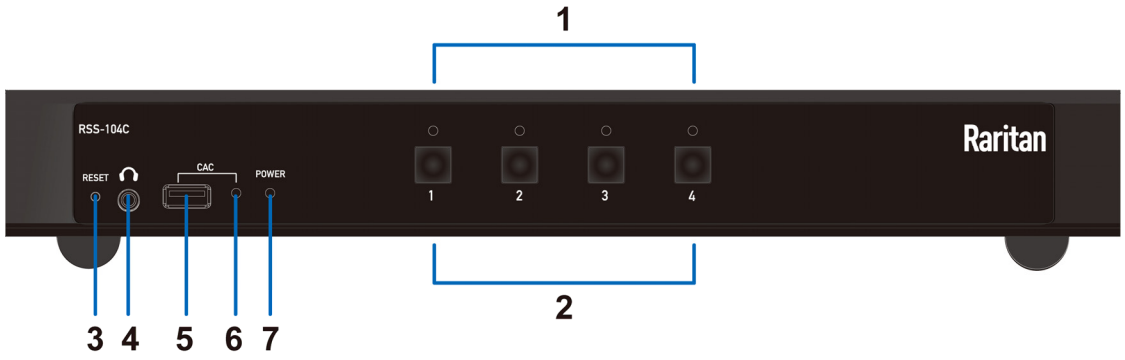
Operating system		Version
Windows		2000/XP/Vista/7/8/8.1/10
Linux	RedHat	6.0 and higher
	SuSE	8.2 and higher
	Mandriva (Mandrake)	9.0 and higher
UNIX	AIX	4.3 and higher
	FreeBSD	3.51 and higher
	Sun	Solaris 9 and higher
Novell	Netware	5.0 and higher
Mac		OS 9 and higher
DOS		6.2 and higher

Note: The Secure Switch also supports Linux Kernel 2.6 and higher.

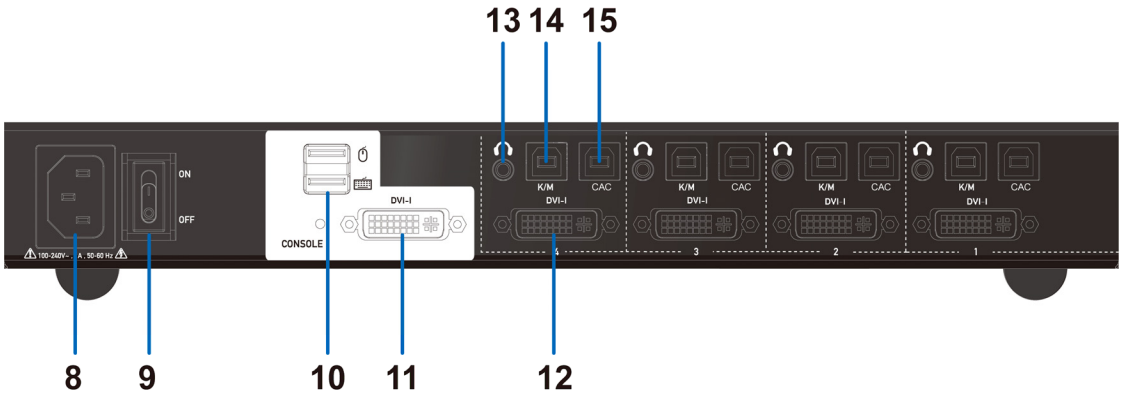
Secure Switch Ports and Connectors

The following diagrams illustrate the *RSS-104C* model, a 4-port USB DVI Secure Switch which supports CAC.

Front View



Rear View



No.	Components	Description
1	Port LEDs	The port LEDs, located on the front panel, indicate port selection or connection status. ▪ *Online state:* An LED is lit (WHITE) to indicate that the computer attached to the corresponding port is up and running. ▪ *Selected state:* An LED turns GREEN to indicate that the computer attached to the corresponding port is being accessed by the KVM console.
2	Port selection pushbuttons	Pressing a port selection pushbutton redirects the keyboard, mouse, video, audio, and optional CAC reader to the computer attached to the corresponding port.
3	Reset button	This button resets the Secure Switch. When performing the reset function by pressing this button for more than 5 seconds, the following will occur: ▪ The Secure Switch reboots and performs self-test. Port 1 will be selected by default after a successful self-test. ▪ The keyboard/mouse buffer is purged. ▪ Each port's CAC function will be reset to the factory default. *Note: If this product fails to display video on the monitor after reset, power off all devices, check the connections, and follow the installation instructions to power on all devices.*
4	Audio port	Connect optional speakers or headphones. ▪ Only standard analog speakers can be connected. ▪ Connection of an analog microphone or line-in audio equipment is NOT permitted.
5	USB port for a USB smart card reader or CAC reader	Only a supported USB authentication device, such as a standard smart card and CAC reader, can be connected to this port. ▪ This port is only available on RSS-102C and RSS-104C.
6	CAC reader LED	▪ A GREEN LED indicates a supported USB authentication device is connected. ▪ A RED LED indicates the connected USB device is improper and rejected, such as a USB thumb drive, USB camera, and so on.
7	Power LED	The LED is lit (WHITE) to indicate that the Secure Switch is powered on.
8	Power socket	Connect the AC power cord.

No.	Components	Description
9	Power switch	Power on and off the Secure Switch.
10	USB console ports	Connect a USB keyboard and mouse. The USB console's keyboard port (lower port) and mouse port (upper port) are only compatible with a standard USB keyboard and mouse. *Note: For security purposes, the Secure Switch does not support wireless keyboards and non-standard keyboards/mice with integrated USB features. Besides, this product does NOT support some functions on the keyboard. For details, refer to* **Using Qualified Peripheral Devices Only** *(on page 11).*
11	DVI-I console monitor port	Connect a DVI monitor using a user-supplied cable.
12	KVM DVI port	Connect the DVI connector of the Raritan Secure Switch KVM cable attached to your computer for video transmission.
13	KVM audio port	Connect the audio connector of the Raritan Secure Switch KVM cable attached to your computer for audio transmission.
14	KVM USB port	Connect the USB connector of the Raritan Secure Switch KVM cable attached to your computer for keyboard/mouse signal transmission.
15	USB-B port for a USB smart card or CAC feature	Connect a Type A-to-B cable attached to your computer for the USB Smart Card /CAC reader function. ▪ This port is only available on RSS-102C and RSS-104C.

Chapter 2 Hardware Setup

In This Chapter

Before You Begin

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

Tampering Prevention and Detection

- The Secure Switch includes 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 is 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 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 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.

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 or composite device functions
- 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.

Video:

- You can use a DVI monitor connected to the DVI-I port of the Secure Switch User Console.
- 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, refer to ***Supported Card Readers*** (on page 12).

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 in the Administrators Guide. Please review it before proceeding.

Secure Operation and Administration

Stacking

The Secure Switch features a rugged, metal enclosure which provides stability and allows the device to be stacked on the desktop.

It can be placed on any level surface that can safely support its weight and the weight of all attached cables.

Ensure that the surface is clean and free of materials that can block the exhaust vents or otherwise interfere with normal operation of the Secure Switch.

Installation Procedure

To install your Secure Switch system, power OFF all devices and then follow the procedure below, which corresponds to the numbers of the installation diagram following this topic.

Important: You CANNOT mix digital and analog video on a single Secure Switch. Make sure all devices connected to Secure Switch are DVI-video-based devices.

Read ***Secure Installation Guidelines*** (on page 13) before proceeding with the installation.

To connect all equipment:

1. Plug your USB keyboard and USB mouse into the USB User Console ports on the Secure Switch's rear panel.
   - Only a *standard* USB keyboard/mouse are supported. Refer to ***Using Qualified Peripheral Devices Only*** (on page 11).
2. Optionally connect your console monitor to the Secure Switch's console Video port on the rear panel, and then power on the monitor.
   - The connected monitor will be filtered after connecting it to the Secure Switch. An unsupported monitor will be rejected.
3. Plug your speakers into the console's speaker jack located on the Secure Switch's front panel.
4. Plug a Raritan Secure Switch KVM cable's DVI connector into the DVI port on one of the Secure Switch's KVM ports, and then plug the cable's USB and speaker connectors into the corresponding USB and speaker connectors.

   For the CAC feature, connect the Type B end of the USB Type A-to-B cable to the CAC port on one of the Secure Switch's KVM ports.

   Note: Secure Switch KVM cables are NOT included with the Secure Switch. You must purchase them from Raritan separately.
5. Plug the USB, video, and speaker connectors at the other end of the same Raritan Secure Switch KVM cable into their respective ports on the computer.

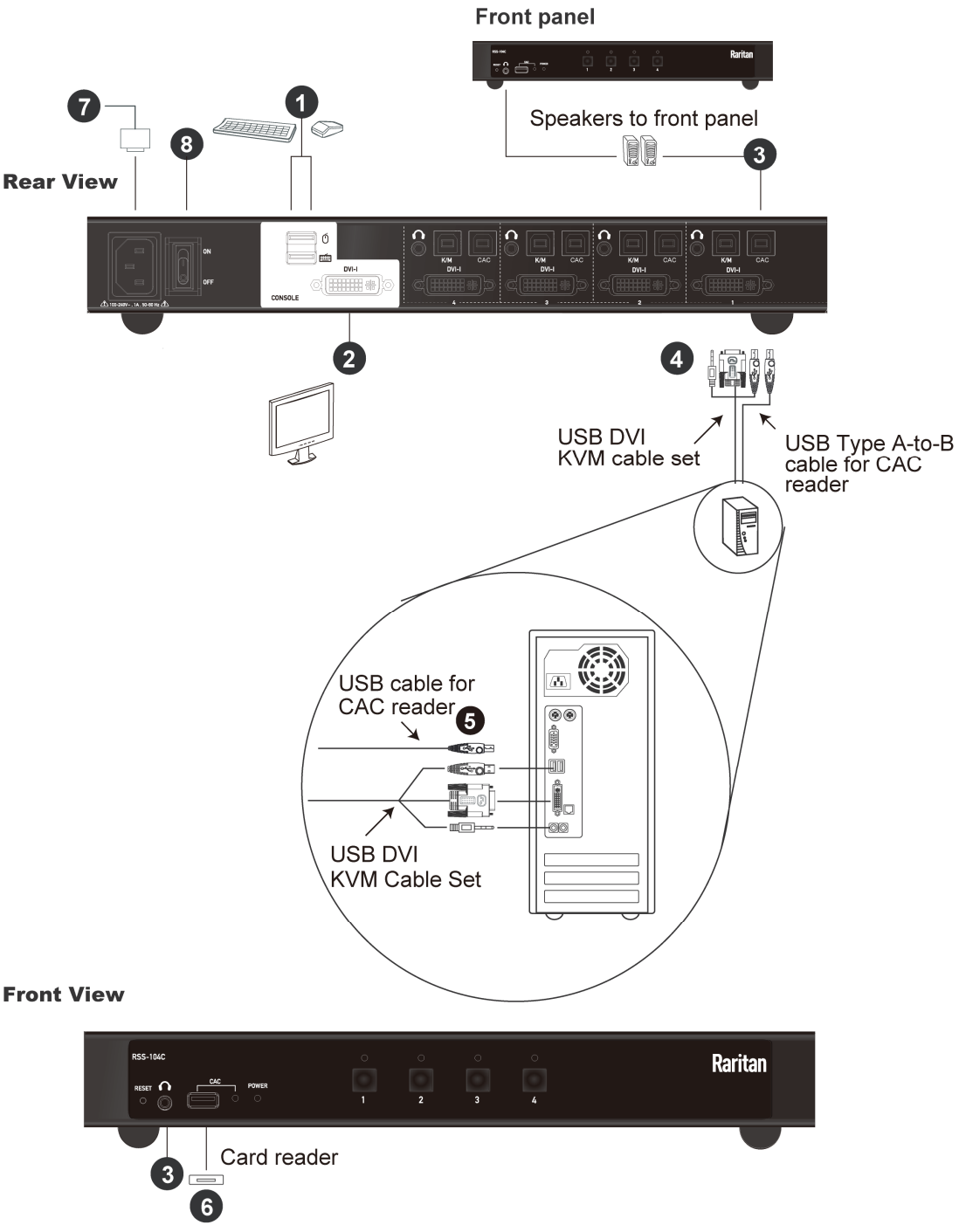
   For the CAC feature, connect the Type A end of the USB Type A-to-B cable to an available USB port on the computer.
   - Repeat steps 3, 4 and 5 for each computer you are connecting to the Secure Switch.
6. If you are installing a Secure Switch with CAC feature, connect the USB smart card / CAC reader to the CAC port on the Secure Switch's front panel.
   - Only appropriate supported USB Authentication devices, including smart card and CAC readers, can be connected to this port. During KVM operation, unsupported or unauthorized USB devices will be filtered and rejected, which is indicated by a flashing CAC LED. Refer to ***LED Display*** (on page 21) for visual indication.
   - For a list of supported USB smart card / CAC readers, refer to ***Supported Card Readers*** (on page 12).

- It is HIGHLY recommended to install the proprietary card reader driver onto the computer(s), which is shipped with the card reader or can be downloaded from the card reader vendor's website. Or the card reader may not function properly.

7. Plug the female end of the power cord into the Secure Switch's power socket, and plug the male end into an AC power source.
8. Turn on the Secure Switch and check that the LEDs light up. The Secure Switch will automatically start KVM self-test.

Note: The Secure Switch performs security self-test at power-on and at each power cycle. Front panel LEDs will indicate self-test status and test result. Refer to **Operation** *(on page 18) and* **LED Display** *(on page 21) for visual identification.*

Installation Diagram



Chapter 3 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 to check the device's integrity and security functions.

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.

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

The Secure Switch filters and emulates both the mouse and keyboard on each port after it is powered on. If the keyboard, mouse, monitor, or smart card / CAC reader fails to operate properly, make sure that you are using the appropriate peripherals that are supported and authorized peripherals. Then power off the Secure Switch, check all cable connections, and power on the device again.

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, refer to ***Port ID Numbering*** (on page 20). 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. Refer to ***Using Qualified Peripheral Devices Only*** (on page 11) and ***Supported Card Readers*** (on page 12).
- 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. Refer to ***Supported Card Readers*** (on page 12) 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, and 1 to 4 for 4-port models. The port numbers are marked on the rear of the Secure Switch. See ***Secure Switch Ports and Connectors*** (on page 7).

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

LED Display

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 21). Port LEDs also indicate the status of the Secure Switch's self-test status. For details, see* **Operation** *(on page 18).*
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. ▪ *Red LED*: The connected USB device is rejected, such as a USB thumb drive, USB camera, and so on.

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.

Appendix A Specifications

In This Chapter

Secure Switch Models without CAC

Function		RSS-102	RSS-104
Computer Connections		2	4
Port Selection		Pushbutton Switches (square-shaped)	
Console Ports	Keyboard	1 x USB Type-A F (Black)	
	Video	1 x DVI-I Dual Link F (White)	
	Mouse	1 x USB Type-A F (Black)	
	Audio/Speaker	1 x Mini Stereo Jack F (Black x 1; Front panel)	
Computer Ports	Keyboard/Mouse	2 x USB Type-B F (White)	4 x USB Type-B F (White)
	Video	2 x DVI-I Dual Link F (White)	4 x DVI-I Dual Link F (White)
	Audio/Speaker	2 x Mini Stereo Jack F (Black)	4 x Mini Stereo Jack F (Black)
Firmware Upgrade		NOT Supported	
Power		1 x 3-prong AC Socket	
LEDS	Power	1 (White)	
	On Line/ Selected	2 (Bi-Color LED): ▪ Online (White) ▪ Selected (Green)	4 (Bi-Color LED): ▪ Online (White) ▪ Selected (Green)

Function		RSS-102	RSS-104
Switches	Reset	1 x Semi-recessed Pushbutton	
	Power	1 x Rocker Switch	
KB/Mouse Emulation		USB	
Resolution		▪ DVI Dual Link: 2560x1600@60Hz; 3840x2160@30Hz ▪ DVI Single Link: 1920x1200@60Hz ▪ DVI-A: 2048x1536@60Hz	
I/P Rating		100–240VAC; 50/60Hz	
Power Consumption (watt)		3.6	4.3
Environment	Operation Temperature	0–40°C	
	Storage Temperature	-20–60°C	
	Humidity	0–80% RH, Non-condensing	
Certificates	Safety	UL, CB	
	EMC	CE/FCC/VCCI Class A	
Physical Properties	Housing	Metal	
	Weight (kg)	1.66	1.68
	Dimension (H X W X D) cm	4.45 x 33.66 x 15.24	4.45 x 33.66 x 15.24

Secure Switch Models with CAC

Function		RSS-102C	RSS-104C
Computer Connections		2	4
Port Selection		Pushbutton Switches (square-shaped)	
Console Ports	Keyboard	1 x USB Type-A F (Black)	
	Video	1 x DVI-I Dual Link F (White)	
	Mouse	1 x USB Type-A F (Black)	
	Audio/Speaker	1 x Mini Stereo Jack F (Black x 1; Front panel)	
Computer Ports	Keyboard/Mouse	2 x USB Type-B F (White)	4 x USB Type-B F (White)
	Video	2 x DVI-I Dual Link F (White)	4 x DVI-I Dual Link F (White)
	Audio/Speaker	2 x Mini Stereo Jack F (Black)	4 x Mini Stereo Jack F (Black)
	CCID/CAC Card Reader	2 x USB Type-B F (White)	4 x USB Type-B F (White)
Firmware Upgrade		NOT Supported	
Power		1 x 3-prong AC Socket	
LEDS	Power	1 (White)	
	On Line/ Selected	2 (Bi-Color LED): ▪ Online (White) ▪ Selected (Green)	4 (Bi-Color LED): ▪ Online (White) ▪ Selected (Green)
	CAC (For warning indication)	1 (Red/Green)	1 (Red/Green)

Function		RSS-102C	RSS-104C
Switches	Reset	1 x Semi-recessed Pushbutton	
	Power	1 x Rocker Switch	
KB/Mouse Emulation		USB	
Resolution		▪ DVI Dual Link: 2560x1600@60Hz; 3840x2160@30Hz ▪ DVI Single Link: 1920x1200@60Hz ▪ DVI-A: 2048x1536@60Hz	
I/P Rating		100–240VAC; 50/60Hz	
Power Consumption (Watt)		4.1	4.8
Environment	Operation Temperature	0–40°C	
	Storage Temperature	-20–60°C	
	Humidity	0–80% RH, Non-condensing	
Certificates	Safety	UL, CB	
	EMC	CE/FCC/VCCI Class A	
Physical Properties	Housing	Metal	
	Weight (kg)	1.66	1.68
	Dimension (H X W X D) cm	4.45 x 33.66 x 15.24	4.45 x 33.66 x 15.24

Appendix B Supported Protocols for Connection Ports

In This Chapter

Protocols for Console Ports

Secure Switch console ports support the following protocols. For the location of console ports, see ***Secure Switch Ports and Connectors*** (on page 7).

▶ Models with CAC: RSS-102C and RSS-104C

Video Output Interface			Keyboard		Mouse		Audio Output	CAC Reader
DisplayPort	HDMI	DVI-I	USB 1.1/2.0	PS/2	USB 1.1/2.0	PS/2	Analogue Audio output (Speaker)	USB 1.1/2.0
		Yes	Yes		Yes		Yes	Yes

▶ Models without CAC: RSS-102 and RSS-104

Video Output Interface			Keyboard		Mouse		Audio Output
DisplayPort	HDMI	DVI-I	USB 1.1/2.0	PS/2	USB 1.1/2.0	PS/2	Analogue Audio output (Speaker)
		Yes	Yes		Yes		Yes

Protocols for KVM Ports

Secure Switch KVM ports for connecting computers support the following protocols. For the location of this product's KVM ports, see ***Secure Switch Ports and Connectors*** (on page 7).

Models with CAC: RSS-102C and RSS-104C

Video Output Interface			Keyboard		Mouse		Audio Output	CAC Reader
DisplayPort	HDMI	DVI-I	USB 1.1/2.0	PS/2	USB 1.1/2.0	PS/2	Analogue Audio output (Speaker)	USB 1.1/2.0
		Yes	Yes		Yes		Yes	Yes

Models without CAC: RSS-102 and RSS-104

Video Output Interface			Keyboard		Mouse		Audio Output
DisplayPort	HDMI	DVI-I	USB 1.1/2.0	PS/2	USB 1.1/2.0	PS/2	Analogue Audio output (Speaker)
		Yes	Yes		Yes		Yes