Raritan Secure Switch

Administrator Guide

Release 1.0

SecureSwitch_admin-0A-v1.0-E
January 2018
255-80-0052-00 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

Chapter 1
Introduction....1
Overview....1
Administrative Functions....1
Chapter 2
Hardware Setup....2
Before You Begin....2
Tampering prevention and detection....2
Always use qualified and authorized peripheral devices....3
Secure Installation....3
Secure Administrative Operation....4
Chapter 3
Operation....5
Powering On....5
Manual Switching....6
LED Display....6
Chassis Intrusion Detection....7
Administrator Functions....8
Appendix....14

ATTENTION

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

If all your front panel LEDs flash continuously, or the switches' enclosure appears breached, avoid using this product and contact your dealer.

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

Image of Tamper-evident seal here

About This Administrator Guide

This Administrator Guide is intended for authorized Administrator.

This Administrator Guide is provided to help authorized Administrator to audit logs and configure the RARITAN Secure Switch. To maximize security, Administrator is advised to audit logs/events record and the Secure Switch configuration on a routine base.

This Administrator Guide covers the following Secure Switch's

Configuration			2-Port	4-Port
PC Video Connection	Console Video Connection	CAC Support		
DVI	DVI	w/ CAC Feature	RSS-102C	RSS-104C
		w/o CAC Feature	RSS-102	RSS -104

Chapter 1 Introduction

Overview

The Raritan Secure Switch series is NIAP-certified and compliant with NIAP PP 3.0 (Protection Profile for Peripheral Sharing Switch version 3.0) requirements, satisfying the latest security requisites 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, mouse, speakers, and CAC Reader) between multiple computers. Conformity with Protection Profile v3.0 certifies that other USB peripherals cannot be connected to the console ports of the Raritan Secure Switch, and that only a keyboard and mouse are accommodated, therefore providing high-level security, protection and safe-keeping of data.

The Raritan Secure Switch 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 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 Raritan Secure Switch series gives you the means to consolidate multiple workstations of various security classification levels with one keyboard, monitor and mouse (KVM) console.

Administrative Functions

To be complaint with Protection Profile 3.0 while providing higher deployment flexibility, wider product support for new authentication devices, and maximum security, the Raritan Secure Switch supports Administrative Functions. Through secured access, authorized Administrator can audit log data, configure the Secure Switch, and perform configurable device filtering.

Note:

1. The National Information Assurance Partnership (NIAP) is a United States government initiative to meet the security testing needs of IT consumers and manufacturers. It is operated by the National Security Agency (NSA) and the National Institute of Standards and Technology (NIST).
2. The Raritan Secure Switch series additionally satisfies Protection Profile version 3.0 for Peripheral Sharing Switch (PSS).

Chapter 2 Hardware Setup

Before You Begin

If the tamper-evident seals are missing or peeled, avoid using the product and contact your Raritan dealer

If all your front panel LEDs flash continuously, or the switches' enclosure appears breached, avoid using this product and contact your Raritan dealer

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

To maximize security and to prevent unauthorized access to Secure Switch, please do change default logon password after your first successful logon.

Tampering prevention and detection

1. The Raritan Secure Switch includes Tamper-evident tape to provide visual indications of intrusion to the switches enclosure. If the tamper-evident seal is missing, peeled, or looks as if it's been adjusted, avoid using the product and contact your RARITAN dealer.
2. The Raritan Secure Switch is equipped with Active always-on chassis intrusion detection. If a mechanical intrusion is detected, the Switch will be permanently disabled and the front panel LEDs will flash continuously. If the switches' enclosure appears breeched or all the LEDs are flashing continuously, stop using it, remove it from service immediately and contact your dealer.
3. Any attempt to open the switches enclosure will activate the chassis intrusion detection security, which will render it inoperable and void the warranty.
4. The Raritan Secure Switch cannot be upgraded, serviced or repaired.
5. The Raritan Secure Switch is equipped with active always-on chassis intrusion detection security. Never attempt to open the enclosure. Any attempt to open the enclosure will permanently damage and disable the switch.
6. The Raritan Secure Switch contains an internal battery which is non-replaceable. Never attempt battery replacement or open the switches' enclosure.

Always use qualified and authorized peripheral devices

1. For security the Raritan Secure Switch supports only standard USB Keyboard/Mouse(or pointing device). Do not connect a wireless keyboard/mouse, or Keyboard/Mouse with internal USB hub or composite device functions to the switch.
2. When connecting a non-qualified keyboard, the keyboard will not function. No keyboard keystrokes will be seen on the screen.
3. When connecting a non-qualified mouse, the mouse will not function. No mouse cursor movement will be seen on the screen.
4. Num Lock LED, Caps Lock LED, and Scroll Lock LED on keyboard will be disabled due to security policy.
5. Special Multi-media keys on keyboard will be disabled due to security policy.
6. For security the Raritan Secure Switch does not support an analogue microphone or line-in audio input. Never connect a microphone to the switches' audio output port, including a headset, only standard analogue speakers and headphones are supported.
7. For security the USB CAC Port by Raritan Secure Switch supports by default only authorized User Authentication Device such as USB Smartcard or CAC reader. Do not connect other USB devices to USB CAC Port. Non-qualified or non-authorized USB devices will be rejected. (for administrative configuration, please refer to Administrator Guide and Port Authentication Utility Guide for detail)
8. For security, do not use USB CAC Authentication device or other peripherals that adopt external power source.
9. Always use qualified monitor, when the device is connected with monitor, it will check the monitor's EDID (Extended display identification data). If the check fails, the content will not be displayed on the monitor and rejected.
10. Do not use wireless video transmitters or any docking device.
11. Do not connect any Thunderbolt device to the Secure Switch.

Secure Installation

1. Do not attempt to connect or install the following devices to the computers connected to the Raritan Secure Switch: TEMPEST computers; Telecommunication equipment; Frame grabber video cards; Special audio processing cards.
2. Important safety information regarding the placement of this device is provided on page 14. 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 console monitor is not allowed. Power off the Secure Switch and the monitor before changing the console monitor.
5. A computer connected to the 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 Raritan Secure Switch user manual for hardware installation.

Secure Administrative Operation

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

Chapter 3 Operation

Powering On

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

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

During the self-test

- All Port LEDs will turn ON and then OFF
- The KVM focus will be switched to Port 1 when the self-test completes successfully (Port 1 Port LED lights GREEN)

Self-test failure

In case of self-test failure, the Secure Switch becomes inoperable, with front panel LED combination indicating the potential cause to the failure (such as button jam and KVM integrity)

- Pre-defined combination of Port LED indicates the cause to the failure.
  - Button jam: The Port of jammed button port will flash green
- If all Port LEDs flash, it means KVM tampering detected or integrity issues happened

For security, the Raritan Secure Switch becomes inoperable if self-test fails. Please verify your KVM installation, pushbuttons, and power cycle again the Security KVM. If the self-test failure remains, stop using the Raritan Secure Switch immediately, remove it from service and contact your Raritan dealer.

Reset the KVM

This Administrator function enables the authorized Administrator to reset the KVM configuration to factory default. For actual instructions, please refer to the Reset KVM to Default in the Administrator Functions Section.

Manual Switching

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

Press and release a port selection pushbutton to bring the KVM focus to the computer attached to its corresponding port (see Port ID Numbering, below). To meet maximum security and channel isolation requirements, Keyboard, Mouse, Video, Audio, and USB CAC reader port will be switched together.

The Selected Port LED lights GREEN to indicate that the computer attached to its corresponding port has the KVM focus (including Keyboard, Mouse, Monitor, Audio, and CAC reader). 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 CAC card reader,

- Please verify if you are using qualified Keyboard, Mouse, or CAC Card reader.
- Please verify if your keyboard, mouse, or CAC reader is a failed device.
- For USB CAC Card reader (USB authentication device), please make sure the USB CAC cable has been securely connected, and the CAC function is enabled.
- For USB CAC Card reader port, please contact your administrator to verify if the device you use has been authorized.

Port ID Numbering

Each KVM port on the Raritan Secure Switch is assigned a port number (1–2 for the 2-Port models; 1–4 for the 4-Port models). The port numbers are marked on the rear of the switch. See *Rear View Section* in *Raritan Secure Switch User Guide, 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, the Raritan Secure Switch has Port LEDs (Online and Selected), and CAC LED that are built into the front panel to indicate Port / CAC reader operating 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 lights WHITE to indicate that the KVM switch is powered on.
Port LED	The Port LEDs are located on the front panel to indicate the Port selection or connection status. ▪ Online – Lights WHITE to indicate that the computer attached to its corresponding port is up and running. ▪ Selected – Lights GREEN to indicate that the computer attached to its corresponding port has the KVM focus. **Note:** 1. Port LEDs will flash constantly when a chassis intrusion is detected. See Chassis Intrusion Detection section for details. 2. Port LEDs also indicate the status of the Secure Switch self-test status. See Operation section for further details
CAC LED	The CAC LED are located on front panel to indicate CAC reader selection or connection status. ▪ Light GREEN when USB authentication device is connected. ▪ Lights RED when connected USB device is rejected. (such as USB thumb drive, USB camera etc.)

Chassis Intrusion Detection

To help prevent malicious tampering with the Raritan Secure Switch, the switch becomes inoperable and the Front Panel LEDs flash GREEN constantly when a chassis intrusion, such as the cover being removed, is detected.

The Intrusion Detection is an always-on function. If all your front panel LED flash continuously, or the switches' enclosure appears breached, avoid using this product and contact your Raritan dealer.

Administrator Functions

Administrator functions by the Raritan Secure Switch enables authorized Administrator to configure the Secure Switch, 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 KVM is manufactured and can not be disabled or erased. The Raritan Secure Switch Administrator Functions enable authorized Administrator to download, view, and audit important log data and events.
- User Authentication Device filtering configuration: This function enables authorized Administrator to assign whitelist and blacklist for the User Authentication Device.
- The Secure Switch configuration: This function enables authorized Administrator to perform functions such as Reset to Factory Default.
- The “Reset to Factory Default” command on KVM clears White/Blacklists by both Admin function and Port Authentication Utility

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

Setup for Administrator Logon

Administrator must logon and be authenticated for the Secure Switch administrative operations. This section helps you setup the installation for Administrator Logon.

1. Connect qualified Keyboard, Mouse, and Display to the Raritan Secure Switch console section. (Please refer to the Secure Switch User manual for details)
2. Connect a secure source computer to Port 1 of the Secure Switch KVM Port section via KVM cable sets. The USB cable that attaches to your computer's Keyboard / Mouse must be plugged in the KVM USB Port. (Please refer to the Secure Switch User manual for details)
3. Power on first the Raritan Secure Switch, and then power on the source computer. The Raritan Secure Switch will switch to Port 1 after a successful KVM self-test.

Administrator Logon

After the Administrator setup

1. Open a text editor on the connected source computer

2. Use the console keyboard and
   a. Press and hold down the Ctrl key
   b. Press the F12 key:
      [Ctrl] + [F12]
   c. Release the Ctrl and F12 key, press [L] key, and then press [Enter]

   After successful input of the key sequence, you will be in Administrator Logon mode and be prompted in text editor to be authenticated.

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

ATTENTION

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

4. The default Administrator password for the first-time logon is:
   ABCD@xyz#2468!

   a. The password is case-sensitive
   b. Use [Shift] key for upper case letters and special characters

5. A [Logon OK] message prompts if the password input is correct; you will be prompt to input password again if the input password is wrong.

   a. With 3 (three) failed attempts to logon, the Administrator Logon mode will be terminated automatically. Access to Administrator Logon mode will be blocked for 15 minutes.
   b. With 9 (nine) failed attempts to logon, the Secure Switch becomes inoperable permanently. Please remove it from service immediately and contact your Raritan dealer.

6. Type [LIST] and press [Enter] for Administrator Functions after [Logon OK] message for Administrator Functions. (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 contain,

    a. At least 8 characters in length, but no longer 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

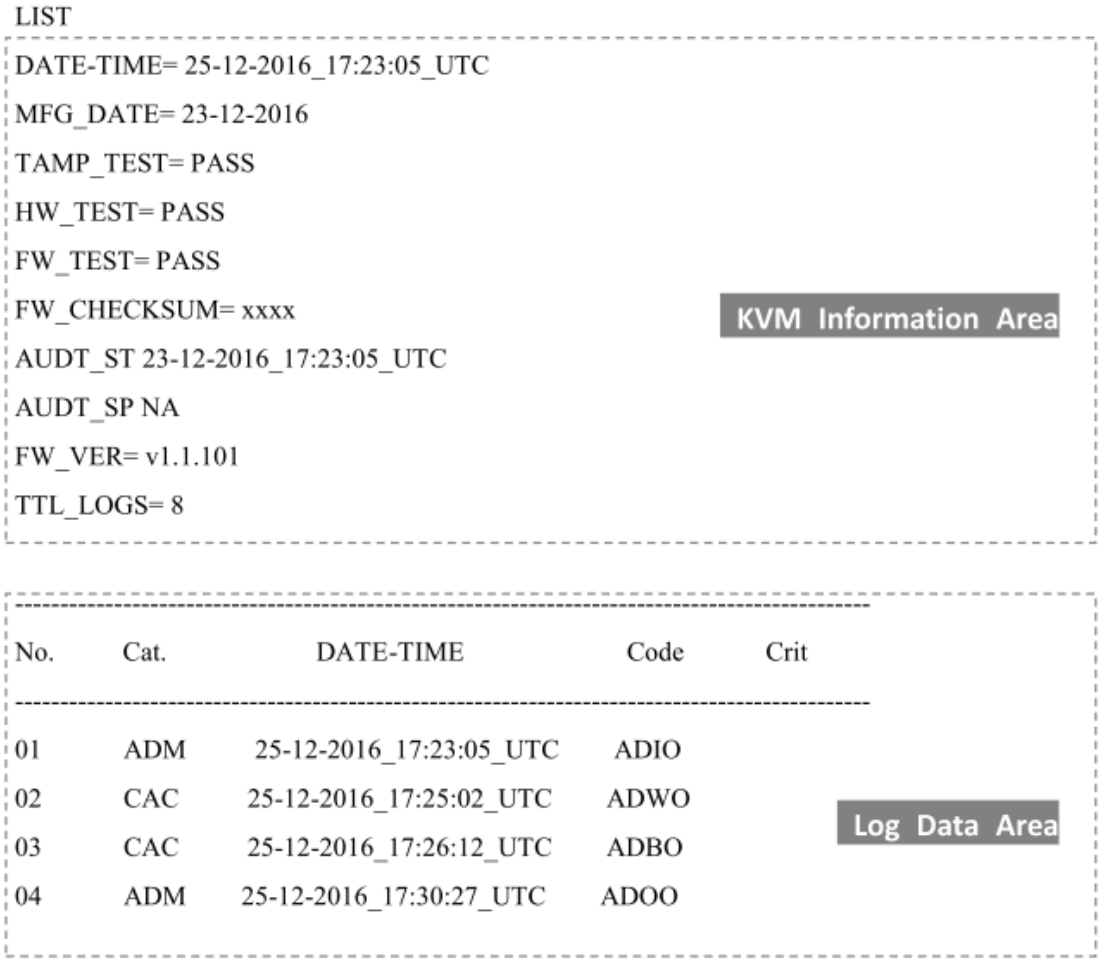
    Do not use the default Administrator password for your new password. Administrator will be asked to enter new password again for confirmation.
    Once the new Administrator Logon password is selected, the default Administrator Logon password will not be restored even after Reset to Factory Default.

Log data audit

Log data recording is activated when the KVM is manufactured and can not be disabled or erased. After the successful Administrator Logon, type the command [LIST] to view logs data in the text editor. (Command “LIST” displays administrator functions)

Administrator Logon Mode
ID: Administrator
Please enter password: ********

Logon ok.



Operation ok

For the menu interface information, please refer to the Raritan PP3.0 Secure Switch Admin Log Audit Code Document.

1. KVM Information Area

   This area displays the Secure Switch status and critical information

   a. DATE-TIME: Current Date and Time in UTC
   b. MFG_DATE: Manufacturing Date (in UTC) of the Secure Switch
   c. TAMP_TEST: The Secure Switch Tamper protection test status
   d. HW_TEST: The Secure Switch hardware self-test status
   e. FW_TEST: The Secure Switch firmware self-test status
   f. FW_CHECKSUM: The Secure Switch firmware checksum for firmware integrity check.
   g. AUDT_ST: Date and Time (in UTC) when the KVM activates all protection mechanism and starts generating log data.

h. AUDT_SP: “NA” will be displayed if the Secure Switch functions normally.
If events that trigger the Secure Switch protection mechanism are detected, and make the KVM shut down and become inoperable, a Date/Time log will be recorded for the Secure Switch manufacturer. (This particular Date/Time log can only be decoded by the Secure Switch manufacture)

i. i. FW_VER: Firmware version

j. j. TTL_LOGS: Total numbers of Log data

2. 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 such as 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.

a. Critical Log Data:
Critical Log Data includes Administrator Logon events (up to four events), Administrator password change events (up to two events), Critical Administrator KVM configuration (one event), and 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 and keep the last one record.

b. Non-critical Log Data:
Non-critical Log Data includes 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.

Maximum thirty-two Non-critical Log Data logs will be kept 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 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 finding the detail description on port authentication utility, please refer to the Raritan Port Authentication Document

Reset KVM to Default

This Administrator function enables the authorized Administrator to reset the KVM configuration to factory default.

1. When Administrator performs Reset KVM to Default, settings previously configured by Administrator (such as USB device whitelist/blacklist) will be cleaned and reset to factory default settings.
2. Once Reset KVM to Default has been 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 Port1, and CAC function of each port will be set to factory default (enabled).
3. Reset KVM to Default will not affect or erase Log data.
4. Reset KVM to Default will not affect previously changed Administrator password
5. Reset KVM to Default will clear the whitelist/blacklist created by both the Secure KVM administrator functions and the Raritan Port Authentication Utility

Reset KVM to Factory Default (Actual Instructions)

1. Press the Reset button on the front panel to reset the Raritan Secure Switch.
2. When performing the reset function by pressing Reset Button for more than 5 seconds, Keyboard/Mouse buffer will be purged and KVM will reboot and perform self-test.
3. After a successful self-test, port focus will be switched to Port1, and CAC function of each port will be set to factory default (enabled).
4. If the Secure Switch fails to generate video on the monitor after reset, please power off the installation, check the installation, and follow the operation instructions in user manual to power on the installation.

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 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 , 50-60Hz 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.
- MAINTENANCE STAFF CAUTION
  RISK OF EXPLOSION IF BATTERY IS REPLACED BY AN INCORRECT TYPE.
  DISPOSE OF USED BATTERIES ACCORDING TO THE INSTRUCTIONS.